UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

“Diseño de un sistema de seguridad CCTV mediante una red WIFI para el monitoreo y control del edificio de la Gobernación de El Oro”

AUTOR:

Ing. Wilson Alejandro Madrid Pacheco

Previa la obtención del Grado Académico de Magíster en Telecomunicaciones

TUTOR:

MSc. Manuel Romero Paz

Guayaquil, 9 de noviembre de 2020

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Ingeniero **Wilson Alejandro Madrid Pacheco** como requerimiento parcial para la obtención del Grado Académico de Magíster en Telecomunicaciones.

Guayaquil, 9 de noviembre de 2020

TUTOR

M. Sc. Manuel Romero

DIRECTOR DEL PROGRAMA

M. Sc. Manuel de Jesús Romero Paz

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

DECLARACIÓN DE RESPONSABILIDAD

YO, WILSON ALEJANDRO MADRID PACHECO

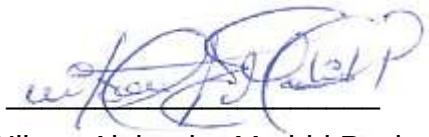
DECLARÓ QUE:

El Trabajo de Titulación **"Diseño de un sistema de seguridad CCTV mediante una red WIFI para el monitoreo y control del edificio de la Gobernación de El Oro",** previa a la obtención del grado Académico de Magíster, ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan en el documento. Consecuentemente este trabajo es mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación del Grado Académico en mención.

Guayaquil, 9 de noviembre de 2020

EL AUTOR



Ing. Wilson Alejandro Madrid Pacheco

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

AUTORIZACIÓN

YO, **WILSON ALEJANDRO MADRID PACHECO**

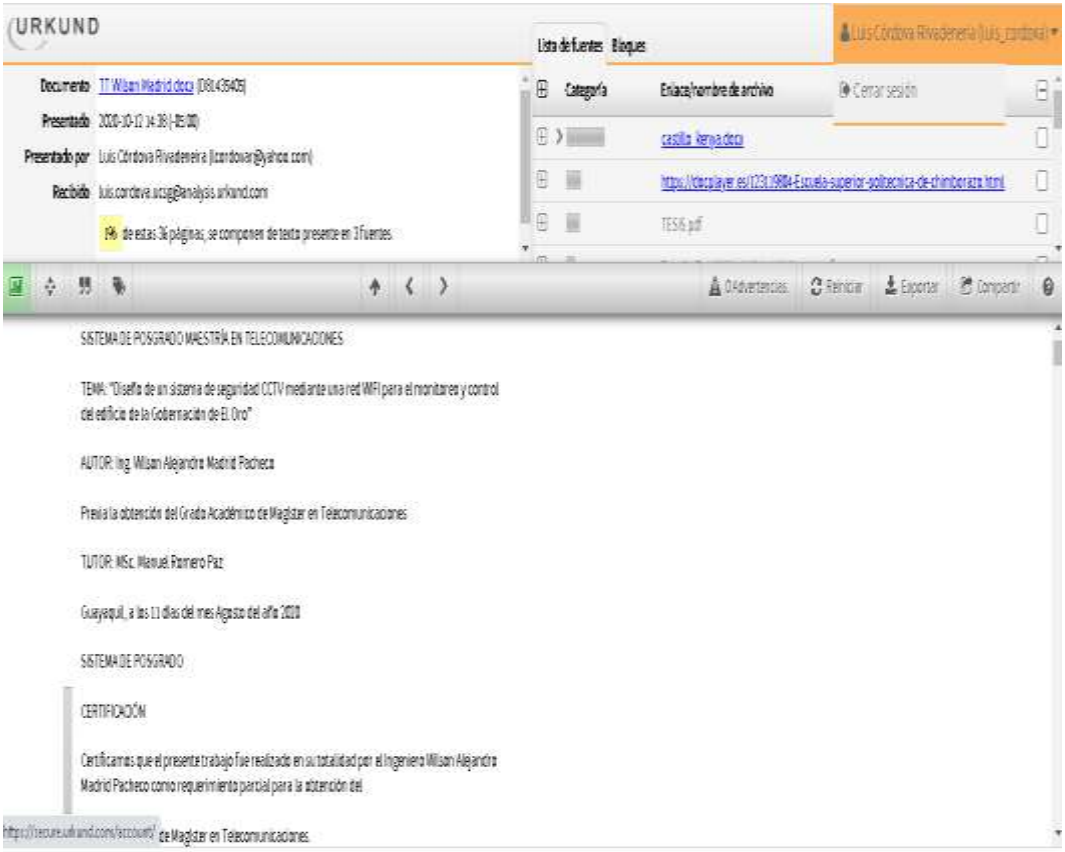
Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación de Maestría titulado: “Diseño de un sistema de seguridad CCTV mediante una red WIFI para el monitoreo y control del edificio de la Gobernación de El Oro”, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, 9 de noviembre de 2020

EL AUTOR

Ing. Wilson Alejandro Madrid Pacheco

REPORTE URKUND



Dedicatoria

La elaboración de este proyecto de tesis está dedicada a mis Hijos, a mis Padres, a mis Hermanos y a mis Sobrinos, pilares fundamentales en mi vida. Sin ellos, jamás hubiera conseguido lo que he logrado hasta ahora. La tenacidad de mis Padres y su lucha insaciable, han hecho de ellos el gran ejemplo a seguir y destacar, no solo para mí, sino para mis hermanos y familia en general.

A mis hijos, por ser mis compañeros inseparables de cada jornada diaria en mi vida, representando grandes esfuerzos y pilares fundamentales en momentos de decline y cansancio con su apoyo sentimental.

A todos ellos este proyecto de tesis, que, sin ellos, no hubiese podido ser.

Ing. Wilson Alejandro Madrid Pacheco

Agradecimientos

Este proyecto de tesis es el resultado del esfuerzo y apoyo de muchas personas que han estado pendiente de mí durante el transcurso de mi trabajo, estudios y de mi vida.

En primer lugar, quiero agradecer a DIOS, por ayudarme a superar los diversos obstáculos que me presenta la vida; y a pesar de las adversidades, bendecirme para llegar hasta donde he llegado el día de hoy.

A los docentes, a quienes les debo gran parte de mis conocimientos, gracias a su paciencia y enseñanza, brindándome siempre su orientación con profesionalismo moral y ético durante este largo camino.

A mis padres Alejandro, Cumandá, a mis hermanos Carlos, Christian, Dhiego, Daniel y a mi tía Blanca, quienes a lo largo de toda mi vida han apoyado y motivado mi formación académica; creyeron en mí en todo momento y no dudaron de mi dedicación y habilidades.

A mis hijos Danna Jackeline y Wilson Alejandro, quienes en el transcurso del camino a pesar de la distancia que nos separa, me ayudaron a seguir con mis estudios, brindándome su amor, confianza y apoyo.

A mi director de tesis, Msc. Manuel Romero Paz, a mis revisores y finalmente a esta prestigiosa Universidad, la cual abre sus puertas a profesionales como yo, preparándonos para un futuro más competitivo.

¡Gracias de corazón!

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

MSc. Manuel Romero Paz
TUTOR

f. _____

MSc. Manuel Romero Paz
DIRECTOR DEL PROGRAMA

f. _____

MSc. Luis Córdova Rivadeneira
REVISOR

f._____

MSc. Edgar Quezada Calle
REVISOR

ÍNDICE GENERAL

ÍNDICE DE TABLAS

CAPÍTULO 2:

CAPÍTULO 3:

ÍNDICE DE FIGURAS

CAPÍTULO 2:

CAPÍTULO 3:

Resumen

El presente proyecto se enfoca en el diseño de un sistema de seguridad de circuito cerrado de televisión CCTV para el monitoreo y control de las actividades diarias que se desarrollan en el edificio donde funciona actualmente la Gobernación de la Provincia de El Oro, utilizando cámaras con protocolo IP que manejan estándares de tecnología inalámbrica para monitorear las oficinas, pasillos y demás departamentos u oficinas en el edificio. La comunicación entre los equipos que conforman el sistema de seguridad CCTV se la realizará mediante una red Wireless, la cual estará conformada mediante dispositivos de Puntos de Acceso (Access Point); es decir equipos que utilizan radiofrecuencia a través de antenas omnidireccionales. Además, estos equipos que pertenecerán a la red Wifi podrán ser usados para que determinados funcionarios puedan tener acceso o salida al internet. El capítulo 1, describe las generalidades del proyecto donde se justifica la propuesta de innovación tecnológica ante un problema palpable dentro de la Institución. El capítulo 2, describe una fundamentación teórica amplia e investigativa correspondiente a los sistemas de circuito cerrado de televisión CCTV y a las tecnologías inalámbricas, sirviendo como herramientas de control, monitoreo y seguridad. El capítulo 3, describe la parte física y el diseño de un sistema de circuito cerrado de televisión CCTV a través de una red Wifi, considerando su funcionalidad basada en la seguridad. Finalmente, se presentan las conclusiones y recomendaciones que surgen de este proyecto.

Palabras clave: WLAN, CCTV, DVR, Cámara de Video Vigilancia, Switch, WiFi

Abstract

This project focuses on the design of a closed circuit television CCTV security system for the monitoring and control of the daily activities that take place in the building where the Government of the Province of El Oro currently operates, using cameras with protocol IP that handle wireless technology standards to monitor offices, corridors and other departments or offices in the building. Communication between the equipment that make up the CCTV security system will be done through a Wireless network, which will be made up of Access Point devices; in other words, equipment that uses radio frequency through omnidirectional antennas. In addition, these computers that will belong to the Wifi network may be used so that certain officials can have access or exit to the internet. Chapter 1 describes the generalities of the graduation project where the technological innovation proposal is justified in the face of a palpable problem within the Institution. Chapter 2 describes a broad theoretical and investigative foundation corresponding to CCTV closed circuit television systems and wireless technologies, serving as control, monitoring and security tools. Chapter 3 describes the physical part and the design of a CCTV closed circuit television system through a Wifi network, considering its functionality based on security. Finally, the conclusions and recommendations arising from this project are presented.

Key words: WLAN, CCTV, DVR, Video Surveillance Camera, Switch, WiFi

Capítulo 1: Descripción del proyecto de intervención.

En este capítulo se presentan las características generales de la investigación, los antecedentes, el problema, los objetivos y la metodología a aplicarse.

1.1 Introducción.

La Gobernación de la Provincia de El Oro es una Institución del Estado que pertenece al Ministerio de Gobierno. El edificio se encuentra ubicado en el centro de la ciudad de Machala en las calles Rocafuerte y Guayas esquina, donde funcionan las oficinas de las unidades administrativas de: Talento Humano, Dirección Administrativa Financiero, Planificación y Gestión Estratégica, Tecnologías de la Información y Comunicación, Comunicación Social, Secretaría, Despacho del Gobernador, Jefatura Política del Cantón Machala, Intendencia General de Policía y Comisaría Primera Nacional de Policía del Cantón Machala, siendo estas tres últimas las que mayor afluencia de personas tienen a diario, debido a la atención y desarrollo de actividades directamente ligadas con la ciudadanía.

Actualmente el edificio se encuentra ubicado en una de las zonas más transitadas de la ciudad y con mayor afluencia de personas. Por tal motivo existe la necesidad de usar y aprovechar la tecnología para mejorar e implementar un sistema de seguridad que sea una ayuda para monitorear a las personas que ingresan a las diferentes unidades u oficinas que conforman la estructura funcional y organizacional de la Gobernación, para lo cual es necesario efectuar en la Institución un sistema de seguridad basada en la utilización de cámaras IP con tecnología Wifi. Actualmente la institución cuenta con una red inalámbrica que no es lo suficientemente robusta para soportar este tipo de implementación, razón por la cual se diseñará una red que permita interconectar todo tipo de dispositivo con esta tecnología.

La tendencia a este tipo de tecnología tiene como finalidad principal evitar la infraestructura física que corresponde al cableado estructurado en una red de telecomunicaciones, por ello la tecnología Wifi brinda este y otros beneficios que permiten trabajar en lugares donde la conexión de dispositivos por medio de cable es prácticamente imposible de realizar. Por ende y gracias a este tipo de avances tecnológicos, los sistemas de seguridad de circuito cerrado de televisión (CCTV, Closed Circuit Television) han ido evolucionando con el tiempo y a la vez adaptándose a las nuevas tecnologías del mercado y para ello las diferentes industrias han creado un sin número de dispositivos de seguridad de tipo inalámbrico como las cámaras de seguridad con wifi incluido, con los que se puede tener un control de las zonas vulnerables y de difícil acceso por medio del cableado estructurado; y de esta forma obtener el monitoreo de las actividades que se generan dentro o fuera de una edificación.

Una de las ventajas de este tipo de tecnología, es poder centralizar la información y administrarla con el fin de que se pueda utilizar en dispositivos móviles.

1.2 Antecedentes.

El sistema CCTV que actualmente se encuentra implementado para monitorear la seguridad del edificio de la Gobernación de la Provincia de El Oro, es de tecnología obsoleta, con el que vienen trabajando desde hace más de cinco años, es un sistema de video seguridad análogo que cuenta con un grabador de video digital o DVR con 24 puertos, en el que se encuentran conectadas 12 cámaras de seguridad tipo domo con una calidad de resolución de video SVGA de 800x600 píxeles, de las cuales actualmente solo 5 se encuentran funcionando y operando con normalidad.

Las cámaras de seguridad se encuentran ubicadas en lugares que no son considerados puntos estratégicos para realizar coberturas correctas de las zonas que se consideran de alto riesgo, esto debido a que con el transcurso del tiempo varios departamentos u oficinas de dicha Institución han sido

reubicadas y por ende existen muchas localidades en los cuales se atiende a los usuarios y deben ser consideradas fundamentales, para su respectivo monitoreo por medio del sistema CCTV.

Como ya se ha mencionado anteriormente, el sistema de CCTV que actualmente dispone la Gobernación de la Provincia de El Oro es un sistema análogo con un cableado estructurado antiguo y deteriorado, que conecta las diferentes cámaras hacia el grabador de video digital o DVR; por lo que presenta ciertas intermitencias al visualizar los videos de las cámaras. Además, cabe recalcar que la Institución no cuenta con puntos de acceso Wifi en la mayoría de los pisos de su estructura.

Este proyecto pretende mejorar todos los aspectos del Sistema CCTV mencionado, a través de un diseño donde se plantea el cambio de tecnología análoga a digital y el uso de cámaras con tecnología Wifi, como también el diseño de una red inalámbrica que permita la conexión de los elementos del sistema CCTV.

1.3 Definición del problema.

La necesidad de la Institución para garantizar la seguridad de los bienes y del personal que labora en el edificio, hace que sea necesario el diseño de un sistema de seguridad CCTV mediante una red Wifi, debido a su versatilidad para adaptarse a los diferentes entornos de una edificación.

1.4 Justificación.

La razón por la que este proyecto se desea llevar a cabo es de carácter tecnológico, porque con este sistema se pretende aprovechar la tecnología Wifi para establecer un sistema de seguridad CTTV, mejorando la calidad de monitoreo y control de las actividades que se realizan dentro del edificio.

Además, otra de las necesidades es disponer de estos dispositivos para poder centralizar y administrar la información, reemplazando de esta manera los equipos de tecnologías obsoletas existentes.

Fundamentalmente, los aspectos antes mencionados llevan a plantearse el diseño de este sistema de seguridad que ayudaría al monitoreo y control de las actividades dentro del edificio de la Institución.

1.5 Objetivos.

Los objetivos que se han planteado para este trabajo de investigación son los siguientes:

1.5.1 Objetivo General.

- Diseñar un sistema de seguridad CCTV mediante una red Wifi para el monitoreo y control de actividades en el edificio de la Gobernación de la Provincia de El Oro.

1.5.2 Objetivos Específicos.

- Establecer la fundamentación teórica de la tecnología de transmisión inalámbrica.
- Presentar los principales fundamentos de los sistemas de video seguridad.
- Caracterizar una red Wifi que pueda soportar la transmisión de video de un sistema CCTV.
- Diseñar un sistema de seguridad digital con tecnología Wifi que sea lo suficientemente viable y estable para el monitoreo permanente de los diferentes departamentos y oficinas de la Institución.

1.6 Hipótesis.

El uso de un sistema de seguridad CCTV mediante una red Wifi es una opción sustentable para potencializar la seguridad dentro del edificio de la Gobernación de la Provincia de El Oro.

Este sistema garantizará un mejor control y monitoreo de las personas que salen e ingresan de las oficinas y el desarrollo de las actividades en los diferentes pisos del edificio de la Institución.

1.7 Metodología de investigación.

Este trabajo de tesis se enmarca en el tipo de investigación descriptiva y exploratoria, utiliza un enfoque metodológico cuantitativo porque se debe diseñar una red Wifi con varios puntos de acceso (AP, Access Point), con el fin de que la cobertura en las áreas administrativas sea total.

Capítulo 2: Fundamentación Teórica.

Entre los avances tecnológicos más importantes que han existido con el transcurso de los años y que siempre ha estado evolucionando, ha sido precisamente la tecnología inalámbrica y el método de transmisión de la información de datos entre diferentes dispositivos, sin la necesidad de utilizar el cableado estructurado o medio físico.

Gracias a este importante crecimiento tecnológico y a un sin número de protocolos de comunicación inalámbrica, se ha venido incrementando la interoperabilidad de dispositivos producidos por diferentes fabricantes de equipos tecnológicos, entre los cuales se encuentran los que conforman un sistema de seguridad de video vigilancia, estos sistemas originalmente empezaron utilizando un circuito cerrado de televisión, el mismo que contaba con cámaras de video analógicas, grabadoras y el medio físico de conexión de dispositivos conformado por cable coaxial.

El sistema CCTV es una tecnología de video vigilancia que tiene como objetivo principal supervisar, monitorear y grabar de manera continua lo que se está llevando a cabo en un área determinada en tiempo real. Se la denomina circuito cerrado, debido a que todos sus componentes se encuentran enlazados entre sí.

2.1 Redes Inalámbricas.

Una red inalámbrica es aquella que permite conectar y comunicar dos o más terminales sin la necesidad de utilizar una conexión física, sino estableciendo la comunicación basada en un enlace mediante ondas electromagnéticas o radio frecuencia. La transmisión y la recepción de datos, requiere de dispositivos que actúen como puertos para poder comunicarse.

Las redes inalámbricas han evolucionado con el pasar de los años, lo que ha llevado a la creación de varios tipos de tecnologías, las cuales van a depender básicamente de la frecuencia, velocidad y distancia de cobertura que se quiera tener en una transmisión de datos entre dos o más dispositivos.

2.1.1 Tipos de Redes Inalámbricas.

Las redes inalámbricas pueden clasificarse en diferentes tipos o categorías de acuerdo con su velocidad, frecuencia y rango de cobertura en:

- Red de Área Personal Inalámbrica (WPAN, Wireless Personal Area Network).
- Red de Área Local Inalámbrica (WLAN, Wireless Local Area Network).
- Red de Área Metropolitana Inalámbrica (WMAN, Wireless Metropolitan Area Network).
- Red de Área Amplia Inalámbrica (WWAN, Wireless Wide Area Network).

2.1.1.1 Red de Área Personal Inalámbrica (WPAN).

Permite establecer la comunicación específicamente en espacios personales o pequeños mediante tecnologías HomeRF, basadas en protocolos de acceso compartido, que utilizan las ondas de radio para la transmisión de datos y la interconexión de equipos o dispositivos de manera inalámbrica, eliminando la necesidad de medios físicos.

Algunos tipos de tecnología HomeRF son:

- Bluetooth.
- Identificación de Radio Frecuencia (RFID, Radio Frequency Identification).

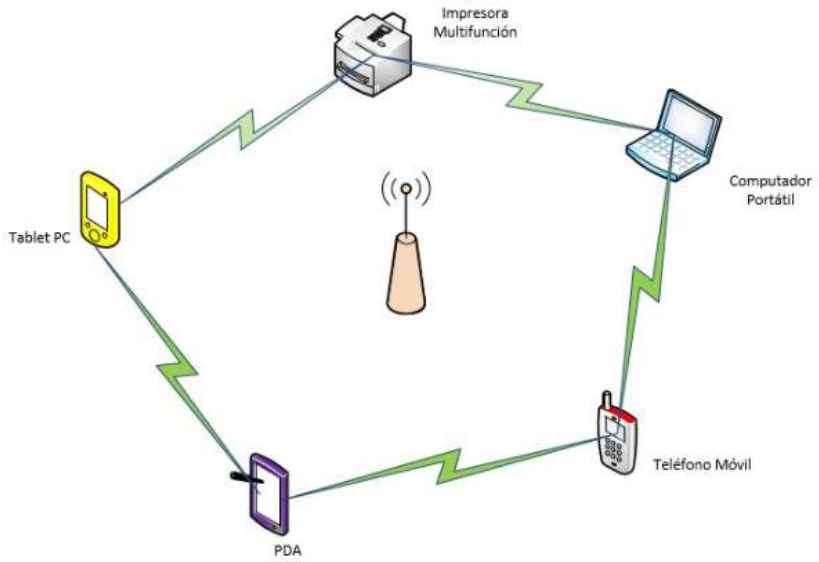


Figura 2.1: Red de Área Personal Inalámbrica (WPAN).
Fuente: Elaborado por el Autor.

Bluetooth: Se utiliza para la conectividad y comunicación inalámbrica de corto alcance con bajas tasas de transmisión de datos entre dispositivos, para compartir y sincronizar información, con la posibilidad de crear redes inalámbricas domésticas.

Figura 2.2: Conectividad Bluetooth entre dos computadores portátiles.
Fuente: Elaborada por el Autor.

RFID: Sistema de comunicación, almacenamiento y recuperación de datos que permite transmitir mediante ondas de radio de alta o baja frecuencia, la identidad de un dispositivo a distancia a un lector cerca sin necesidad de tener contacto.

Figura 2.3: Sistema RFID.
Fuente: Elaborada por el Autor.

2.1.1.2 Red de Área Local Inalámbrica (WLAN).

Este tipo de redes permite transmitir y recibir datos por radiofrecuencia en áreas moderadas donde la cobertura no es muy extensa. Está basada en el estándar IEEE802.11 (WiFi/Wireless Fidelity), la misma que será utilizada en este proyecto por su gran flexibilidad y movilidad en la comunicación entre sus dispositivos.

Figura 2.4: Red de Área Local Inalámbrica (WLAN).
Fuente: Elaborada por el Autor.

2.1.1.3 Red de Área Metropolitana Inalámbrica (WMAN).

Este tipo de redes inalámbricas son también conocidas como bucle local inalámbrico (WLL, Wireless Local Loop), fueron desarrolladas bajo el estándar IEEE 802.16, usan la tecnología WIMAX (Worldwide Interoperability for Microwave Access), para un largo alcance con mayor transmisión de ancho de banda y ofrecen velocidades de 1 a 10 Mbps, con una cobertura de 4 a 10 kilómetros.

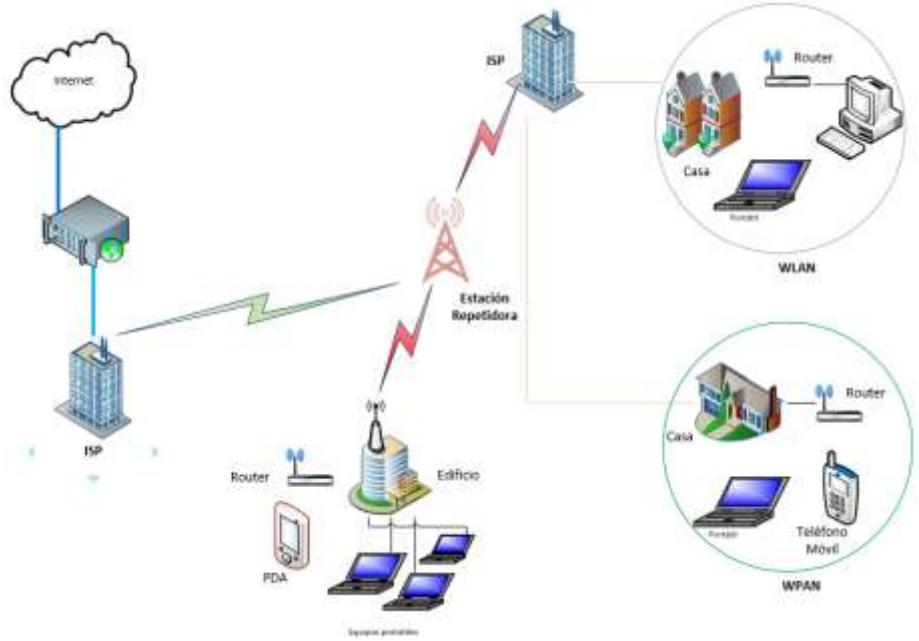


Figura 2.5: Red de Área Metropolitana Inalámbrica (WMAN).
Fuente: Elaborada por el Autor.

2.1.1.4 Red de Área Amplia Inalámbrica (WWAN).

Posee el alcance más amplio entre las redes inalámbricas, usan tecnologías de red celular de comunicaciones móviles como WiMAX, UMTS (Universal Mobile Telecommunications System), GPRS (General Packet Radio Service), EDGE (Enhanced Data Rates for GSM Evolution), GSM (Global System for Mobile communications), HSPA (High-Speed Packet Access), 3G y 4G entre otras, para transferir los datos y comunicarse. También incluye el sistema de distribución local multipunto (LMDS, Local Multipoint Distribution Service) y Wifi autónoma para conectar a internet.

Figura 2.6: Red de Área Amplia Inalámbrica (WWAN).
Fuente: Elaborada por el Autor.

2.2 Estándares de Redes Inalámbricas WLAN.

El desarrollo de estándares está a cargo de organismos reconocidos internacionalmente, los cuales se convierten en la base de los fabricantes para desarrollar sus productos para permitir la interoperabilidad con otros dispositivos inalámbricos.

Uno de los organismos reconocidos internacionalmente es el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, Institute of Electrical and Electronics Engineers) y su estándar principal en redes WLAN es el 802.11.

2.2.1 Estándar Inalámbrico IEEE 802.11 o Wifi.

Este estándar fue aprobado en 1997, con el objetivo de definir normas y modalidades para la transmisión de datos, utilizando al aire como medio de transmisión para lograr la comunicación a través de ondas electromagnéticas, de los equipos o dispositivos en áreas limitadas.

Además, es un estándar que define el uso de los dos niveles más bajos de la arquitectura OSI (Open System Interconnection), capa física y enlace de

datos, especificando sus normas de funcionamiento en una red WLAN y soportando velocidades de transmisión entre 1 Mbps y 2 Mbps.

Los protocolos que contiene este estándar son:

- IEEE 802.11 a.
- IEEE 802.11 b.
- IEEE 802.11 g.
- IEEE 802.11 n.
- IEEE 802.11 ac.
- IEEE 802.11 ad.
- IEEE 802.11 ah.

2.2.1.1 Estándar IEEE 802.11a.

Aprobado en 1999, utiliza el mismo protocolo de base que el estándar original y una técnica de modulación de 52 sub-portadoras de Acceso Múltiple por División de Frecuencia (OFDM, Orthogonal Frequency Division Multiplexing) para la velocidad de transmisión de datos.

Las características del estándar IEEE 802.11a son:

Tabla 2.1: Características del estándar IEEE 802.11a.

IEEE 802.11a	
Banda de Frecuencia:	5 GHz
Ancho de banda de canal o espectro:	22 MHz
Esquema de Modulación:	BPSK a 256-QAM
Técnica de Radio:	OFDM
Tasa mínima de Datos:	25 Mbps
Tasa Máxima de Datos:	54 Mbps
Alcance:	35 metros
Máxima potencia de transmisión:	100 mW

Fuente: Elaborada por el Autor.

2.2.1.2 Estándar IEEE 802.11b.

Este estándar fue aprobado en 1999, utiliza exclusivamente la técnica de modulación del espectro ensanchado por secuencia directa (DSSS, Direct Sequence Spread Spectrum) con el sistema de codificación de clave de código complementario (CCK, Complementary Code Keying), que permiten aumentar la velocidad de transmisión de datos y lograr una máxima de hasta 11 Mbps. Además, ofrece seguridad de calidad de servicio (QoS, Quality of Service) con menos interferencias que el estándar anterior.

Las características del estándar IEEE 802.11b son:

Tabla 2.2: Características del estándar IEEE 802.11b.

IEEE 802.11b	
Banda de Frecuencia:	2.4 GHz
Ancho de banda de canal o espectro:	21 MHz
Esquema de Modulación:	BPSK a 256-QAM
Técnica de Radio:	DSSS
Tasa mínima de Datos:	6.5 Mbps
Tasa Máxima de Datos:	11 Mbps
Alcance:	35 metros
Máxima potencia de transmisión:	100 mW

Fuente: Elaborada por el Autor.

2.2.1.3 Estándar IEEE 802.11g.

Este estándar fue aprobado en el año 2003, además de usar la técnica de modulación DSSS como el estándar anterior, incorpora la modulación OFDM para obtener una mayor velocidad en la banda de frecuencia 2.4GHz.

Las características del estándar IEEE 802.11g son:

Tabla 2.3: Características del estándar IEEE 802.11g.

IEEE 802.11g	
Banda de Frecuencia:	2.4 GHz
Ancho de banda de canal o espectro:	23 MHz
Esquema de Modulación:	BPSK a 256-QAM
Técnica de Radio:	DSSS - OFDM
Tasa mínima de Datos:	25 Mbps
Tasa Máxima de Datos:	54 Mbps
Alcance:	100 metros – 150 metros
Máxima potencia de transmisión:	100 mW

Fuente: Elaborada por el Autor.

2.2.1.4 Estándar IEEE 802.11n.

Este estándar fue aprobado en el año 2009 y es el primero en incorporar las tecnologías de enlaces de canales (Channel Bonding) y múltiple entrada-múltiple salida (MIMO, Multiple-Input Multiple-Output), lo que permite utilizar varios canales para transmitir datos simultáneamente. Además, puede trabajar en dos bandas de frecuencia como 2.4 GHz y 5 GHz, lo que le permite tener una compatibilidad con todas las versiones del estándar 802.11 y mejorar la recepción de la señal y el rango de recepción.

Las características del estándar IEEE 802.11n son:

Tabla 2.4: Características del estándar IEEE 802.11n.

IEEE 802.11n	
Banda de Frecuencia:	2.4 GHz - 5 GHz
Ancho de banda de canal o espectro:	24 MHz – 40 MHz
Esquema de Modulación:	BPSK a 256-QAM
Técnica de Radio:	OFDM
Tasa mínima de Datos:	200 Mbps
Tasa Máxima de Datos:	600 Mbps
Alcance:	820 metros
Máxima potencia de transmisión:	100 mW

Fuente: Elaborada por el Autor

2.2.1.5 Estándar IEEE 802.11ac.

Este estándar fue aprobado en el año 2014, mejora las tasas de transferencia por flujo de datos y amplía el ancho de banda hasta 160 MHz utilizando hasta 8 flujos MIMO, para transmitir datos idénticos al mismo tiempo y a múltiples destinatarios, optimizando la conectividad y aumentando la velocidad. Además, es compatible con las anteriores versiones del estándar 802.11 debido a que puede operar en frecuencias de 2.5 GHz y 5 GHz, es conocido también como Wifi 5.

Teóricamente la velocidad de transmisión de datos por este estándar inalámbrico puede llegar a ser tan rápida como la velocidad de transmisión de datos por cable.
Las características del estándar IEEE 802.11ac son:

Tabla 2.5: Características del estándar IEEE 802.11ac.

IEEE 802.11ac	
Banda de Frecuencia:	5 GHz.
Ancho de banda de canal o espectro:	20 MHz – 40 MHz – 80 MHz – 160 MHz
Esquema de Modulación:	BPSK a 256-QAM
Técnica de Radio:	OFDM
Tasa mínima de Datos:	450 Mbps
Tasa Máxima de Datos:	1.3 Gbps
Alcance:	90 a 100 metros
Máxima potencia de transmisión:	160 mW

Fuente: Elaborada por el Autor.

2.2.1.6 Estándar IEEE 802.11ad.

Este estándar fue aprobado en el año 2013, utiliza la modulación OFDM y permite comunicaciones de alta velocidad, pero de corto alcance en líneas de visión directas, es decir, en áreas que no presenten obstáculos como paredes, techos u otros objetos que puedan obstruir la señal, se puede transmitir una mayor cantidad de datos desde un dispositivo a otro en una

misma área con una velocidad de hasta 6,76 Gbps. Este estándar es conocido también como WiGig. Las características del estándar IEEE 802.11ad son:

Tabla 2.6: Características del estándar IEEE 802.11ad.

IEEE 802.11ad	
Banda de Frecuencia:	60 GHz.
Ancho de banda de canal o espectro:	Hasta 2160 MHz.
Esquema de Modulación:	BPSK a 64-QAM
Técnica de Radio:	SC - OFDM
Tasa Máxima de Datos:	6.76 Gbps
Alcance:	10 metros
Máxima potencia de transmisión:	10 mW

Fuente: Elaborada por el Autor

2.2.1.7 Estándar IEEE 802.11ah.

Este estándar fue aprobado en el año 2016, se encuentra diseñado para trabajar en el espectro de espacios en blanco de las bandas VHF (Very High Frequency) y UHF (Ultra High Frequency), que habitualmente se asocian a las señales de televisión, operando por debajo de las bandas de frecuencia de 1 GHz que son espectros que los canales de televisión no utilizan, permitiendo de esta manera realizar transmisiones de datos hasta 1 kilómetro de distancia con un menor consumo de energía por parte del equipo o dispositivo. Este estándar es conocido también como Súper Wifi. Las características del estándar IEEE 802.11ah son:

Tabla 2.2.1.7: Características del estándar IEEE 802.11ad.

IEEE 802.11ah	
Banda de Frecuencia:	900 MHz
Ancho de Banda:	1 MHz–2 MHz–4 MHz–8 MHz–16 MHz
Esquema de Modulación:	BPSK a 256-QAM
Técnica de Radio:	SC - OFDMA
Tasa Máxima de Datos:	7 Gbps
Alcance:	1 km
Máxima potencia de transmisión:	100 mW

Fuente: Elaborada por el Autor.

2.2.2 Ventajas del Estándar IEEE 802.11.

Las ventajas de este estándar se las puede clasificar en:

- **Escalabilidad:** Las redes WLAN pueden ser utilizadas en varias topologías para poder satisfacer y cubrir necesidades de los usuarios finales. Además, brinda facilidad en la configuración e incorporación de nuevos usuarios a la red.
- **Flexibilidad:** Este tipo de tecnología inalámbrica permite llegar a los dispositivos donde la implementación por medio del cableado para realizar la comunicación entre dos dispositivos es imposible o complicada de realizar.
- **Movilidad:** Pueden proveer a los usuarios de una red LAN el acceso a la información en tiempo real, desde cualquier lugar dentro del entorno y cobertura en el que se encuentran desplegadas, que incluye oportunidades de productividad y servicio que no es posible en una red cableada.
- **Manejo e Instalación:** Es fácil y rápida de configurar, además de que su instalación es muy sencilla y va a depender del área que se requiere cubrir.
- **Costo:** La inversión inicial en una estructura LAN inalámbrica es mayor a la de una cableada, pero los beneficios y costos a largo plazo pueden ser superiores en ambientes donde los movimientos estructurales son frecuentes.

2.2.3 Desventajas del Estándar IEEE 802.11.

Las desventajas de este estándar son:

- **Seguridad:** Son vulnerables y accesibles a través de dispositivos móviles.
- **Velocidad:** Son de menor velocidad que una red cableada, debido a las interferencias y pérdidas de señal que el entorno pueda provocar.

- **Interferencia:** Son propensas a las interferencias, debido a la progresiva saturación del espectro radioeléctrico con señales comunes como las de los teléfonos móviles, lo que afecta la conexión a larga distancia.

El estándar 802.11 siempre está en continua evolución, debido a las investigaciones para mejorarlo a partir de sus especificaciones.

2.3 Seguridad en redes Wifi.

La seguridad en redes inalámbricas es la encargada de que los datos transmitidos a nivel de protocolo tengan un algoritmo de codificación y gestión de claves, para que no puedan ser descifrados y así obtener una red inalámbrica segura, ante posibles amenazas.

2.3.1 Tipos de protocolos de seguridad en redes WiFi.

Los tipos de protocolos de seguridad existentes en las redes Wifi hasta la actualidad son:

- Protocolo WEP (Wired Equivalent Privacy).
- Protocolo WPA (Wifi Protect Access).
- Protocolo WPA2.
- Protocolo WPA3

2.3.1.1 Protocolo WEP.

Este protocolo fue desarrollado y aprobado en el año 1999 con el objetivo de proteger la conectividad y la trasmisión de datos en una conexión inalámbrica, posee el mecanismo de encriptación más básico, poco fiable y vulnerable, utiliza el algoritmo de cifrado RC4 (Rivest Cipher 4), para cifrar los datos que se intercambian entre los usuarios y los puntos de acceso. Los equipos o dispositivos que dependen de este tipo de protocolo deben realizar constantemente la actualización de seguridad.

2.3.1.2 Protocolo WPA.

Este protocolo surge en el año 2003 con el objetivo de solucionar los problemas de seguridad de su antecesor, para lograr aquello implementa el estándar de cifrado avanzado (AES, Advanced Encryption Standard), la autenticación de clave pre-compartida (PSK, Pre-Shared Key), el protocolo de integridad de clave temporal (TKIP, Temporal Key Integrity Protocol) para cambiar las claves dinámicamente y la verificación de integridad del mensaje (MIC, Message Integrity Codes) o conocido también como algoritmo de Michael, lo que permite mejorar la seguridad de la comunicación y de los datos transmitidos inalámbricamente entre equipos o dispositivos conectados en un mismo punto de acceso.

2.3.1.3 Protocolo WPA2.

Este protocolo surge en el año 2006 con el objetivo de solucionar los problemas de vulnerabilidad en las redes inalámbricas que surgieron con su antecesor, para ello además de incorporar las características del estándar IEEE 802.11i, reemplaza la verificación MIC o algoritmo de Michael, por el protocolo CCMP (Counter Mode CBC-MAC Protocol), que ayuda al estándar AES para que pueda operar en modos diferentes dependiendo de la gestión, autenticación y seguridad en la transmisión de datos inalámbricamente. Cumpliendo también de esta manera con los requerimientos y normas del estándar de seguridad FIPS 140-2 (Federal Information Processing Standard) del Gobierno de los Estados Unidos, que es un requerimiento para la acreditación de módulos criptográficos.

2.3.1.4 Protocolo WPA3.

Este protocolo surge en el año 2018 con el objetivo de solucionar los problemas de vulnerabilidad, tras aparecer un error de seguridad en el protocolo WPA2, que permitía escuchar el tráfico de los datos de voz entre dispositivos que se comunicaban mediante Wifi, para ello reemplaza la

autenticación PSK por el algoritmo SAE (Simultaneous Authentication of Equals) que evita el descifrado del tráfico de datos, agrega el encriptado OWE (Opportunistic Wireless Encryption) y la tecnología Wifi Easy Connect que simplifica el proceso de conexión entre dispositivos inteligentes con el enrutador (router).

2.4 Equipos que conforman una red Wifi.

Como ya se ha mencionado anteriormente, una red Wifi es una tecnología utilizada para interconectar varios dispositivos entre sí en un área local, sin la necesidad de la utilización del medio físico, los elementos principales para que exista este tipo de comunicación son:

- Punto de Acceso (AP, Access Point).
- Switch.
- Router de borde.

2.4.1 Punto de Acceso (AP).

Es un dispositivo o equipo electrónico cuya función principal es ampliar la red local y así tener una mayor cobertura de esta, con lo cual varios dispositivos finales como laptops, celulares o cualquier equipo conectado a él, puedan compartir información o tener salida a internet si este fuera el caso. Este equipo tiene su propia dirección IP para poder acceder a su configuración y de esta forma poder ser administrado.

Figura 2.6 (a): Ejemplos de puntos de acceso (AP).
Fuente: Elaborada por el Autor con imágenes de los fabricantes.

Figura 2.6 (b): Ejemplo de red ampliada con punto de acceso (AP).
Fuente: Elaborada por el Autor.

2.4.2 Switch.

Es un dispositivo de red también conocido como conmutador, diseñado para establecer interconexiones y resolver problemas de rendimiento en la red debido a anchos de banda pequeños y embotellamientos de tráfico de datos, es decir que su función principal es interconectar varios dispositivos en una misma red física para que así todos puedan intercambiar información entre ellos.

Figura 2.7 (a): Ejemplos de tipos y modelos de Switch.
Fuente: Elaborada por el Autor con imágenes de los fabricantes.

Figura 2.7 (b): Diseño de una red utilizando un Switch.
Fuente: Elaborada por el Autor.

2.4.3 Router de borde.

También conocido como router Gateway, es el equipo encargado de enrutar o encaminar el tráfico interno de una red LAN hacia otra red o hacia internet, este tipo de dispositivo trabaja a nivel de la capa de red del modelo OSI y permite interconectar varias redes entre sí.

Figura 2.8 (a): Ejemplos de tipos y modelos de Routers de borde.
Fuente: Elaborada por el Autor con imágenes de los fabricantes.

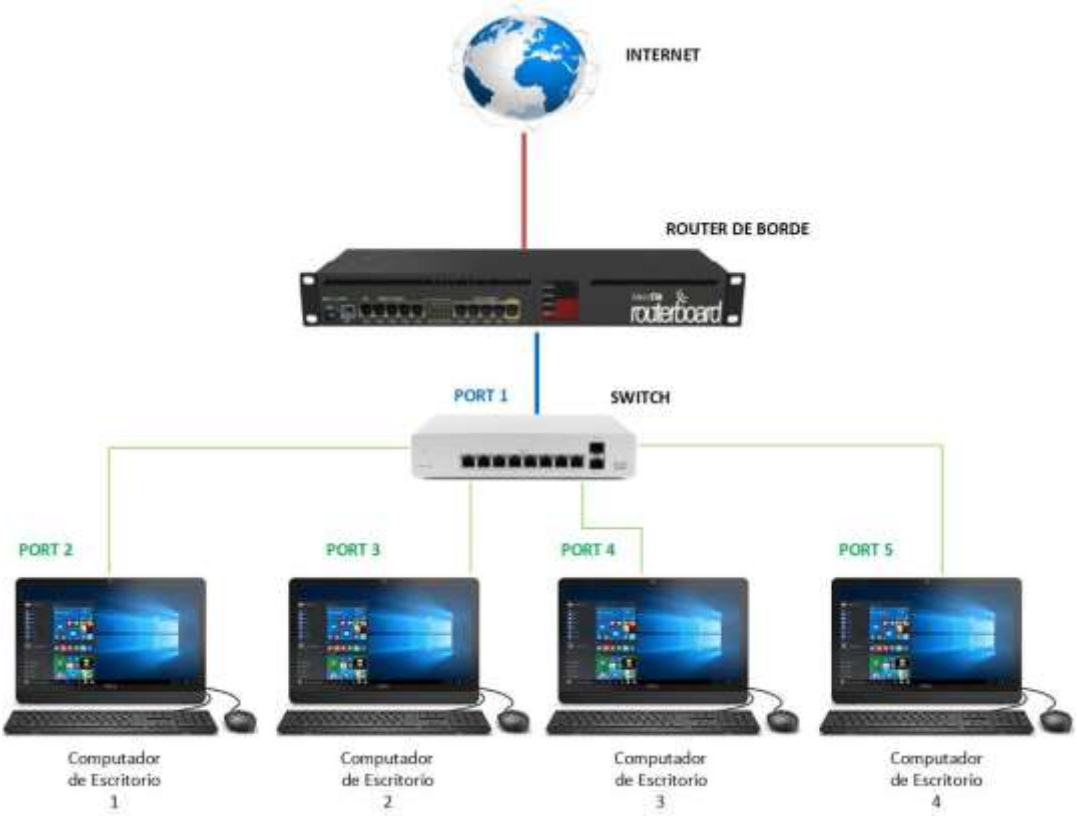


Figura 2.8 (b): Router de borde en una red.
Fuente: Elaborada por el Autor

2.5 Sistema de Seguridad de Circuito Cerrado de Televisión (CCTV).

Un sistema CCTV está compuesto básicamente por una o varias cámaras de seguridad, ya sean cableadas o inalámbricas, que captan imágenes que están dentro de su ángulo de cobertura y son enviadas a través de un medio de transmisión hacia el grabador de video o DVR (Digital Video Recorder) para que posteriormente sean proyectadas por monitores o en otros dispositivos.

Se le llama circuito cerrado de televisión, debido a que sus componentes están directamente conectados entre ellos, creando un circuito de imágenes que no pueden ser vistas por otras personas que estén fuera de esta instalación de componentes. Sin embargo, con el avance tecnológico los sistemas de video vigilancia han ido evolucionando y actualmente pueden ser monitoreados y controlados remotamente desde cualquier

lugar, considerando que dicho sistema de seguridad debe estar conectado a la red global como Internet.

Existen dos tipos de sistemas de CCTV: análogo y basado en IP, donde los primeros utilizan señales continuas en el tiempo de tipo eléctrico que son transportadas en un medio físico entre la cámara y el sistema de grabación, por el contrario, los sistemas basados en IP, que actualmente son los más usados, utilizan señales de tipo digital que son a su vez transmitidas por un medio físico o inalámbrico desde una cámara hacia el sistema de grabación, tomando en consideración que esta transmisión se realiza bajo el protocolo TCP/IP (Transmisson Control Protocol/Internet Protocol) en redes Ethernet

Los componentes principales que forman parte de un sistema CCTV son:

- Grabador de Video Digital o DVR.
- Cámara
- Medio de transmisión
- Monitor

2.5.1 Grabador de Video o DVR.

A principios de la década de los años 50´s, el DVR inicialmente surge como una necesidad de las industrias de Televisión y Seguridad, para grabar y almacenar archivos de video durante el desarrollo y visualización en tiempo real de un determinado evento, que permita un mejor acceso a la información y a la programación de entretenimiento respectivamente.

Posteriormente, en 1951 se inventa la cinta de video grabado, lo cual permitiría el almacenamiento de imágenes en una cinta de video VTR (Video Tape Recorder). En la década de los 60´s, debido a que ya existía la posibilidad de un sistema de grabación de imágenes, este tipo de dispositivo fue incluido en los sistemas CCTV para el almacenamiento, control y monitoreo de lo que transmitían las cámaras de seguridad.

Figura 2.9 (a): Ejemplos de los primeros DVR.
Fuente: www.secureweek.com

Con el pasar de los años la evolución en las características de los DVR irían cambiando y adaptándose a las nuevas tecnologías; desde su capacidad de almacenamiento, formatos de compresión de video, hasta los puertos de conexión de entrada y salida.

Figura 2.9 (b): Ejemplo de DVR.
Fuente: www.abowone.com

Cabe indicar que en el campo de la seguridad la estructura de los DVR fue diseñada para trabajar con cámaras análogas, la conexión entre el equipo y las cámaras era mediante cable coaxial. Posteriormente con la evolución de la tecnología, su estructura mejoraría para trabajar con cámaras digitales o IP.

En la actualidad, existen versiones híbridas de este tipo de dispositivo, es decir que utilizan una combinación de compatibilidad tanto para cámaras análogas como para digítales o IP.

En general, al momento de pensar en realizar un proyecto de CCTV es de vital importancia conocer el entorno en el cual se implementará dicho sistema de seguridad, puesto que esto determinará qué tipo de sistema CCTV se utilizará y a su vez que tipo de DVR se adapta a las necesidades y condiciones económicas. Tomando en cuenta que estos sistemas no siempre son compatibles entre sí, cada sistema requiere de su propio tipo de cámara específico o también se puede optar por un sistema DVR Hibrido. A continuación, se presentan los tipos de DVR:

2.5.1.1 Grabador de video DVR Análogo.

Es utilizado únicamente en sistemas CCTV análogos utilizados para conectar cámaras análogas tipo estándar con resoluciones de no más de 450 y 1000 líneas, que son las encargadas de enviar la señal de video analógica hacia el DVR, donde se procesan y digitalizan la señal para almacenarla en su disco duro. Pueden disponer de 4, 8,16 o 32 canales tipo BNC (Bayonet Neill-Concelman), donde se conectan las cámaras con cable coaxial RG49 o UTP (Unshielded Twisted Pair), sin embargo, para las instalaciones donde se implemente este tipo de cable hay que tomar en cuenta que deben adaptarse en cada uno de sus extremos dispositivos llamados transceptores de video, que permiten adaptar la impedancia que se genera (Figura 2.10).

2.5.1.2 Grabador de Video DVR TVI/CVI/SDI.

Con el pasar de los años y gracias a los avances tecnológicos que se han generado en los sistemas de seguridad de CCTV, se pudo obtener los llamados DVR TVI/CVI/SDI que son DVR que soportan cámaras análogas de tipo entandar y a su vez nos permiten agregar cámaras análogas con protocolos TVI/CVI/SDI, cuyos aspectos físicos son similar al de las cámaras tradicionales; sin embargo la diferencia radica en el tipo de resolución que nos permite alcanzar, es decir que este tipo de cámaras nos permiten tener resoluciones de hasta 2.4 megapíxeles.

Figura 2.10: DVR Analógico y elementos de conexión.
Fuente: Elaborada por el Autor con imágenes de los fabricantes.

Con relación al medio de transmisión que se usa entre las cámaras y el DVR, es prácticamente el mismo que el de un sistema de CCTV análogo y por ende para la implementación de un proyecto de sistema de seguridad se puede aprovechar el cableado existente, ya sea cable coaxial o UTP para la transmisión de los videos, logrando así optimizar los recursos económicos donde se requiera la implementación de un sistema de seguridad de alta resolución.

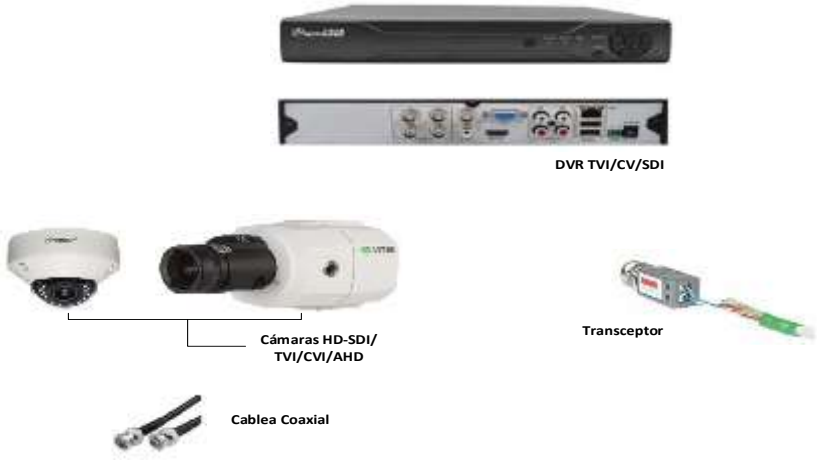


Figura 2.11: DVR TVI/CVI/SDI y elementos de conexión.
Fuente: Elaborada por el Autor con imágenes de los fabricantes.

2.5.1.3 Grabador de video DVR sobre IP.

Este tipo de equipos admiten únicamente la conexión de cámaras IP, logrando de esta forma conjugar en un solo sistema las ventajas de los sistemas análogos y las redes de comunicación IP, debido al uso de cable UTP para su conexión. Debido a que son cámaras diseñadas para la visualización de imágenes en alta resolución, estos DVR soportan altas tasas de compresión, utilizando estándares H.264, MPEG-4 y MJPEG; evitando de esta manera el alto consumo en espacio de almacenamiento y ancho de banda por la información obtenida de cada cámara.

El rendimiento de este equipo se mide en Mbps y requiere de la instalación de un switch de red para que todos los dispositivos que conforman el sistema de video vigilancia digital puedan estar conectados entre sí, o a su vez se requiere de un DVR IP con switch integrado para la comunicación entre las diferentes cámaras que conformen el sistema de seguridad IP.

Figura 2.12: DVR IP y elementos de conexión.
Fuente: Elaborada por el Autor con imágenes de los fabricantes.

2.5.1.4 Grabador de video DVR Híbrido.

Esta clase de equipo es la más completa de los tipos de DVR, en lo que se refiere a los tipos de cámaras que puede admitir debido a la versatilidad de compatibilidad en las características de su estructura. Este equipo admite la conexión tanto de cámaras análogas como de cámaras digitales o IP, por lo que pueden recibir las señales digitales ya codificadas para posteriormente comprimirlas; o en caso de recibir señales análogas realizar la compresión.

Figura 2.13: Sistema CCTV con DVR Híbrido.
Fuente: Elaborada por el Autor con imágenes de los fabricantes.

2.5.2 Cámara de Video Vigilancia.

A principio de la década de los 40´s, las cámaras de video vigilancia se originan como un elemento de seguridad en el ámbito militar y surgen con la finalidad de controlar y monitorizar el flujo de personas y objetos.

Las primeras cámaras de video vigilancia que formaban parte de la estructura de un circuito CCTV fueron análogas y se conectaban a través de cable coaxial, trasmitían imágenes de video en blanco y negro, ayudando de esta manera a la observación de misiles y ataques en la preparación militar.

Figura 2.14 (a): Ejemplo de primeras cámaras de video vigilancia.
Fuentes: www.racalarm.com / www.seguridadviaip.com.ar

Estas primeras cámaras de video vigilancia transmitían una señal sinusoidal entre +0,5 y -0.5 voltios y debido a que el cable coaxial es un medio de transmisión muy susceptible a interferencias, originaban que las imágenes visualizadas sean de muy baja calidad.

A principios de los 90´s con el avance de nuevas tecnologías se desarrollaría por parte de la empresa AXIS la primera cámara de video vigilancia IP Neteye 200, permitiendo de esta manera el cambio de tecnología análoga a digital.

Figura 2.14 (b): Cámara de video vigilancia IP Neteye 200.
Fuente: www.axis.com

Con la tecnología IP se aprovecha la conexión a internet, para que mediante las redes de telecomunicaciones se logre tener acceso desde cualquier ubicación en el mundo a los sistemas de CCTV que tengan este tipo de infraestructura.
Las cámaras de video vigilancia se clasifican en:

- Cámaras de Video vigilancia Análogas.
- Cámaras de Video vigilancia Digítales IP.

2.5.2.1 Cámaras de Video vigilancia Análogas.

Este tipo de cámaras necesitan una conexión a través de cable coaxial o UTP con adaptadores de impedancia, también llamados video balun para llevar la señal de video al DVR, debido a que generalmente poseen una salida con impedancia de 75 ohm.

Figura 2.15: Ejemplo de cámaras de video vigilancia análogas.
Fuente: Elaborada por el Autor con imágenes de los fabricantes.

Ventajas. - las ventajas de estas cámaras son las siguientes:

- Son compatibles con cualquier tipo y modelo de DVR.
- Transmiten sin compresión videos al DVR, lo que permite ser monitoreado en vivo sin el retraso que genera la compresión.

Desventajas. - sus desventajas son las siguientes:

- Debido al cableado estructurado que utilizan, necesitan convertidores para transmitir video, datos y alimentación eléctrica.
- No permiten el acceso al monitoreo desde dispositivos móviles.
- Tienen un índice de seguridad muy bajo, ya que pueden ser interceptadas o visualizadas por cualquiera que tenga acceso a la infraestructura del cableado.

2.5.2.2 Cámara de Video Vigilancia Digitales IP.

Es también conocida como cámara de red, son diseñadas para enviar señales de video y audio utilizando internet a través de un explorador web o un Hub o Switch dentro de una LAN o una red externa.

Estas cámaras pueden clasificarse en:

- Con puerto Ethernet.
- Con puerto Wifi.

Cámaras de Video Vigilancia Digital IP con puerto Ethernet RJ45. Son diseñadas para utilizar cableado UTP como medio de transmisión para enviar las señales de imagen, audio y video a través de su puerto Ethernet RJ45 hacia el DVR o NVR (Network Video Recorder).

Figura 2.16: Cámara Digital IP con puerto Ethernet RJ45.
Fuente: Elaborada por el Autor con imágenes de los fabricantes.

Cámaras de Video Vigilancia Digital IP con puerto Wifi. Son diseñadas para utilizar el aire como medio de transmisión para enviar inalámbricamente las señales de imagen, audio y video, a través de su puerto Wifi hacia el DVR o NVR.

Figura 2.17: Cámara Digital IP con puerto Wifi.
Fuente: Elaborada por el Autor con imágenes de los fabricantes.

Ventajas:

- Visualizar imágenes y videos en tiempo real simultáneamente desde diferentes ubicaciones y en cualquier parte del mundo.
- Manipular a través de software o desde un navegador o explorador web, el movimiento de las cámaras.
- Grabar y almacenar la información en cualquier computador con conexión a internet o a una red local.
- Monitorear la seguridad desde dispositivos móviles.
- El cableado estructurado que se utiliza para este tipo de cámaras tiene la capacidad de transmitir y proveer alimentación eléctrica (PoE, Power over Ethernet), video, voz y datos.
- Eliminan el cableado estructurado y ahorran costos, sobre todo cuando las cámaras tienen tecnología Wifi.

Desventajas.

- La calidad para poder visualizar imágenes y video depende de la velocidad de la conexión a internet.
- Algunos modelos de cámaras IP son incompatibles con ciertos sistemas operativos.
- No se puede cambiar el lente de la cámara para poder obtener una mejor resolución.

2.5.3 Medio de transmisión.

Los medios de transmisión son los diferentes caminos por los cuales se envía la comunicación o transmisión de datos entre dos o más dispositivos, es el soporte físico por medio del cual emisor y receptor se comunican en un sistema de transferencia de información, los cuales disponen de características técnicas que van a predominar a la hora de la transmisión de la señal, puesto que de ellos va a depender su velocidad, ancho de banda y distancia de conexión entre dispositivos.

Tomando en consideración la forma en la cual se va a transmitir la señal en el medio, existen dos tipos de medios de transmisión: medios guiados o por cable y no guiados o inalámbricos.

2.5.3.1 Medio de transmisión guiado.

Son aquellos que guían las ondas electromagnéticas a través de un camino físico como el cable y entre los más utilizados en telecomunicaciones para la conexión de dispositivos se tiene el coaxial, UTP y fibra óptica.

Cable coaxial. es cilíndrico y está constituido principalmente en su parte central por un alambre de cobre, recubierto por un material aislante y a su vez éste se encuentra recubierto por una malla cilíndrica de cobre. Los elementos que forman la estructura del cable coaxial permiten que este medio físico guiado alcance un gran ancho de banda, dependiendo de la longitud del cable puede alcanzar velocidades de 10 Mbps.

Las ventajas y desventajas de la utilización del cable coaxial son:

- Permite alcanzar mayor distancia que lo que admite el cable UTP o STP (Shielded Twisted Pair), debido a que puede alcanzar los 10 kilómetros.
- Su implementación es de bajo costo y fácil instalación.
- Soporta aplicaciones de voz, pero no en tiempo real.
- El ancho de banda máximo que puede soportar es de 10 Mbps.

- Debido a su estructura y funcionamiento, está expuesto a interferencias electromagnéticas y a ruidos eléctricos.
- A partir de que va creciendo su longitud va disminuyendo considerablemente su ancho de banda.

Figura 2.18: Cable Coaxial y cámara con cable coaxial.
Fuente: Elaborada por el Autor con imágenes de los fabricantes.

Cable par trenzado: es comúnmente utilizado en las comunicaciones telefónicas y conexiones de redes Ethernet más modernas, el más utilizado es el UTP, constituido por cuatro pares de hilos conductores de cobre cruzados entre sí, con el objetivo de lograr reducir las perturbaciones electromagnéticas producidas en un canal de comunicación o atenuación. Estos pares de hilos permiten enviar señales de video, datos, audio o corriente a través del mismo cable.

Los cables de pares trenzados sin blindaje son UTP y con blindaje STP.

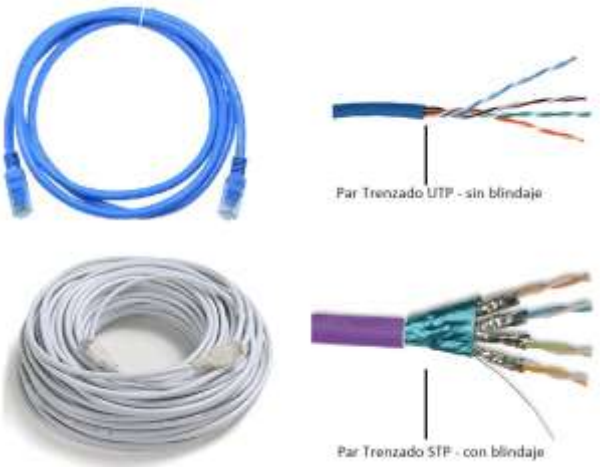


Figura 2.19: Cables de pares trenzados UTP y STP.
Fuente: Elaborada por el Autor.

Entre las ventajas y desventajas de utilizar cable UTP se tiene:

- Bajo costo en su construcción.
- Alto número de estaciones de trabajo por segmento.
- Facilidad para el rendimiento y la solución de problemas.
- Puede estar previamente cableado en un lugar.
- Altas tasas de error a altas velocidades.
- Ancho de banda limitado.
- Baja inmunidad al ruido.
- Baja inmunidad al efecto crosstalk (diafonía).
- Distancia limitada (100 metros por segmento).

Cable de fibra óptica.

La fibra óptica se ha convertido en el medio de transmisión más utilizado en la actualidad, reemplazando así a los medios de transmisión más comunes como el cable coaxial y el UTP en la mayoría de los campos en los que se los utiliza, esto debido a su alto rendimiento y calidad de transmisión de datos. La fibra óptica está constituida por uno o más hilos muy finos de vidrio con propiedades ópticas, por donde se transmiten los datos a través de pulsos de luz. Este medio de transmisión es aplicado con frecuencia en redes de telecomunicaciones debido a que su estructura le permite ser inmune a las interferencias electromagnéticas, así como la transmisión de datos a altas velocidades en grandes distancias.

Figura 2.20: Cables de fibra óptica de 1 y 6 hilos de fibra.
Fuente: Elaborada por el Autor.

Entre las ventajas y desventajas de utilizar fibra óptica en una transmisión de datos, se tiene:

- Una banda de paso muy ancha permite flujos de datos muy elevados (del orden de GHz).
- Inmunidad total a las perturbaciones de origen electromagnético, implica una calidad de transmisión muy buena, la señal es inmune a las tormentas.
- Gran seguridad, la intrusión en la fibra óptica es fácilmente detectable por el debilitamiento de la energía luminosa en la recepción, no irradia nada, es particularmente interesante para aplicaciones que requieren alto nivel de confidencialidad.
- No produce interferencias.
- Insensibilidad a los parásitos, lo que es una propiedad principalmente utilizada en los medios industriales fuertemente perturbados (por ejemplo, en los túneles del metro). Esta propiedad también permite la coexistencia por los mismos conductos de cables ópticos no metálicos con los cables de energía eléctrica.
- Atenuación muy pequeña independiente de la frecuencia, lo que permite salvar distancias importantes sin elementos activos intermedios.
- Gran resistencia mecánica debido a su resistencia a la tracción, facilitando su instalación.
- Resistencia al calor, frío, corrosión.
- Facilidad para localizar los cortes gracias a un proceso basado en la telemetría, lo que permite detectar rápidamente el lugar y posterior reparación de la avería, simplificando la labor de mantenimiento.
- Alta fragilidad de las fibras.
- Necesidad de usar transmisores y receptores más caros.
- Los empalmes entre fibras son difíciles de realizar, especialmente en el campo, lo que dificulta las reparaciones en caso de ruptura del cable.
- No puede transmitir electricidad para alimentar repetidores intermedios.
- No existen memorias ópticas.

2.5.3.2 Medios de Transmisión No Guiado.

Estos medios cada vez han obtenido mayor acogida en el campo de las comunicaciones, esto gracias a su gran versatilidad a la hora de su implementación en lugares donde instalación de cables es muy costosa o prácticamente nula, por ende, estos medios inalámbricos no necesitan ningún tipo de medio físico para la transmisión de señales, se propagan libremente a través del aire o el vacío, como por ejemplo señales de radio, microondas o satelitales.

En este tipo de medio de transmisión, la comunicación se lleva a cabo a través de dos antenas que son encargadas de emitir y recibir ondas electromagnéticas entre sí, tomando en consideración que estas ondas electromagnéticas pueden ser irradiadas por la antena emisora de manera direccional u omnidireccional, dependiendo del tipo de dispositivo que se vaya a utilizar en el medio. Las distancias que se pueden alcanzar dependen de la potencia de salida del transmisor y la ganancia de la antena.

Figura 2.21: Ejemplo de medio de transmisión no guiado.
Fuente: Elaborada por el Autor.

2.5.4 Monitor.

Los sistemas de video vigilancia CCTV en un principio hacían referencia a su nombre de circuito cerrado de televisión, es decir que, la visualización de las imágenes captadas por las cámaras de seguridad, solo le era

permitido a los monitores que se encontraban dentro de dicho circuito de seguridad, es decir que ningún otro monitor, ni mucho menos otro tipo de dispositivo que no esté dentro del sistema de CCTV podía visualizar absolutamente nada. Gracias a los avances tecnológicos que se han generado con el transcurso de los años, en la actualidad el modo de visualización de las cámaras de seguridad de un circuito cerrado puede ser visto desde varios dispositivos a la vez y desde cualquier parte del mundo, esto siempre y cuando el DVR se encuentre conectado a Internet.

Entre los principales medios que existen en la actualidad para la visualización de las cámaras de seguridad de un sistema de CCTV, se tiene:

- Monitor conectado directo al DVR: Como ya se ha mencionado, el monitor es uno de los elementos que conforman un sistema de circuito cerrado de CCTV, el cual conectado directamente al DVR permite la visualización directa de las cámaras que conforman dicho circuito de seguridad.

Figura 2.22: Ejemplos de Monitores para un sistema CCTV.
Fuente: Elaborada por el Autor.

- Dispositivos móviles: Gracias al crecimiento tecnológico de los últimos años, en la actualidad existen un sin número de aplicaciones para dispositivos móviles que permiten visualizar o realizar el monitoreo de las cámaras de seguridad de un circuito cerrado de CCTV, esto siempre y

cuando el dispositivo móvil, así como el sistema de seguridad de CCTV se encuentren conectados a internet.

Figura 2.23: Ejemplos de Dispositivos Móviles.
Fuente: Elaborada por el Autor.

- Computadora externa: Así mismo, en la actualidad existen varios tipos de software de diferentes fabricantes de cámaras de seguridad, que pueden ser descargados e instalados en un computador, para poder realizar la visualización o el monitoreo de las cámaras de seguridad de un circuito cerrado CCTV desde cualquier parte del mundo.

Figura 2.24: Ejemplos de visualización de CCTV en computadora externa.
Fuente: Elaborada por el Autor.

Capítulo 3: Diseño del sistema de seguridad CCTV mediante una red Wifi.

Para el diseño de un sistema de seguridad CCTV por medio de una red inalámbrica, lo primero que se debe tomar en cuenta es la ubicación estratégica de cada cámara de seguridad, lo que va a depender básicamente de la infraestructura del edificio y los lugares o áreas que se pretende dar cobertura con cada una de ellas, luego de lo cual se procede al diseño de la red inalámbrica para la conexión de los diferentes dispositivos del sistema CCTV, la cual sería el medio no guiado de transmisión.

3.1 Diseño de un sistema CCTV.

Para el diseño del sistema CCTV, lo primero que debe tomarse en cuenta es la edificación donde se lo va a implementar, con lo cual se determina el tipo de cámaras más adecuadas y el medio de comunicación a utilizarse para la transmisión de información entre los dispositivos del sistema.

3.1.1 Infraestructura o lugar de implementación del Sistema CCTV.

Este proyecto fue pensado para el diseño de seguridad CCTV para las instalaciones de la Gobernación de la Provincia de El Oro, en la ciudad de Machala. Esta edificación se encuentra constituida por 6 pisos, de los cuales solo 3 pisos son de uso exclusivo de la Institución y en donde funcionan las diferentes unidades administrativas.

La infraestructura de los diferentes departamentos o unidades que conforman la Gobernación se encuentran distribuidos de la siguiente manera:

Piso 2:

- Unidad de Tecnologías de la Información y Comunicación
- Unidad de Guardalmacén.

- Comisaría I Nacional de Policía del Cantón Machala.
- Intendencia General de Policía de la Provincia de El Oro.

Piso 3:

- Unidad de Planificación y Gestión Estratégica.
- Unidad de Talento Humano.
- Compras Públicas.
- Dirección Administrativa Financiera.

Piso 4:

- Unidad de Comunicación Social.
- Secretaria General.
- Jefatura Política del Cantón Machala.
- Salón de Integración “Dra. Patricia Montero Armijos”.
- Despacho del Gobernador.
- Asesoría Jurídica.
- Unidad de Transporte

Teniendo así la distribución gráfica y física de las Unidades y Oficinas que funcionan en cada piso de la Institución (Figuras 3.1, 3.2 y 3.3).

Cabe recalcar que el edificio donde actualmente se encuentra instalada la Gobernación de la provincia de El Oro en la ciudad de Machala fue creado aproximadamente en el año 1970, hasta la actualidad no ha sido modificado o mejorado en sus instalaciones físicas, es decir que su obra civil interna y externa aún se mantiene con el transcurso de los años, lo que implica un sistema de ductos para el cableado estructurado de la red interna totalmente saturado, esto prácticamente imposibilita el diseño de nuevas redes de datos por un medio cableado.

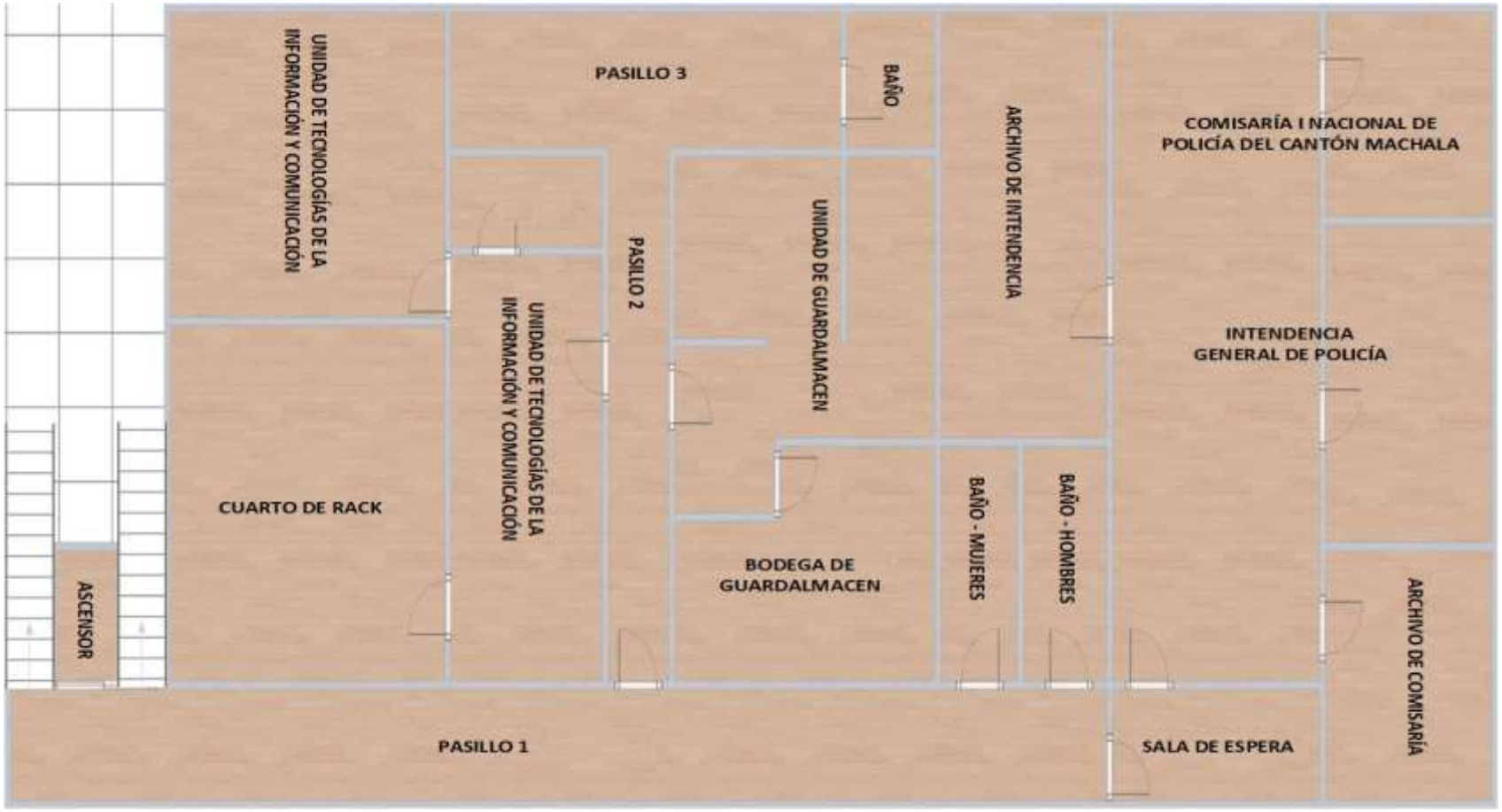


Figura 3.1: Distribución gráfica de las diferentes Unidades que funcionan en el Piso 2.
Fuente: El Autor.

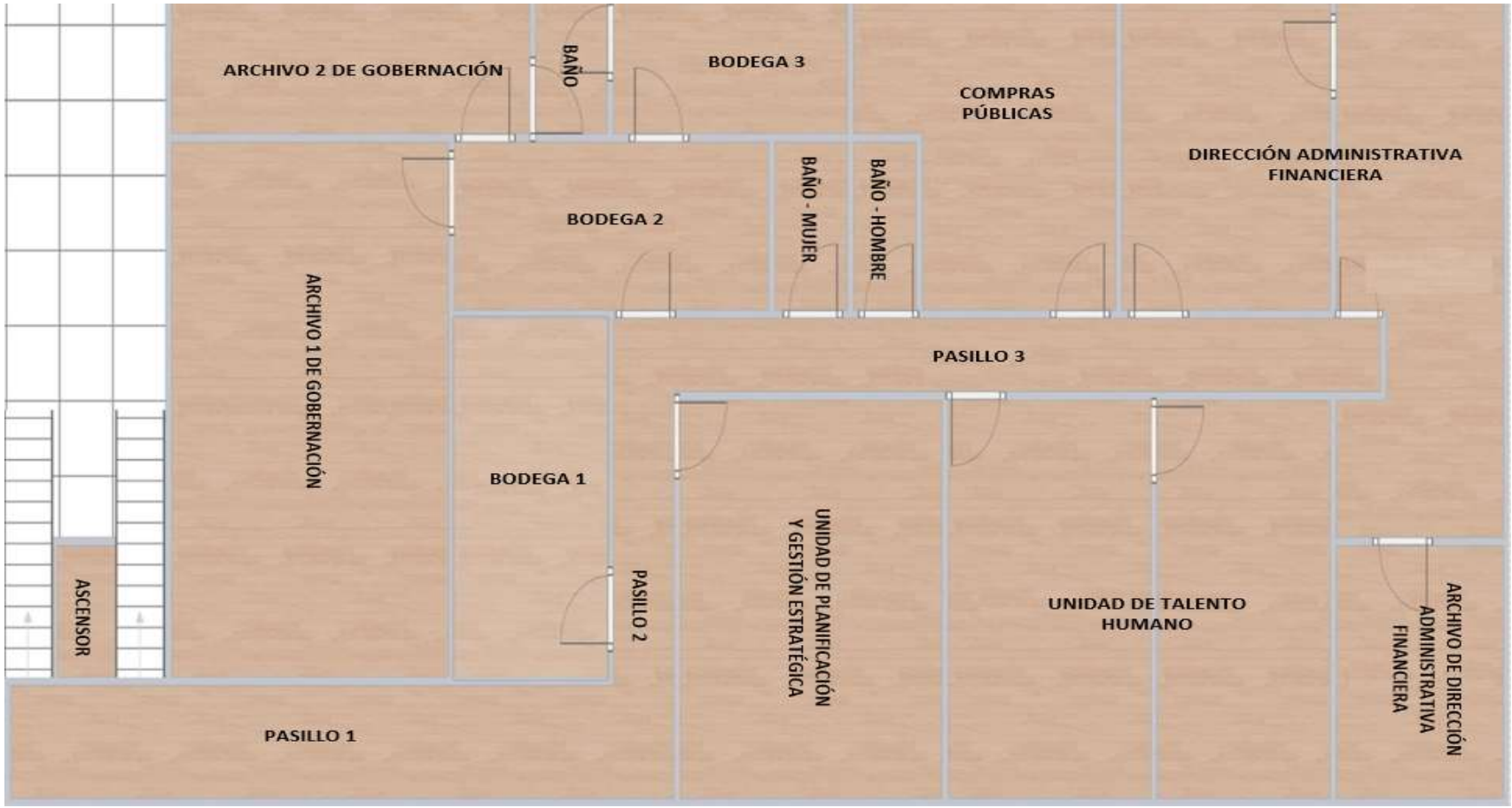


Figura 3.2: Distribución gráfica de las diferentes Unidades que funcionan en el Piso 3.
Fuente: El Autor.

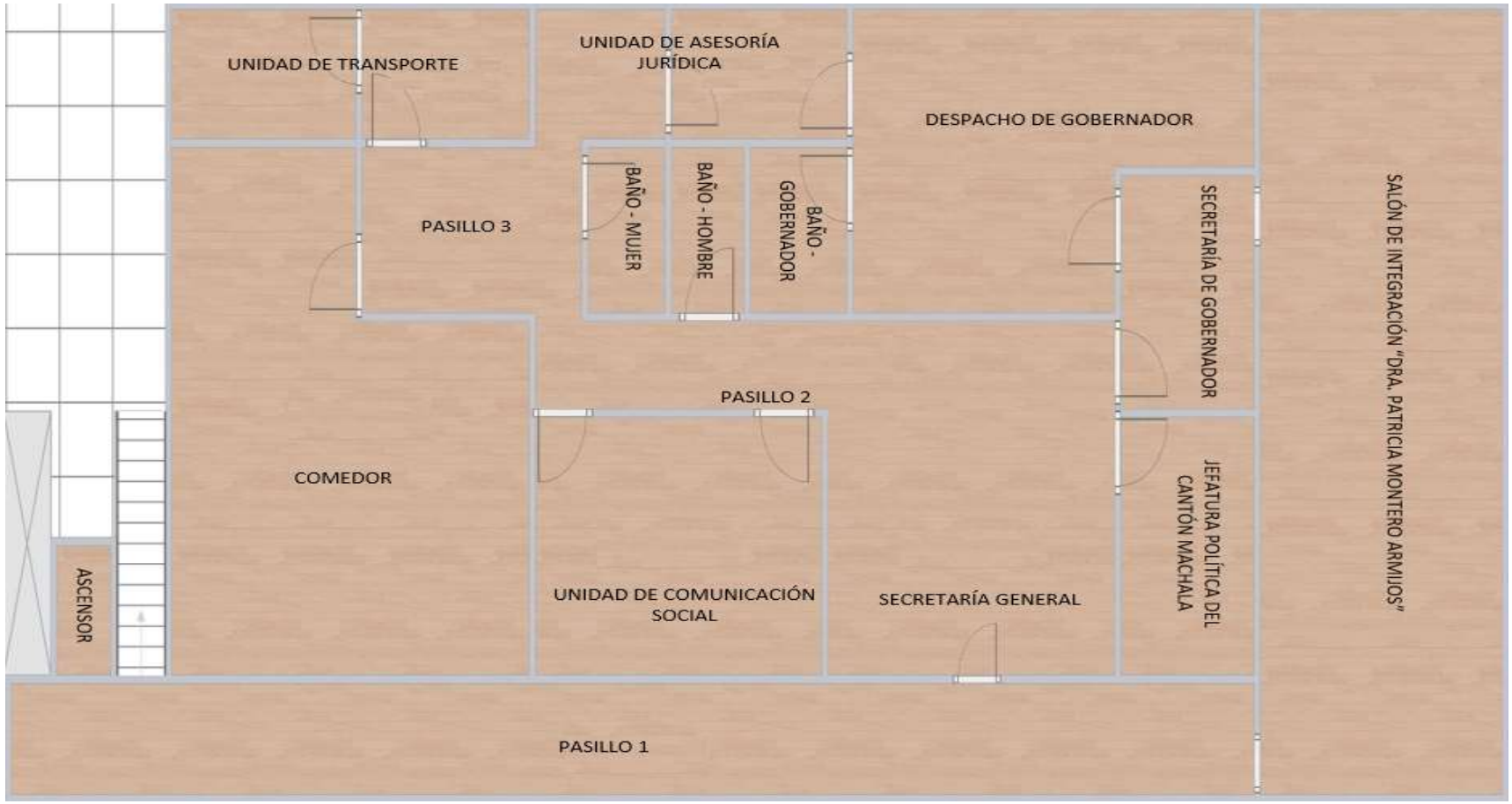


Figura 3.3: Distribución gráfica de las diferentes Unidades que funcionan en el Piso 4.
Fuente: El Autor.

Una vez que se conoce la infraestructura del edificio, se determina qué sistema de seguridad es el más indicado para su implementación. En este caso, se plantea un proyecto de CCTV digital por IP a través de una red inalámbrica, debido a que como ya se ha indicado no es posible realizar un nuevo cableado estructurado o reutilizar el que actualmente existe en las instalaciones de la Gobernación de la Provincia de El Oro.

3.1.2 Diseño del sistema de seguridad CCTV digital sobre IP.

Los sistemas de seguridad digital basados en IP son aquellos que utilizan señales digitales que son transmitidas por un medio físico o inalámbrico desde una cámara hacia el sistema de grabación, esta transmisión se realiza bajo el protocolo TCP/IP en redes Ethernet. Por lo cual, y debido a la infraestructura física del edificio de la gobernación de la provincia de El Oro en la ciudad de Machala, se determina que el sistema de seguridad digital sobre IP con cámaras inalámbricas es el más adecuado para la implementación de dicho proyecto, considerando que el medio para la comunicación entre dispositivos del sistema de CCTV es la conexión inalámbrica.

Gracias a un previo análisis en conjunto con personal encargado de seguridad, personal de redes y administrativo de la Gobernación de la provincia de El Oro, se determina los lugares con mayor vulnerabilidad para que puedan ser monitoreados las 24 horas del día por medio de cámaras de seguridad. Con lo cual el diagrama del sistema de seguridad de CCTV para las áreas de cobertura quedaría conformado de la siguiente manera:

3.1.2.1 Diseño del sistema de seguridad en el Piso 2.

La figura 3.4 muestra la distribución de las cámaras en el piso 2 del edificio de la Gobernación de El Oro, como se puede apreciar se necesitan 5 cámaras de seguridad para cubrir en su totalidad los puntos más

vulnerables del piso en mención. Cabe recalcar que en este piso se encuentra ubicado el cuarto de redes principal, donde se encuentran los equipos principales de red y es lugar adecuado para instalar el DVR para el almacenamiento de las grabaciones y de donde partirán las conexiones principales hacia cada una de las cámaras.

- Unidad de Tecnologías de la Información y Comunicación.
- Unidad de Guardalmacén.
- Comisaría I Nacional de Policía del Cantón Machala.
- Intendencia General de Policía de la Provincia de El Oro.

3.1.2.2 Diseño del sistema de seguridad en el Piso 3.

La figura 3.5 muestra la distribución de las cámaras en el piso 3 del edificio de la Gobernación de El Oro, como se puede apreciar se necesitan 6 cámaras de seguridad para cubrir los puntos más vulnerables del piso en mención.

- Unidad de Planificación y Gestión Estratégica.
- Unidad de Talento Humano.
- Compras Públicas.
- Dirección Administrativa Financiera.

3.1.2.3 Diseño del sistema de seguridad en el Piso 4.

La figura 3.6 muestra la distribución de las cámaras en el piso 4 del edificio de la Gobernación de El Oro, como se puede apreciar se necesitan 5 cámaras de seguridad para cubrir los puntos más vulnerables del piso en mención.

- Unidad de Comunicación Social.
- Secretaria General.
- Jefatura Política del Cantón Machala.
- Salón de Integración “Dra. Patricia Montero Armijos”.
- Despacho de Gobernador.
- Asesoría Jurídica.
- Unidad de Transporte

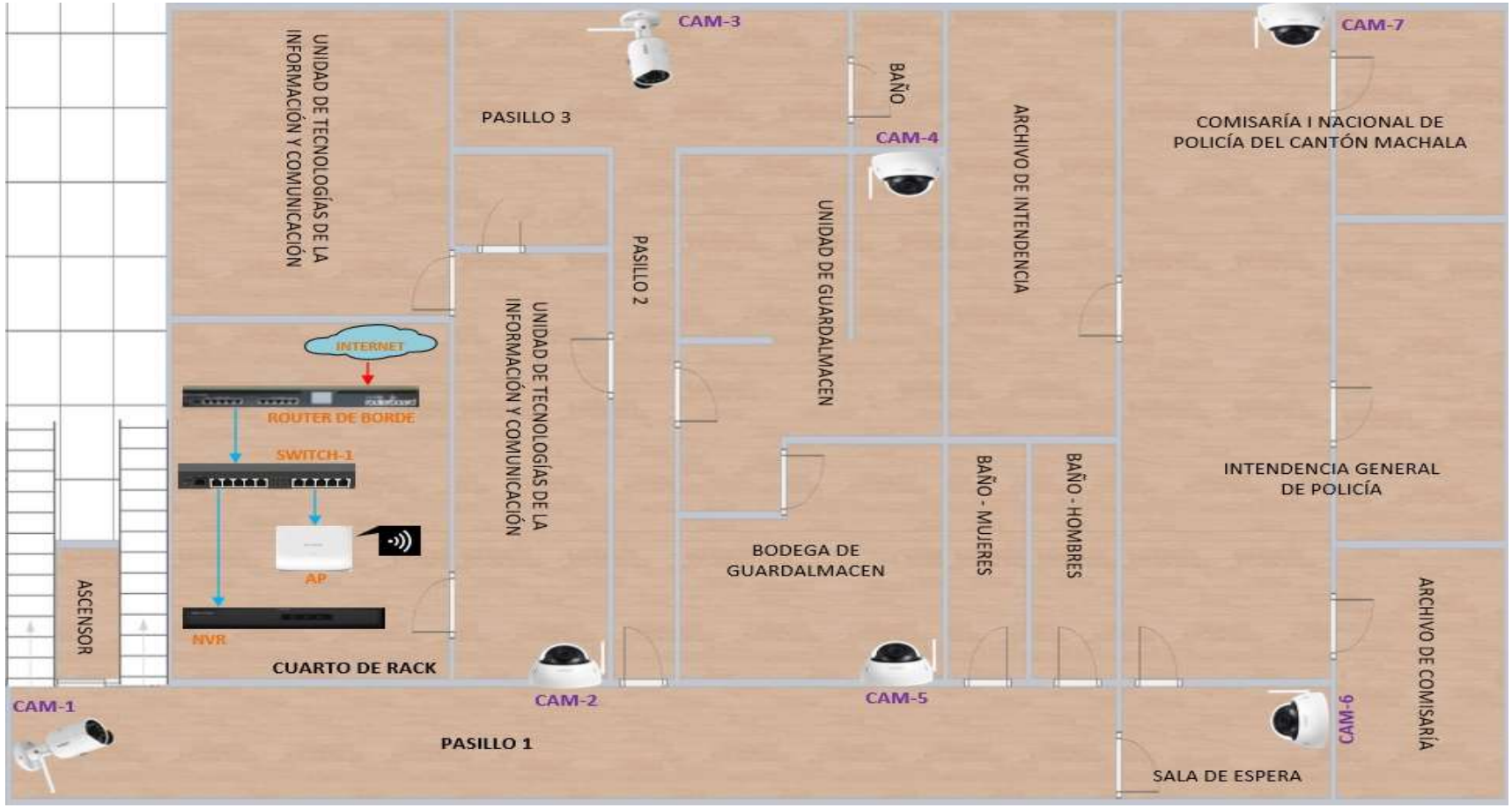


Figura 3.4: Distribución de las cámaras en el Piso 2.
Fuente: El Autor.

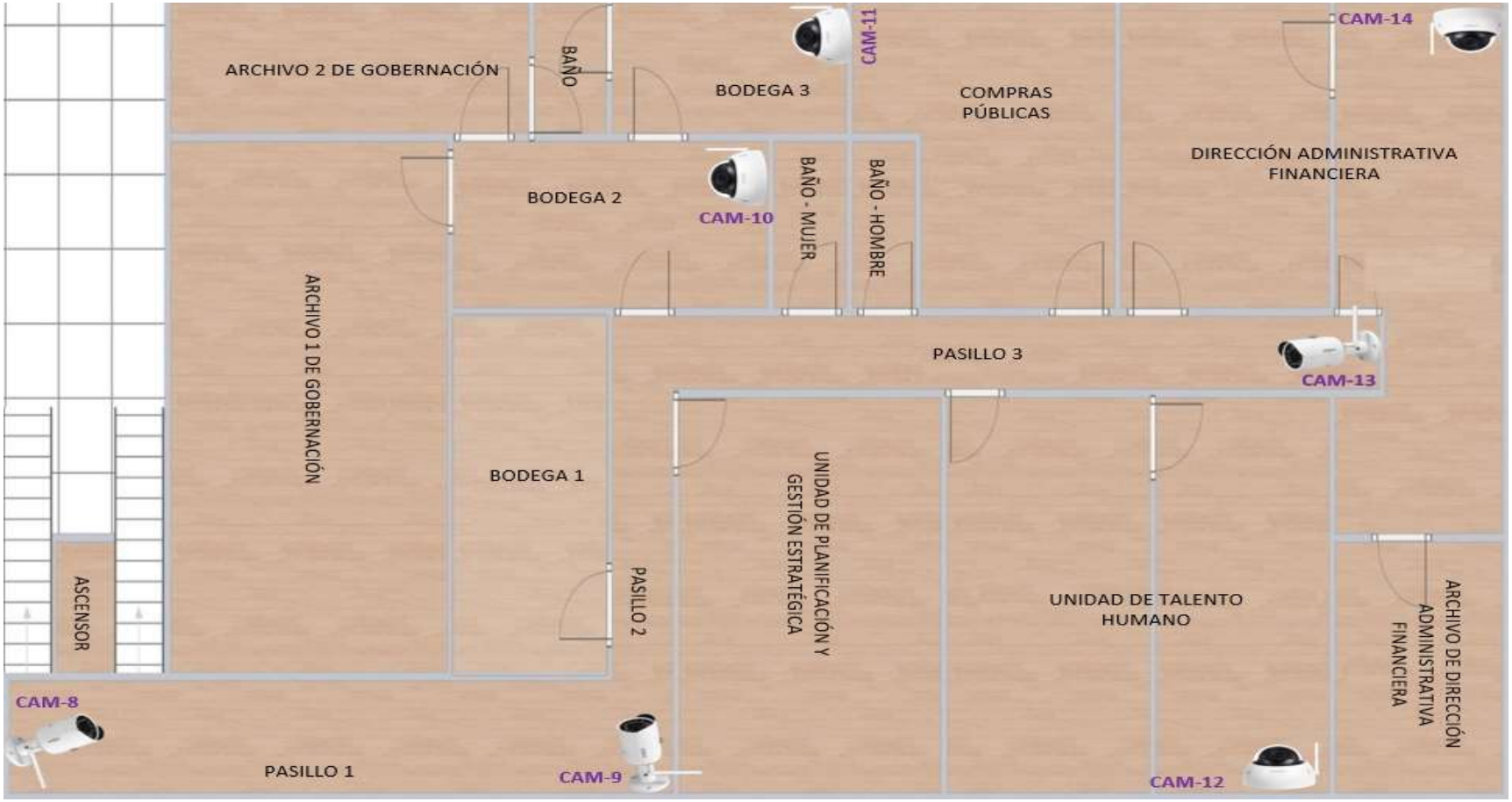


Figura 3.5: Distribución de las cámaras en el Piso 3.
Fuente: El Autor

Figura 3.6: Distribución de las cámaras en el Piso 4.
Fuente: El Autor

3.1.3 Equipos a utilizar en el diseño del sistema CCTV.

De acuerdo con la distribución de las cámaras en cada uno de los pisos donde funciona la Institución, se determina que para la implementación de este proyecto se necesitan 20 cámaras de video vigilancia digital IP con puerto Wifi de seguridad para la cobertura de áreas y puntos más vulnerables del edificio de la Gobernación.

Para la implementación de este proyecto se han escogido los siguientes modelos de cámaras de video vigilancia con puerto Wifi, las mismas que varían según el área de cobertura en las cuales van a ser utilizadas.

- Cámara con puerto Wifi tipo Domo IPC-HDBW1235E-W.
- Cámara con puerto Wifi tipo Bala IPC-HFW2325S-W.

Figura 3.7: Cámaras de video vigilancia con puerto Wifi a utilizar en el diseño del sistema CCTV.
Fuente: www.dahua.com

Así mismo, se ha considerado el siguiente modelo de NVR como dispositivo de almacenamiento de los videos de seguridad.

- Video Grabador NVR5816/5832/5864-16P-4KS2E.

Figura 3.8: Video grabadora en red NVR a utilizar en el diseño del sistema CCTV.
Fuente: www.dahua.com

3.1.3.1 Cámara de video vigilancia IPC-HDBW1235E-W.

Es una cámara tipo Mini-Domo con un lente fijo de 3.6 mm, soporta Micro SD, una resolución de 2 megapíxeles y conexión inalámbrica. Entre las características principales de este tipo de cámara, se tiene:

- **Easy4ip:** aplicación web que permite a través de internet y sin asignar una dirección IP fija, el acceso en tiempo real para visualizar lo que sucede en las áreas donde se encuentran instalados los dispositivos, mediante dispositivos móviles o a través de la web. Permite el almacenamiento en la nube de las grabaciones de video que se generan diariamente, además de ser guardadas en el equipo local.
- **True Day/Night:** permite a través de espectros infrarrojos (IR) la visualización de imágenes de color durante el día y monocromáticas durante la noche, a medida que el área oscurece.
- **IR Inteligente:** permite por medio de IR y del ajuste de la intensidad de los LED infrarrojos integrados en la cámara, capturar y mejorar imágenes que se encuentran detalladas con poca luz u oscuridad total dependiendo de la distancia del objeto, hasta 30 metros.
- **Interoperabilidad:** aseguran la interoperabilidad a nivel de red entre los diferentes productos que existen en el mercado, independientemente del fabricante, debido a que cumplen con las especificaciones del protocolo de interfaz de video de red abierta fórum ONVIF (Open Network Video Interface Forum).

A continuación, se presenta la tabla 3.1 con las especificaciones técnicas más importantes de la cámara IPC-HDBW1235E-W.

Tabla 3.1: Especificaciones técnicas más importantes de la cámara IPC-HDBW1235E-W.

CÁMARA	
Sensor de Imagen:	CMOS progresivo de 1 / 2,9 "y 3 megapíxeles.
Pixeles Efectivos:	1920(H) x 1080(V).
RAM/ROM	256MB / 16MB.
Sistema de Escaneo:	Progresivo.
Iluminación Mínima:	0.1 Lux / F2.0 (Color), 0 Lux / F2.0 (IR on)
Relación S/N:	Más de 50dB.
Distancia IR:	Distancia hasta 30 metros.
	Auto.

Control de encendido/apagado por infrarrojos:	Manual.	
LED´s de Infrarrojos:	24.	
LENTE		
Tipo de Lente:	Fija.	
Tipo de Montaje:	Fijo	
Longitud Focal:	3.6 mm	
Abertura Máxima:	F2.0 / F2.0	
Campo de Visión:	83°(H), 44°(V), 98°(D)	
Control de Enfoque:	Fijo.	
RED		
Ethernet:	RJ-45 (10/100Base-T)	
Wi-fi	WiFi (IEEE802.11b/g/n), 50m en campo abierto.	
Protocolos:	HTTP-TCP-ARP-RTSP-RTP-UDP-SMTP-FTP DHCP-DNS-DDNS-PPPOE-IPv4/v6-QoS-UPnP-NTP	
Interoperabilidad:	ONVIF – PSIA – CGI.	
Método de transmisión:	Unicast – Multicast.	
Acceso Máximo de Usuarios:	10 usuarios - 20 usuarios	
Almacenamiento Perimetral:	NAS (almacenamiento conectado a la red), PC local al instante Grabación de hasta 128GB	
Visor Web:	IE – Chrome – Firefox – Safari.	
Administración de Software:	Smart PSS – DSS - Easy4ip.	
Teléfono Inteligente:	iPhone – iPad - Teléfonos Android	
VIDEO		
Compresión:	H.265 - H.264H - MJPEG (Sub Stream)	
Capacidad de Transmisión:	2 Streams	
Resolución:	1080P (1920×1080) 1.3M (1280×960) 720P (1280×720)	D1 (704×576/704×480) VGA (640×480) CIF (352×288/352×240)
Cuadros por Segundo:	Transmisión principal: 1080P (1 ~ 25 / 30fps) Transmisión secundaria: D1 (1 ~ 25 / 30fps)	
Control de Tasa de Bits:	CBR / VBR	
Tasa de Bits:	H.265: 12K ~ 6400Kbps H.264: 32K ~ 10240Kbps	
Día/Noche:	Auto(ICR) - Color - B/W	
Modo BLC:	BLC - HLC – DWDR.	
Balance de Blancos:	Auto - Natural - Street Lamp - Outdoor – Manual	
Ganar Control:	Auto / Manual	
Reducción de Ruido:	3D DNR	
Detección de Movimiento:	Apagado / Encendido (4 zonas, rectángulo)	
Región de Interés:	Apagado / Encendido (4 zonas)	
Imagen Electrónica:	Sí.	
IR Inteligente:	Sí.	
Zoom Digital:	16x	
ELECTRICO		
Fuente de Alimentación:	DC12V	
Consumo de Energía:	< 6.5 W	

Fuente: Elaborada por el Autor

3.1.3.2 Cámara de video vigilancia IPC-HFW2325S-W.

Es una cámara tipo Mini-Bellet con un lente que permite trabajar en 2.8mm y 3.6mm, soporta Micro SD y una resolución de 3 megapíxeles y conexión inalámbrica. Entre las características principales de este tipo cámara, se tiene:

- **Image flip:** permite rotar la imagen capturada por la cámara de video vigilancia y rotarla hasta 180 grados, logrando de esta manera mejorar la optimización de video.
- **True Day/Night:** permite a través de IR la visualización de imágenes de color durante el día y monocromáticas durante la noche, a medida que el área oscurece.
- **IR Inteligente:** permite por medio IR y del ajuste de la intensidad de los LED infrarrojos integrados en la cámara, capturar y mejorar imágenes que se encuentran detalladas con poca luz u oscuridad total dependiendo de la distancia del objeto, hasta 30 metros.
- **Interoperabilidad:** asegura la interoperabilidad a nivel de red entre los diferentes productos del mercado, independientemente del fabricante, debido a que cumplen con las especificaciones del protocolo ONVIF.

En la tabla 3.2 se observan las especificaciones técnicas más importantes de la cámara IPC-HFW2325S-W.

Tabla 3.2: Especificaciones técnicas más importantes de la cámara IPC-HFW2325S-W.

CÁMARA	
Sensor de Imagen:	CMOS progresivo de 1/3” y 3 megapíxeles
Pixeles Efectivos:	2304(H) x1536(V
RAM/ROM:	256MB/16MB
Sistema de Escaneo:	Progresivo.
Iluminación Mínima:	0.1Lux / F2.0 (Color).
	0Lux / F2.0 (IR encendido).
Relación S/N:	Más de 50dB.
Distancia IR:	Distancia hasta 30 metros.
Control de encendido / apagado por infrarrojos	Auto.
	Manual.
IR LED:	24
LENTE	
Tipo de Lente:	Fijo.
Tipo de Montaje:	Fijo.
Longitud Focal:	2,8 mm (3,6 mm opcional)
Abertura Máxima:	F2.0/F2.0

Punto de Vista:	H:100°/77°, V:55°/42°
Control de Enfoque:	Fijo.
RED	
Ethernet:	RJ-45 (10/100Base-T)
Wi-Fi:	Wi-Fi (IEEE802.11b / g / n) 50 m en campo abierto.
Protocolos:	HTTP-HTTPs-TCP-ARP-RTSP-RTP-UDP-SMTP-FTP
	DHCP-DNS-DDNS-IPv4/v6-QoS-UpnP-NTP
	Bonjour-Multicast-ICMP-IGMP
Interoperabilidad:	ONVIF, PSIA, CGI
Método de Transmisión:	Unicast / Multicast
Acceso Máximo de Usuarios:	10 usuarios / 20 usuarios
Almacenamiento Perimetral:	NAS (almacenamiento conectado a la red) PC local para grabación instantánea.
	Tarjeta Micro SD de 128 GB
Visor Web:	IE, Chrome, Firefox, Safari
Software de Gestión:	Smart PSS, DSS, Lechange
Tele´fono Inteligente:	iOS, Android
VIDEO	
Compresión:	H.264 - H.264B - H.264H – MJPEG.
Capacidad de transmisión:	2 Streams
Resolución:	3M(2304×1296)/1080P(1920×1080)/ 1.3M(1280×960)/720P(1280×720)/720P(1280×720) / VGA(640×480)/QVGA(320×240)
Cuadros por segundo:	3M(1 ~ 20fps)/2M (1 ~ 25/30fps)
	VGA(1 ~ 25/30fps)
Control de tasa de bits:	CBR - VBR
Tasa de Bits:	H264:32K ~ 10Mbps
Día / noche	Auto(ICR) - Color - B/W
Modo BLC:	BLC - HLC – DWDR.
Balance de Blancos:	Auto – Natural - Street Lamp - Outdoor- Manual.
Reducción de Ruido:	3D DNR.
Detección de movimiento:	Off / On (4 Zonas, Rectangulo).
Imagen electrónica:	Sí.
IR inteligente:	Sí.
Zoom Digital.	16x
Flip:	0°/90°/180°/270°
Espejo:	Off / On
Enmascaramiento de privacidad:	Apagado.
	Encendido (4 áreas, rectángulo)
ELECTRICO	
Fuente de alimentación:	DC12V
consumo de energía:	<4.4W

Fuente: Elaborada por el Autor

3.1.3.3 Grabador de video en red NVR5816/5832/5864-16P-4KS2E.

Este grabador de video en red NVR5000-4KS2, ofrece un excelente rendimiento y una alta calidad de grabación para aplicaciones IP de video

vigilancia, posee un potente procesador, proporciona la capacidad de procesamiento de resolución de hasta 4K para aplicaciones donde se requieren detalles de imagen súper altas.

Debido a su diseño, este NVR es ideal para una amplia gama de ambientes de implementación como instituciones públicas, financieras, escuelas, empresas privadas, etc. Cuenta con una arquitectura abierta que admite el acceso multiusuario y es compatible con el protocolo ONVIF, que permite la interoperabilidad con cámaras 4K. Entre las características principales de este NVR, se tiene:

- **Smart H.265+:** Este códec de compresión de video, es la implementación optimizada del H.265, utiliza una estrategia de codificación adaptativa de escena, GOP y ROI dinámico, estructura flexible de referencia multitrama y reducción inteligente de ruido, logrando de esta manera la entrega de videos de alta calidad sin forzar la red. Con esta nueva tecnología se obtiene la reducción de la tasa de bits de transmisión y de la capacidad de almacenamiento hasta en un 70% en comparación con la compresión de video H.265.
- **Smart Fan:** Este NVR se encuentra equipado con un ventilador inteligente para lograr una alta eficiencia de enfriamiento, es decir que ajusta automáticamente la velocidad del ventilador de acuerdo con la temperatura del CPU y la temperatura ambiente.
- **Aplicación DMSS:** es un sistema de vigilancia móvil digital (DMSS, Digital Mobile Surveillance System), que instalada en cualquier dispositivo móvil permite acceder de forma remota al NVR, obteniendo de esta manera la visualización en tiempo real de los videos de las cámaras de video vigilancia desde cualquier lugar en el mundo con acceso a internet.
- **Tecnología de reposición automática de red (ANR):** Los grabadores de video en red, que tienen en su estructura la función ANR (Automatic Network Reset), almacenan automáticamente los datos de video de una cámara IP en una tarjeta micro SD, cuando la red se encuentra desconectada por algún tipo de daño en la conexión y cuando se haya

recuperado la conexión a la red, el NVR recupera automáticamente los datos de los videos almacenados en cada cámara. Tema muy importante en este proyecto, puesto que en el mismo se va a utilizar un medio de conexión inalámbrico.

En la tabla 3.3 se observan las especificaciones técnicas más importantes del video grabador en red NVR5816/5832/5864-16P-4KS2E.

Tabla 3.3: Especificaciones técnicas del NVR5816/5832/5864-16P-4KS2E.

SISTEMA		
Procesador Principal:	Procesador integrado de cuatro núcleos (Quad-core)	
Sistema Operativo:	LINUX integrado.	
AUDIO Y VIDEO		
Entrada de Cámara IP:	16/32/64 canales	
Charla Bidireccional:	Entrada de 1 canal - Salida de 2 canales.	
MONITOR		
Interfaz:	2 HDMI - 2 VGA	
Resolución:	**HDMI1:** 3840x2160 – 1920x1080 – 1280x1024 – 1280x 720 – 1024x768.	
	VGA1: 1920x 080 – 1280x1024 – 1280x720 – 1024x768.	
	HDMI2/VGA2: 1920x1080.	
Capacidad de Decodificación:	4-canales de 8MP (30fps).	
	16-canales de 1080P (30fps).	
Monitor Multi-pantalla:	1era Pantalla:	**16CH:** 1/4/8/9/16
		32CH: 1/4/8/9/16/25/36
		64CH: 1/4/8/9/16/25/36/64
	2da Pantalla:	1/4/8/9/16
OSD:	Título de la cámara – Hora – Bloque de la cámara – Detección de movimiento – Grabación.	
GRABACIÓN		
Compresión:	Smart H.265+	Smart H.264+
	H.265	H.264
	MJPEG	
Resolución:	12MP - 8MP - 6MP - 5MP - 4MP - 3MP -1080P - 1.3MP - 720P - D1.	
Tasa de Bits:	16Kbps ~ 20Mbps por canal	
Modo de Grabación:	Manual – Horario.	
	MD (detección de movimiento).	
Intervalo de Registro:	1 ~ 120 min (predeterminado: 60 min), Pre-grabación: 1 ~ 30 segundos.	
	Post-grabación: 10 ~ 300 Segundo's.	
REPRODUCCIÓN Y COPIA DE SEGURIDAD		
Modo de Búsqueda:	Hora - fecha, alarma - MD y búsqueda exacta (con precisión de segundos).	
Función de Reproducción:	Reproducir, Pausar - Detener, Rebobinar - Reproducción rápida - Reproducción lenta - Archivo siguiente - Archivo anterior - Cámara	

	siguiente - Cámara anterior - Pantalla completa - Selección de respaldo - Zoom digital.
Modo de Respaldo:	Dispositivo USB - Red - Dispositivo eSATA.
RED	
Interfaz:	1 RJ-45 Port (10/100/1000Mbps)
PoE:	16 puertos (IEEE802.3af / at)
	1-8 puertos compatibles con ePoE y EoC.
Función de Red:	HTTP – HTTPS - TCP/IP - IPv4/IPv6 – UpnP – SNMP – RTSP – UDP – SMTP – NTP – DHCP – DNS - IP Filter – PPPoE – DDNS – FTP – Servidor de alarmas – Búsqueda de IP (cámara IP, DVR, NVS, etc.) - P2P.
Acceso Máximo de Usuarios:	128 usuarios.
Interoperabilidad:	ONVIF 2.4, SDK, CG.
INTERFAZ AUXILIAR	
USB:	4 puertos USB (2 USB 3.0 posteriores, 2 USB 2.0 frontales)
RS232:	1 puerto, para comunicación con PC y teclado
RS485:	1 puerto para control de PTZ.

Fuente: Elaborada por el Autor

Para el diseño de este sistema de seguridad de CCTV y debido a las condiciones físicas de la edificación de la Gobernación de El Oro, el medio de comunicación entre las cámaras y DVR para la transmisión de la información será inalámbrica por medio de una red conformada por varios puntos de acceso en los diferentes pisos del edificio. Por ende, el siguiente tema a tratar es el diseño de la red inalámbrica.

3.2 Diseño de la Red Wi-fi para el sistema de seguridad CCTV.

Para diseñar la red Wifi lo primero que se debe toma en cuenta, es el lugar donde se pretende implementarla, para saber qué tipo de equipos se deben de utilizar, tomando en cuenta el área de cobertura, la tecnología más adecuada, debido a que la red debe ser lo suficientemente robusta para soportar la tasa de transmisión para la cual va a ser utilizada.

Esta red Wifi va a ser elaborada en las instalaciones de la Gobernación de la provincia de El Oro, como medio de comunicación entre los equipos que van a conformar un sistema de seguridad de CCTV y se debe saber la ubicación de las cámaras a conectar en el sistema inalámbrico y determinar

cuántos Access Point se van a utilizar en el diseño de red wifi y como van a ser conectados a la LAN que actualmente dispone la institución.

Como ya se trató anteriormente el diseño de un sistema CCTV para las instalaciones de la gobernación de El Oro, en base al mismo se determina cuántos AP se utilizarán por piso y cómo se conectarán a la LAN, considerando que el edificio dispone actualmente con una red de este tipo que dispone de pequeños racks en cada piso, conectados a la red principal del cuarto de equipos de dicha institución.

Por ende, para este diseño se va a determinar los equipos a utilizar, para posteriormente determinar su ubicación en los diferentes pisos que conforman la Gobernación de El Oro.

3.2.1 Equipos a utilizar en el diseño de la red Wifi.

De acuerdo con la distribución de las cámaras en cada piso donde funciona la Institución, se determina el diseño de la red Wifi del proyecto para que pueda soportar la transferencia de datos de cada cámara, para lo cual se necesitarán 6 AP inalámbricos del modelo AP UniFi UAP-AC-HD.

Así mismo, se ha considerado el modelo de Switch administrable Hp 1920s-24g Jl381a de 24 Puertos Gigabit, como dispositivo de conexión para los AP a la red y como vínculo entre la red inalámbrica y la LAN de la Institución.

3.2.1.1 Punto de acceso (AP) UniFi UAP-AC-HD.

Para elegir el equipo que se va a utilizar en esta red wifi, se debe tener en cuenta el área de cobertura y el tráfico de información que se va a manejar en la misma y considerando que la red Wifi está siendo diseñada como medio de comunicación en un sistema de seguridad de CCTV se ha elegido los AP UniFi AP AC HD, que son sumamente robustos y con las características necesarias para la implementación de este proyecto.

Figura 3.9: Punto de acceso UniFi AP AC HD.
Fuente: www.unifi-hd.ui.com

Características: entre las principales se tiene:

- **RF Environment:** permite detectar en el entorno las frecuencias de radio y solucionar los problemas de interferencia que puedan causar.
- **PowerFul RF:** permite realizar análisis espectral, equidad de tiempo aire y dirección de banda.
- **Wireless Uplink:** permite la conectividad inalámbrica entre AP para extender el alcance de cobertura de la red inalámbrica y realizar cambios en tiempo real en la topología de la red.
- **Hotspot Support:** permite aplicar diferentes tasas de ancho de banda para carga y descarga para limitar la cantidad de datos y tiempo de uso de estos dentro de la red.

Especificaciones técnicas: en la tabla 3.4 se observan las más importantes del AP UniFi UAP-AC-HD.

Tabla 3.4: Especificaciones técnicas del Access Point UniFi UAP-AC-HD.

Interfaz de Red:	2 puertos Ethernet 10/100/1000.
Método de Energía:	802.3at PoE+
Rango de voltaje admitido:	44 to 57VDC
Fuente de alimentación:	UniFi Switch (PoE)
Ahorro de energía:	Sí.
Consumo máximo de energía	17W
PODER DE TX	
2.4 GH	6-25 dBm
5 GHz	6-25 dBm

ANTENAS	
2.4 GHz	2 Antenas de doble puerto y polaridad dual, 3 dBi cada una.
5 GHz	2 Antenas de doble puerto y polaridad dual, 4 dBi cada una.
Estándares de Wi-Fi:	802.11 a/b/g/n/r/k/v/ac/ac-wave2
Seguridad inalámbrica:	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
	802.11w/PMF
BSSID:	Hasta 8 por radio.
GESTIÓN DE TRÁFICO AVANZADO	
VLAN:	802.1Q
QoS avanzada:	Limitación de tasa por usuario
Aislamiento de tráfico de invitados:	Sí.
WMM:	Voz, video, mejor esfuerzo y fondo
Clientes Concurrentes:	1000+
TASAS DE DATOS ADMITIDOS (Mbps)	
Estándar	**Tasas de transferencia de datos**
802.11a	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11n	6.5 Mbps a 450 Mbps (MCS0 - MCS23, HT 20/40)
802.11ac	6.5 Mbps a 1.7 Gbps (MCS0 MCS9 NSS1 / 2/3/4, VHT 20/40/80)
	58 Mbps a 1,7 Gbps (MCS0 MCS9 NSS1 / 2, VHT 160)
802.11b	2, 5.5, 11 Mbps
802.11g	6, 9, 12, 18, 24, 36, 48, 54 Mbps

Fuente: El Autor

Una vez determinado el modelo del AP a utilizar en el diseño de la red inalámbrica, lo siguiente es la distribución de ellos en los diferentes pisos del edificio y su conexión a la red LAN de este.

3.2.1.2 Switch para la conexión de los equipos Wifi a la red LAN

Para el diseño de una red Wifi, uno de los equipos principales a tomar en cuenta es el Switch, al cual van conectados todos los AP que forman parte de la red inalámbrica y los equipos del sistema de seguridad de CCTV, para su posterior conexión a la red LAN activa que actualmente dispone la Gobernación de la provincia de El Oro y así puedan tener salida a Internet. Por ende, para este tipo de proyecto y debido a las exigencias del tráfico

que se va manejar en el mismo, el equipo que se va a utilizar es un Switch administrable Hp 1920s-24g Jl381a de 24 Puertos Gigabit.

Figura 3.10: Switch Hp 1920s-24g Jl381a de 24 Puertos Gigabit.
Fuente: www.buy.hpe.com/us/en

Características Principales:

- **Gestión Web:** permite al usuario gestionar la parte administrativa del equipo a través de una interfaz web gráfica que admite HTTP y HTTPS son iguales
- **Duplicación de puertos:** característica conocida como Port Mirroring, permite que el tráfico de datos de los puertos del equipo se envíe de manera simultánea a un analizador de red para su posterior monitoreo.
- **Puertos SPF:** Este tipo de puerto permite al equipo conectarse a otros dispositivos a través de una amplia variedad de cables de fibra óptica y aumentar el alcance de la transmisión de datos de la red.
- **Lista de control de acceso (ACL, Access Control List):** permite que el equipo pueda filtrar mediante una lista de control, el acceso o la denegación de los paquetes de datos, obteniendo de esta manera el aumento en el rendimiento de la red.
- **Aislamiento de puertos:** permite el aislamiento de grupos de puertos en el equipo, impidiendo de esta manera el tráfico de datos en los puertos de un mismo grupo, proporcionando de esta forma privacidad y seguridad de los datos.

Especificaciones Técnicas.

En la tabla 3.5 se pueden observar las especificaciones técnicas más importantes del Switch administrable Hp 1920s-24g Jl381a de 24 Puertos Gigabit.

Tabla 3.5: Especificaciones Switch HP 1920s-24g Jl381a 24 Puertos Gigabit

Puertos y ranuras de E / S:	**24 puertos RJ-45 10/100/1000 con detección automática**
	IEEE 802.3 Tipo 10BASE-T, IEEE 802.3u Tipo 100BASE-TX, IEEE 802.3ab Tipo 1000BASE-T
	Dúplex: 10BASE-T / 100BASE-TX: medio o completo
	1000BASE-T: solo completo
	2 puertos SFP 100/1000 Mbps
	(IEEE 802.3z Tipo 1000BASE-X, IEEE 802.3u Tipo 100BASE-FX
Memoria y procesador:	ARM Cortex-A9 @ 400 MHz, 256 MB
	SDRAM, 64 MB flash; packet buffer: 1.5 MB
Latencia de 100 Mb:	< 7µs
Latencia de 1000 Mb:	< 2 µs
Rendimiento:	hasta 38,6 Mbps (paquetes de 64 bytes)
Capacidad de enrutamiento / conmutación:	52 Gbps.
Tamaño de la tabla de enrutamiento:	32 entradas.
Tamaño de la tabla de direcciones MAC:	8000 entradas.
Características eléctricas	
Frecuencia:	50/60 Hz
Voltaje de corriente alterna:	100 - 240 VAC
Corriente:	0.2 A

Fuente: Elaborada por el Autor

Una vez determinados los AP y el Switch que se utilizarán en el diseño de la red inalámbrica, el paso siguiente es la distribución de cada uno de los equipos en los diferentes pisos de la Gobernación de la provincia de El Oro, así como la conexión respectiva de los equipos a la red LAN de la institución.

3.2.2 Diseño de la Red Wifi en el Piso 2.

La figura 3.11 muestra la distribución de los diferentes AP en el piso número 2 del edificio de la Gobernación de El Oro, se puede apreciar que se necesitan 2 AP para cubrir toda el área donde se encuentran ubicadas las cámaras Wifi y se puedan conectar a la red LAN, para su conexión con el NVR.

Cabe recalcar que estos AP estarán conectados con cable UTP CAT 6E hasta el Switch en el rack principal, ubicado en el piso 2 formando parte de la red LAN activa de la gobernación de El Oro y que es parte del cuarto de equipos principales donde se encuentran todos los dispositivos de red, incluido el NVR (figura 3.11):

- Unidad de Tecnologías de la Información y Comunicación.
- Unidad de Guardalmacén.
- Comisaría I Nacional de Policía del Cantón Machala.
- Intendencia General de Policía de la Provincia de El Oro.

3.2.3 Diseño de la Red Wifi en el Piso 3.

La figura 3.12 muestra la distribución de los AP del piso 3 del edificio de la Gobernación de El Oro, se puede apreciar que se necesitan 2 AP, con la finalidad de tener una cobertura total del área donde se encuentran ubicadas las cámaras Wifi y así se puedan conectar a la red LAN para que a su vez tengan conexión con el NVR.

Así mismo se debe tomar en cuenta que estos AP estarán conectados por cable UTP CAT 6E hasta un rack secundario ubicado en este piso y el cual forma parte de la red LAN activa de la gobernación de El Oro, que tiene conexión directa con el cuarto de equipos principales donde se encuentran todos los equipos de red, incluido el NVR y donde se conecta con el Switch principal de la red Wifi.

- Unidad de Planificación y Gestión Estratégica.
- Unidad de Talento Humano.
- Compras Públicas.
- Dirección Administrativa Financiera.

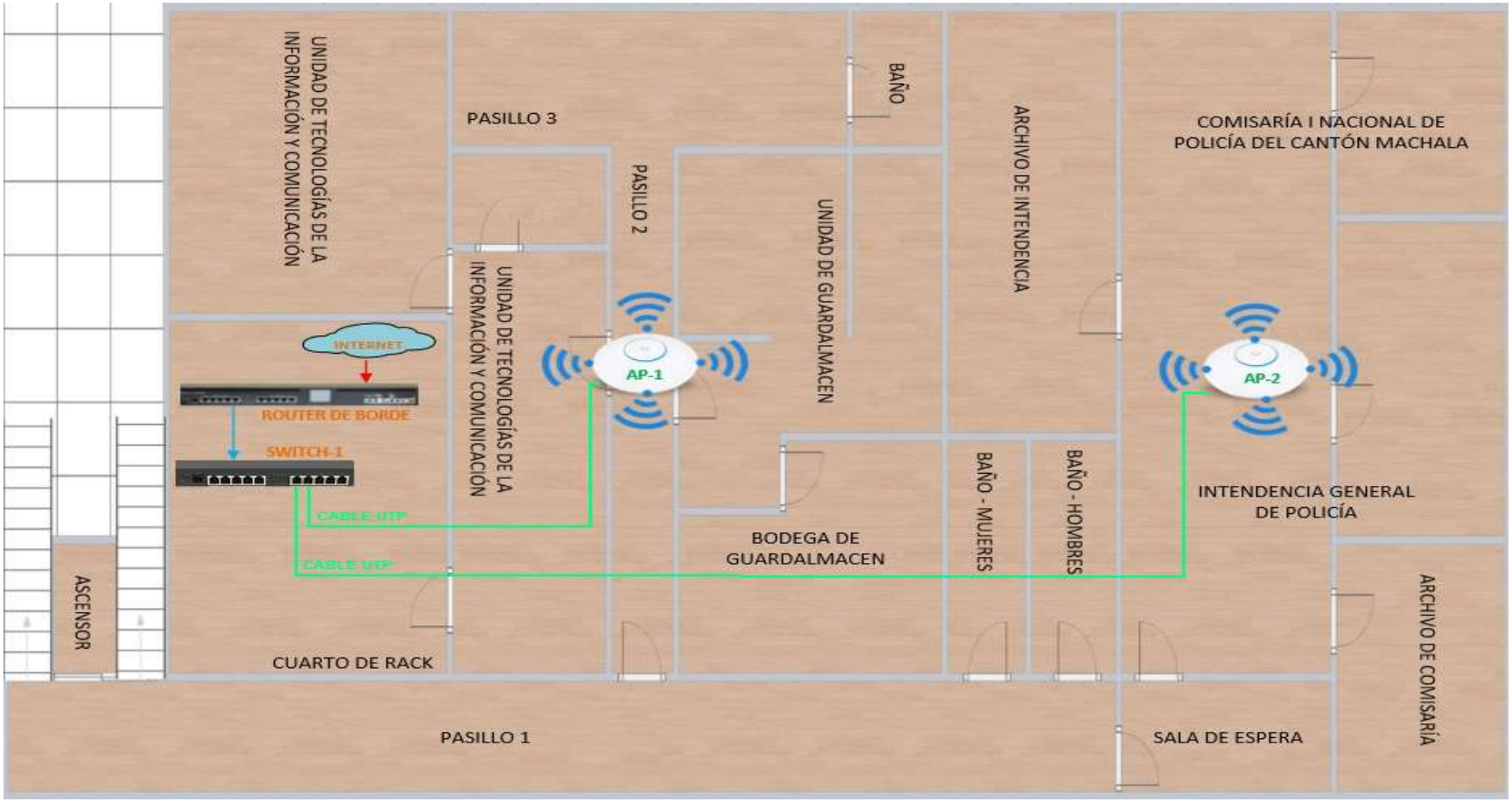


Figura 3.11: Distribución y ubicación de los AP en el Piso 2.
Fuente: El Autor.

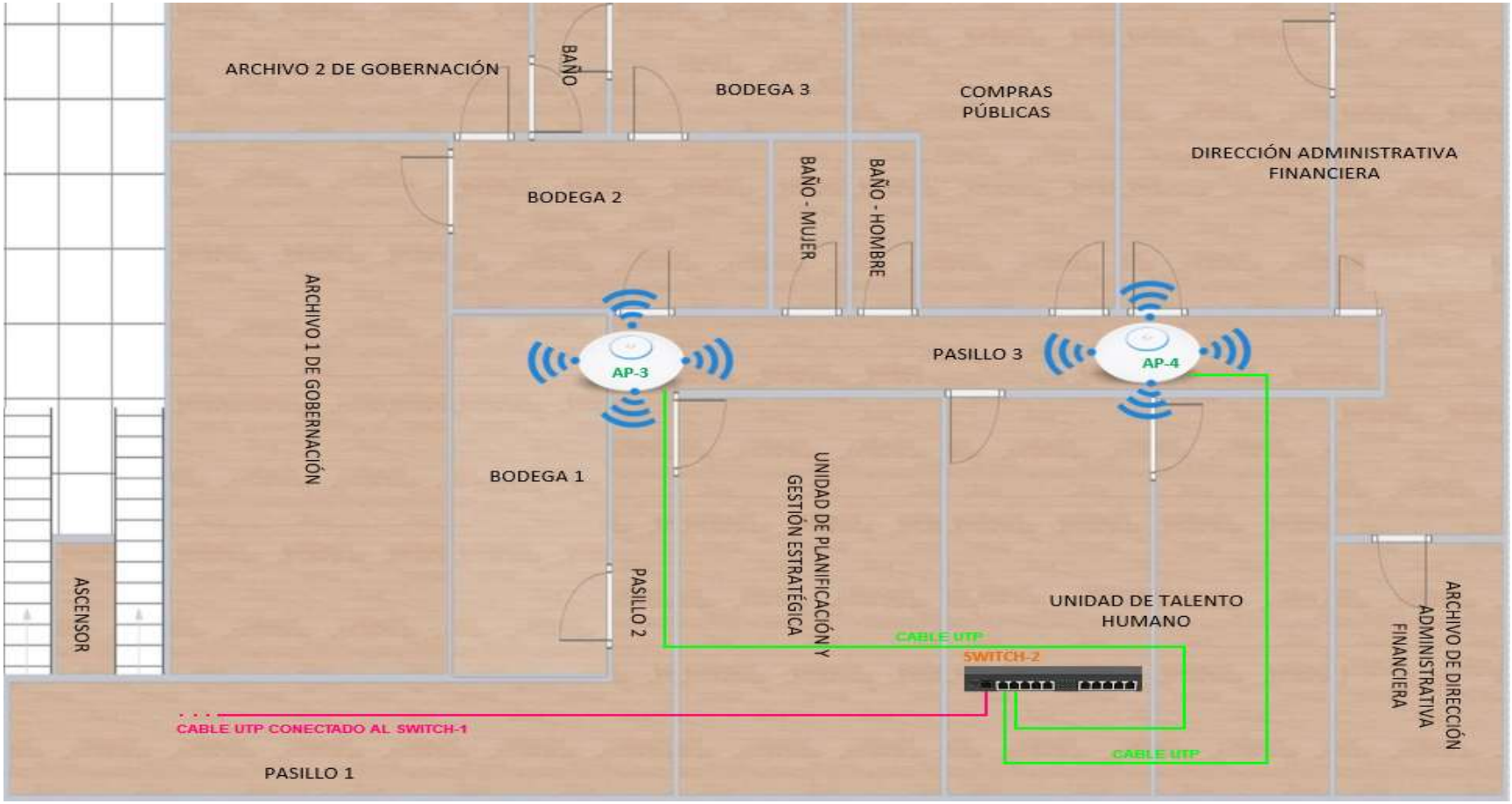


Figura 3.12: Distribución y Ubicación de los AP en el Piso 3.
Fuente: El Autor.

3.2.4 Diseño de la red Wifi en el Piso 4.

La Figura 3.13 muestra la distribución de los diferentes AP en el piso 4 del edificio de la Gobernación de El Oro, y como se puede apreciar se necesitan 2 AP, para tener una cobertura total del área donde se encuentran ubicadas las cámaras Wifi y así se puedan conectar a la red LAN, para que a su vez tengan conexión con el NVR del sistema de seguridad CCTV.

Así mismo, se debe tomar en cuenta que en este piso del edificio se encuentra ubicado un rack secundario para la conexión a la red LAN de los diferentes dispositivos de la Institución, por ende, los AP que serán instalados en este piso irán conectados por medio de cable UTP CAT 6E hacia este rack secundario, el mismo que ya tiene conexión directa con el cuarto de equipos principales donde se encuentran todos los equipos de red, incluido el NVR y donde se conectará con el Switch principal de la red WIFI que conecta lodos los dispositivos del sistema de seguridad CCTV.

- Unidad de Comunicación Social.
- Secretaria General.
- Jefatura Política del Cantón Machala.
- Salón de Integración “Dra. Patricia Montero Armijos”.
- Despacho de Gobernador.
- Asesoría Jurídica.
- Unidad de Transporte.

Una vez que se ha determinado la ubicación de cada AP en los diferentes pisos de la Gobernación de El Oro y su respectiva conexión a la red LAN activa de la institución, corresponde observar cómo esta Wifi trabaja como medio de conexión del sistema de seguridad de CCTV.

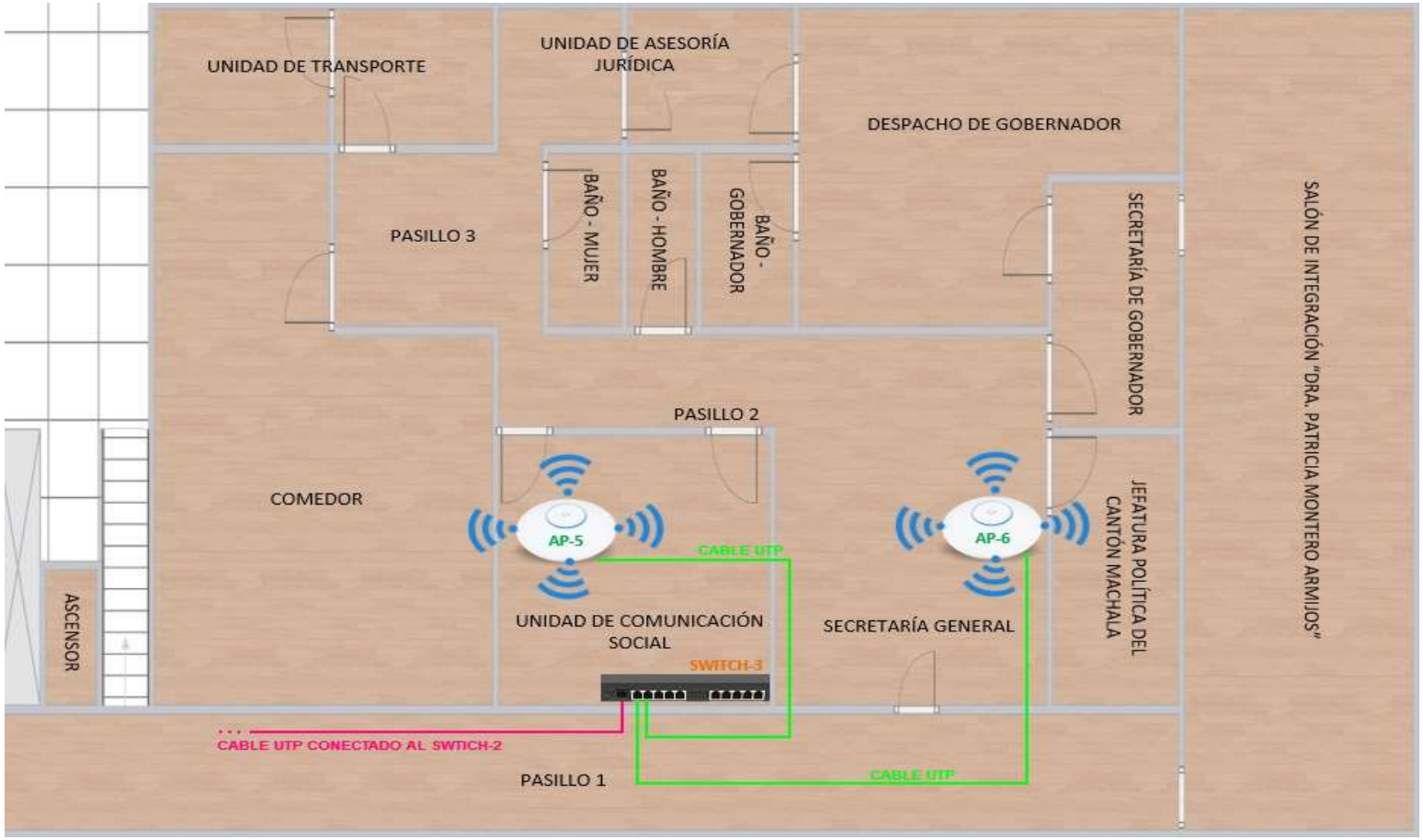


Figura 3.13: Distribución y Ubicación de los AP en el Piso 4.
Fuente: El Autor.

3.3 Diseño de un sistema de seguridad CCTV mediante una red WIFI.

Este proyecto fue diseñado con la finalidad de cubrir las necesidades que actualmente tiene la Gobernación de la Provincia de El Oro, mediante la implementación de un sistema de seguridad que cumpla con los requerimientos y exigencias de video vigilancia las 24 horas del día en dicha institución, tomando en consideración las complicaciones que conllevaría la ejecución de dicho proyecto en sus instalaciones, debido a la infraestructura en la que se encuentran ubicados, la misma que no dispone de tuberías para un nuevo cableado estructurado para el sistema de seguridad, por ende y como objetivo principal de este proyecto es precisamente la creación de una red Wifi que funcione como medio de conexión entre los dispositivos de la red de seguridad de CCTV.

A continuación, se pueden observar los diagramas del diseño del sistema de seguridad de CCTV por medio de una red WIFI para cada piso de la Gobernación de la provincia de El Oro, en las cuales se observa como las cámaras WIFI que se encuentran ubicadas en el edificio se conectarán a los AP que forman parte de la red inalámbrica y que servirán como medio de conexión del sistema de seguridad CCTV para la transmisión de los videos de seguridad que generan cada una de estas cámaras hacia el NVR que va estar instalado y conectado al Switch principal (Swtich-1) donde se enlazará todo el sistema Wifi y el mismo que usará la red LAN activa que actualmente dispone la Institución.

3.3.1 Sistema de seguridad CCTV mediante una red WIFI en Piso 2.

La figura 3.14 detalla la distribución de las cámaras Wifi, así como la de los AP en el piso 2 del edificio de la Gobernación de la provincia de El Oro, que a su vez permite ver como cada cámara Wifi se conecta a los AP correspondientes para la transmisión de los videos hacia el NVR, que se encuentra en el cuarto de equipos principal y conectado por medio del

Switch a la red LAN activa de dicha institución, de donde sale la conexión a cada uno de los AP de la red Wifi.

3.3.2 Sistema de seguridad CCTV mediante una red WIFI Piso 3.

La figura 3.15 muestra la distribución y de las cámaras Wifi, así como la de los AP en el piso 3 del edificio, al igual que permite observar cómo cada cámara inalámbrica se conecta a los AP correspondientes para la transmisión de los videos hacia el NVR, que se encuentra en el cuarto de equipos principal, tomando en consideración que en este piso existe un rack secundario que pertenece a la red LAN activa que actualmente dispone dicha institución, el cual tiene conexión directa con el cuarto de equipos de la gobernación, donde se encuentra el Switch principal (Switch-1) para la conexión a cada AP de la red Wifi que sirve como medio de comunicación entre los dispositivos del sistema de seguridad CCTV.

3.3.3 Sistema de seguridad CCTV mediante una red WIFI Piso 4.

La figura 3.16 detalla la distribución de las cámaras inalámbricas, así como la de los AP en el piso 4 del edificio y a su vez permite observar la conexión de las cámaras Wifi a los AP para la transmisión de los videos al NVR que se encuentra en el cuarto de equipos principal, tomando en cuenta que en este piso existe un rack secundario que sirve como conexión principal para los dos AP que a su vez se conectan al cuarto de equipos principal por medio de dicho rack, llegando al Switch que forma parte de la red inalámbrica.

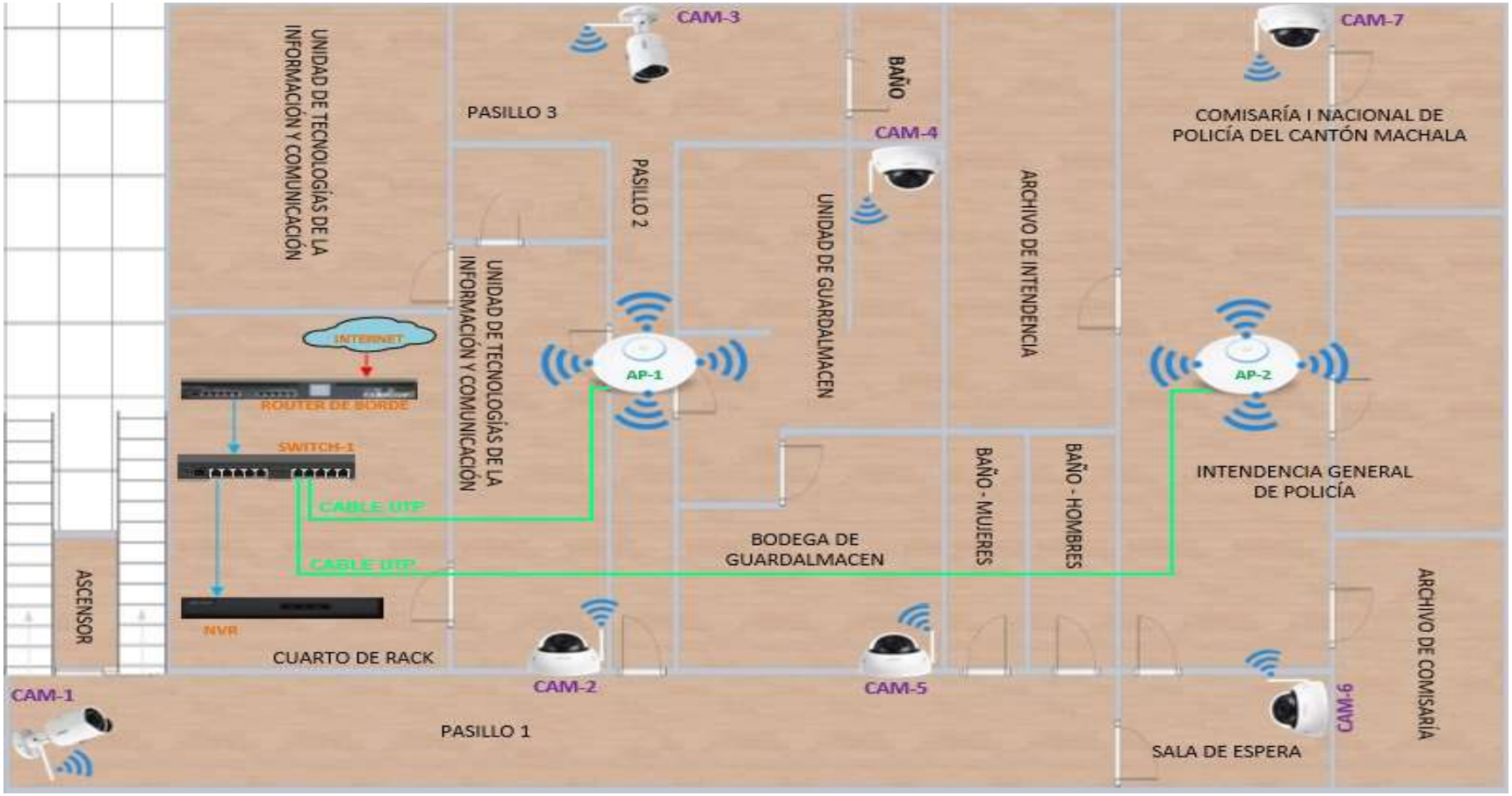


Figura 3.14: Diseño del sistema de seguridad CCTV mediante una red Wifi para el Piso 2.
Fuente: El Autor.

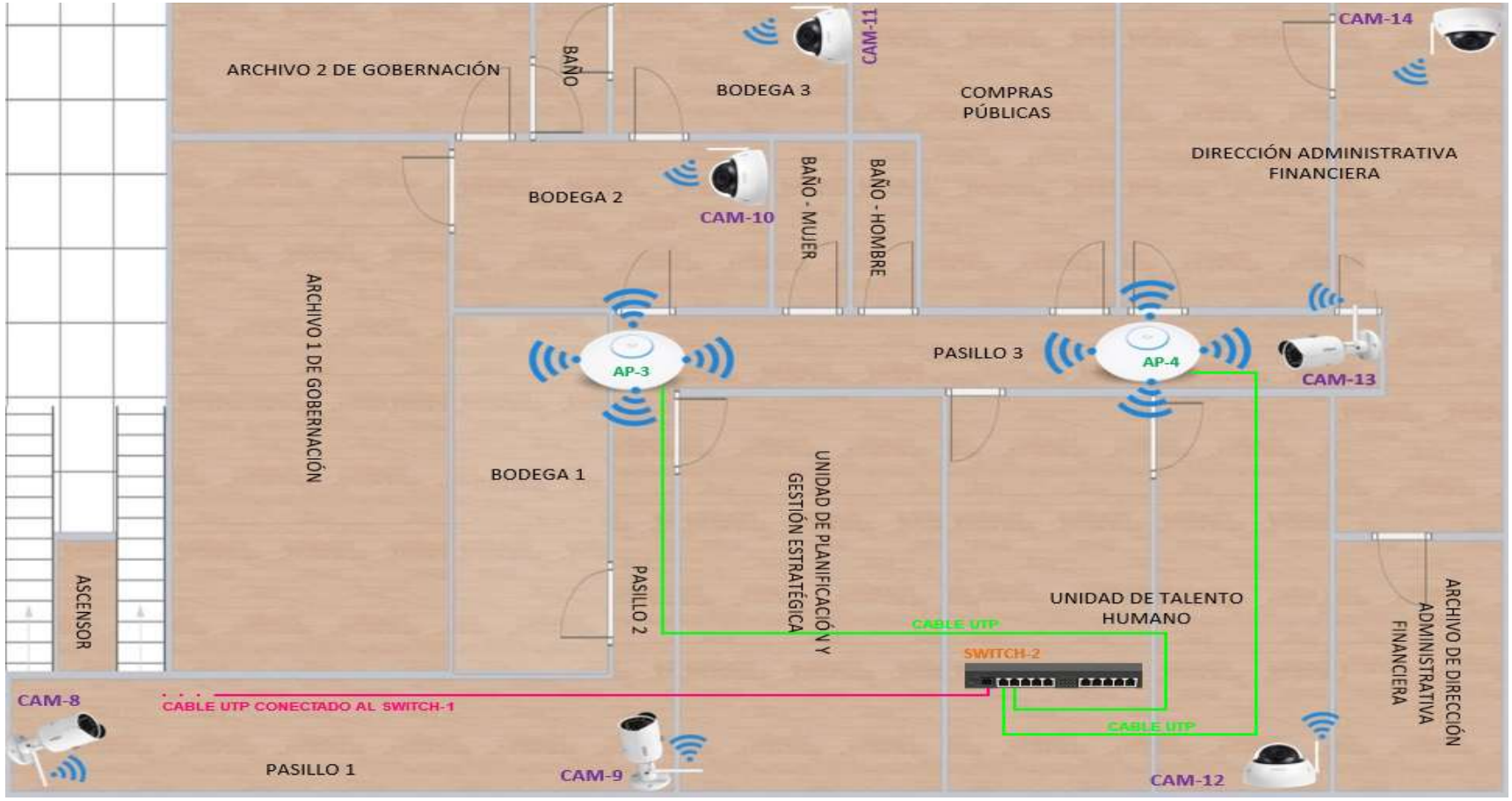


Figura 3.15: Diseño del sistema de seguridad CCTV mediante una red Wifi para el Piso 3.
Fuente: El Autor.

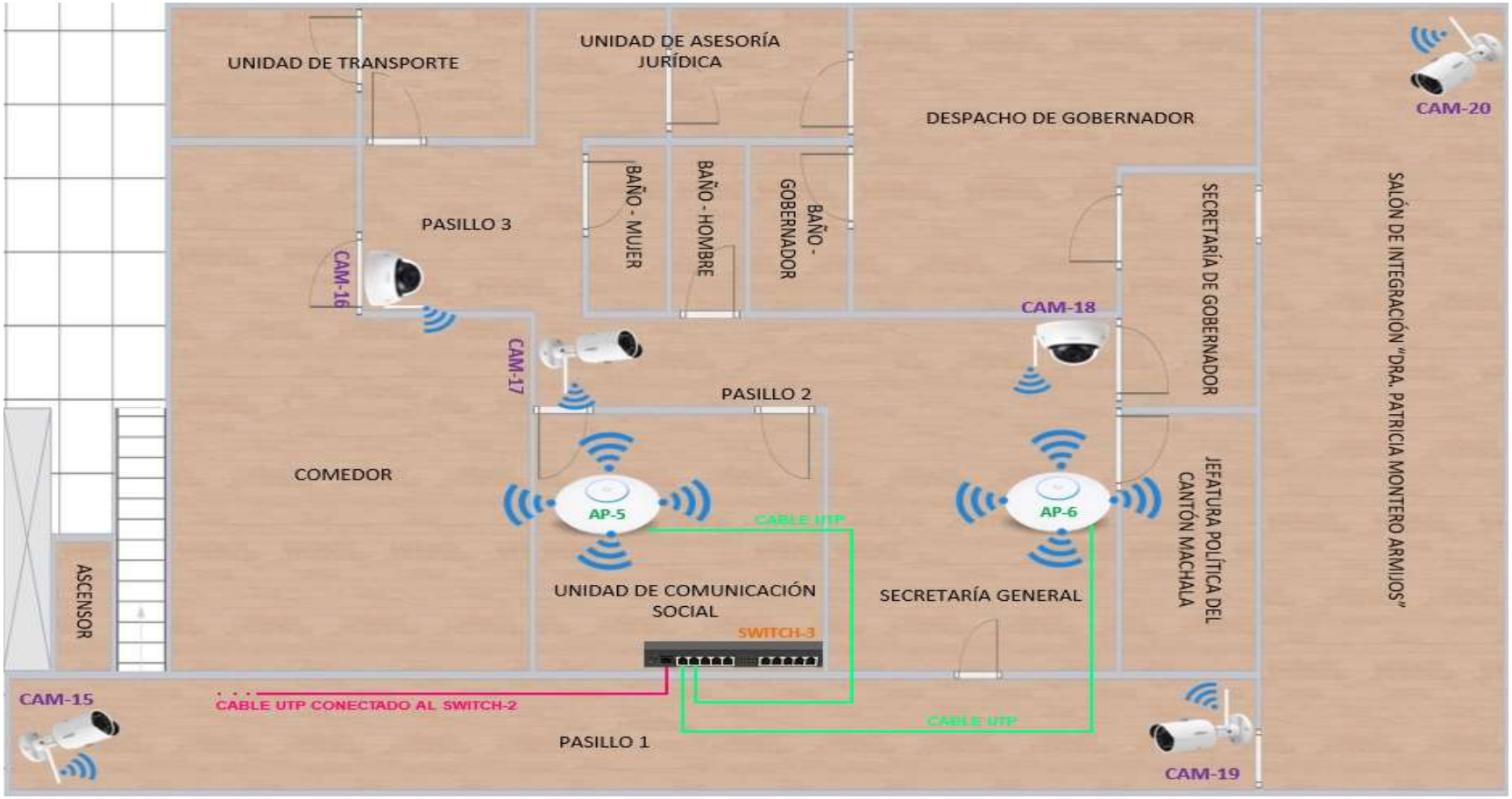


Figura 3.16: Diseño del sistema de seguridad CCTV mediante una red Wifi para el Piso 4.
Fuente: El Autor

Conclusiones.

1. Gracias a las investigaciones, avances tecnológicos y creación de nuevos estándares que se han generado con el transcurso de los años para las tecnologías de comunicación inalámbrica, se han convertido en la actualidad en medios de transmisión estables, seguras y con capacidad para transmitir una gran cantidad de ancho de banda, convirtiéndolas de esta manera en uno de los medios de transmisión más utilizados para la comunicación entre dispositivos, entre ellos los dispositivos que forman parte de un sistema de seguridad de CCTV.

2. Los sistemas de circuito cerrado de televisión (CCTV) como sistemas de seguridad permiten monitorear áreas de forma remota por medio de la apreciación de videos, imágenes y audio, con el objetivo de proporcionar protección a personas y bienes materiales, logrando minimizar pérdidas ante incidentes de seguridad y de siniestros que pueden ocurrir durante el transcurso del día.

3. Gracias a la diversidad de tipos de tecnologías a los que se pueden acoplar actualmente los diferentes sistemas de seguridad de CCTV, hacen que sean más flexibles con respecto a los diferentes lugares y entornos físicos en los cuales se los desea implementar; tomando siempre en consideración el medio de transmisión que se va a emplear.

4. Las características de una red WIFI se determinan a partir de los diferentes parámetros de velocidad de transmisión, frecuencia y área de cobertura que soportarán los diversos dispositivos seleccionados de acuerdo al estándar IEEE 802.11, para formar parte de la estructura de la red inalámbrica. Las redes inalámbricas WIFI pueden ampliar su área de cobertura fácilmente gracias a su flexibilidad y escalabilidad para soportar el aumento de puntos de

acceso AP, para satisfacer la demanda del aumento de nuevos usuarios o nuevos dispositivos conectados a la red.

5. Se analizaron varias opciones para el diseño de un sistema de seguridad de CCTV para la Gobernación de la Provincia de El Oro en la ciudad de Machala, sin embargo, debido a las condiciones físicas y estructurales en las cuales se encuentra el edificio de la Institución actualmente, se determinó por medio de este proyecto que la opción más viable y segura es precisamente la creación de una red inalámbrica que sirva como medio de transmisión para el sistema de seguridad de CCTV que se pretende implementar.

Recomendaciones.

1. Para obtener una comunicación inalámbrica correcta entre los puntos de acceso (AP) y las cámaras de video vigilancia, se necesita tener una cobertura de área optima por parte de los AP de los lugares que se van a visualizar para el control y monitoreo en la Institución.

2. Debido a que los diferentes dispositivos que formarán parte de la estructura del sistema de CCTV usarán una red inalámbrica WIFI como medio de transmisión, se recomienda tener una cantidad de ancho de banda que garantice y soporte el flujo constante de la transmisión de audio y video.

3. Para determinar la ubicación para la instalación de las cámaras que formarán parte del sistema de CCTV, se recomienda verificar la iluminación del lugar y el mejor posicionamiento visual posible de las áreas que se pretende monitorear.

4. Una vez implementado este proyecto, se puede analizar la opción de realizar el diseño para la segmentación del tráfico de la red interna por medio de VLAN, con la finalidad de separar justamente el tráfico interno de la red LAN de los diferentes usuarios de la Institución y el que genera el sistema de seguridad de CCTV, con el objetivo de obtener mayor seguridad en el mismo

Referencias Bibliográficas

Bibliografía

AXIS. (s.f.). *www.axis.com*. Obtenido de www.axis.com: https://www.axis.com/es-ec/about-axis/history

Briceño Sanz, J. (2010). *Implementación de un Sistema de Seguridad en un Edificio Público.* Leganes: Repositorio de Universidad Carlos III de Madrid. Obtenido de http://hdl.handle.net/10016/10587

Cabezas Granado, L., & González Lozano, F. (2010). *Redes Inalámbricas.* Madrid: ANAYA MULTIMEDIA.

Cadavid Parra, J. (16 de Noviembre de 2017). *www.americacomunicaciones.com*. Obtenido de www.americacomunicaciones.com: https://www.americacomunicaciones.com/videovigilancia-historia/

Carballar Falcón, J. (2010). *WI-FI: Lo que se necesita conocer.* Madrid: RC Libros.

Chimborazo Toro, D. (2015). *Diseño de un sistema de videovigilancia con tecnología IP para el barrio La Delicia de la Ciudad de Ambato.* Quito: Repositorio de la Escuela Politécnica Nacional. Obtenido de http://bibdigital.epn.edu.ec/handle/15000/10770

Chóez Jalca, C. (2019). *Diseño de un Sistema Videovigilancia a través de cámaras con tecnología IP para el fortalecimiento de la seguridad en el laboratorio telecomunicaciones de la carrera de ingeniería en Computación y Redes.* Jipijapa: Repositorio de la Universidad Estatal del Sur de Manabí. Obtenido de http://repositorio.unesum.edu.ec/handle/53000/1601

Funcia, M. (02 de Julio de 2018). *www.camarasdeseguridadparacasa.com*. Obtenido de www.camarasdeseguridadparacasa.com: https://camarasdeseguridadparacasa.com/historia-de-la-camara-de-seguridad/

Huidobro Moya, J. M. (2015). *Telecomunicaciones. Tecnologías, Redes y Servicios. 2ª Edición Actualizada.* Madrid: RA-MA.

Instituto Nacional de Estadística e Informática Sub-Jefatura de Informática. (2015). *Redes inalámbricas Wireless.* Lima: INEI.

Josan, M. (29 de Octubre de 2018). *www.naseros.com*. Obtenido de www.naseros.com: https://naseros.com/2018/10/29/pasado-presente-y-futuro-de-las-conexiones-wifi/

Manrique Rey, F. (2011). *Diseño de un sistema de CCTV basado en red IP inalámbrica para seguridad en estacionamientos vehículares.* Lima: Repositorio de la Pontificia Universidad Católica del Perú. Obtenido de http://hdl.handle.net/20.500.12404/890

Marrone, L., Barbieri , A., & Robles, M. (2011). *Tecnologías Wireless y Movilidad en IPv4/IPv6.* Buenos Aires: Editorial de la Universidad Nacional de La Plata.

Martí Martí, S. (2013). *Diseño de un sistema de televigilancia sobre IP para el edificio CRAI de la Escuela Politécnica Superior de Gandia.* Gandia: Repositorio de la Universidad Politécnica de Valencia. Obtenido de http://hdl.handle.net/10251/34082

Merchán, J. (2012). *Diseño e Intalación de Sistemas de Videovigilancia CCTV Digitales.* Madrid: EDITOR ANTONIO MADRID VICENTE.

Monteros Mejía, J. (2015). *Diseño de un sistema de video-vigilancia inalámbrico para la ciudad de Cayambe.* Quito: Repositorio de la Escuela Politécnica Nacional. Obtenido de http://bibdigital.epn.edu.ec/handle/15000/10648

Moreno Larco, C., & Puente Morenacho, A. (2014). *Diseño e Implementación de una red Wifi y un Circuito Cerrado de Televisión para el sistema de seguridad , monitoreo y control de la Unidad Académica Héroes del Cenepa de la ESPE.* Sangolqui.

Narváez Pupiales, S. (2015). *Estudio de QoS basado en el estándar IEEE 802.11e y alternativas de seguridad para las redes locales inalámbricas aplicado en la WLAN de la Universidad Politécnica Estatal de Carchi.* Quito: Repositorio de la Pontificia Universidad Católica del Ecuador. Obtenido de http://repositorio.puce.edu.ec/handle/22000/9696

Pellejero, I., Andreu, F., & Lesta, A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN.* Barcelona: MARCOMBO S.A.

Reyes Rodríguez, J. (2018). *Implementación de un sistema de circuito cerrado por TV-CCTV basado en tecnología móvil para el monitoreo de la seguridad de los niños del nivel inicial del centro educativo preuniversitario Salesiano.*

Chiclayo: Repositorio de la Universidad Católica Santo Toribio de Mogrovejo. Obtenido de http://hdl.handle.net/20.500.12423/1440

Sabando C., J. (2011). *Fundamentos de Comunicaciones Inalámbricas.* México: Pearson Educación.

Salazar , J. (2017). *Wireless networks.* Praha: TechPedia. Obtenido de http://techpedia.fel.cvut.cz/es/single/?objectId=112

Salvetti, D. (2011). *Redes Wireless.* Buenos Aires: Fox Andina; Dalaga.

Serrano Castro, G. (2018). *Diseño de un sistema inalámbrico punto-multipunto con segmentación de tráfico por VLAN, para brindar servicio de internet a la parroquia Barbones del Cantón El Guabo en la Provincia de El Oro por medio de la empresa IPS CESCONET.* Guayaquil: Repositorio de la Universidad Católica de Santiago de Guayaquil. Obtenido de http://repositorio.ucsg.edu.ec/handle/3317/10849

Shaw, K. (03 de Febrero de 2018). *www.networkworld.es.* Obtenido de www.networkworld.es: https://www.networkworld.es/wifi/80211-estandares-de-wifi-y-velocidades

Villamar Chamba, G. (2018). *Análisis y diseño de un sistema de seguridad de video vigilancia sobre IP para una industria de alimentos balanceados.* Guayaquil: Repositorio de la Universidad Católica de Santiago de Guayaquil. Obtenido de http://repositorio.ucsg.edu.ec/handle/3317/10801

Glosario Técnico

CAPÍTULO 1:

CCTV Closed Circuit Television / Circuito Cerrado de Televisión.

DVR Digital Video Recorder / Grabadora de Video Digital.

SVGA Super Video Graphics Array / Súper Matriz de Gráficos de Vídeo.

WiFi Wireless Fidelity / Fidelidad Inalámbrica.

CAPÍTULO 2:

CCTV Closed Circuit Television / Circuito Cerrado de Televisión.

WPAN Wireless Personal Area Network / Red de Área Personal Inalámbrica.

WLAN Wireless Local Area Network / Red de Área Local Inalámbrica.

WMAN Wireless Metropolitan Area Network / Red de Área Metropolitana Inalámbrica.

WWAN Wireless Wide Area Network / Red de Área Amplia Inalámbrica.

HomeRF Home Radio Frequency / Radio Frecuencia Casera.

RFID Radio Frequency Identification / Identificación por Radio Frecuencia.

WLL Wireless Local Loop / Bucle Local Inalámbrico.

IEEE Institute of Electrical and Electronics Engineers / Instituto de Ingeniería Eléctrica y Electrónica.

WiMAX Worldwide Interoperability for Microwave Access / Interoperabilidad Mundial para Acceso por Microondas.

Mbps Mega bits per second / Mega bits por Segundo.

UMTS Universal Mobile Telecommunications System / Sistema Universal de Telecomunicaciones Móviles.

GPRS	General Packet Radio Service / Servicio General de Paquetes vía Radio.
GSM	Global System for Mobile communications / Sistema Global para las comunicaciones Móviles.
HSPA	High Speed Packet Access / Acceso a Paquetes de Alta Velocidad.
3G	Third Generation / Tercera Generación.
LMDS	Local Multipoint Distribution Service / Sistema de Distribución Local Multipunto.
WiFi	Wireless Fidelity / Fidelidad Inalámbrica.
OSI	Open System Interconnection / Interconexión de Sistemas Abiertos.
GHz	Giga Hertz / Giga Hercio.
MHz	Mega Hertz / Mega Hercio.
BPSK	Phase Shift Keying / Modificación de Cambio de Fase.
QAM	Quadrature Amplitude Modulation / Modulación de Amplitud en Cuadratura.
OFDM	Orthogonal Frequency-Division Multiple Access / Multiplexión por División en Frecuencias Ortogonales.
mW	mili Watts / mili Vatios.
DSSS	Direct Sequence Spread Spectrum / Espectro Encendido de Secuencia Directa.
CCK	Complementary Code Keying / Clave de Código Complementario.
QoS	Quality of Service / Calidad de Servicio.
MIMO	Multiple Input Multiple Output / Múltiple Entrada Múltiple Salida.
WiGig	Wireless Gigabit Alliance / Alianza Gigabit Inalámbrica.
SC-OFDMA	Single Carrier Frequency Division Multiple Access / Acceso Múltiple por División de Frecuencia de Operador único.
LAN	Local Area Network / Red de Área Local.
VHF	Very High Frequency / Frecuencia Muy Alta.
UHF	Ultra-High Frequency / Frecuencia Ultra Alta.

WEP	Wired Equivalent Privacy / Privacidad Equivalente a Cableado.
WPA	WiFi Protected Access / Acceso WiFi Protegido.
WPA2	WiFi Protected Access 2 / Acceso WiFi Protegido 2.
WPA3	WiFi Protected Access 3 / Acceso WiFi Protegido 3.
RC4	Rivest Code 4 / Código Rivest 4.
AES	Advanced Encryption Standard / Estándar de Cifrado Avanzado.
PSK	Pre Shared Key / Clave Compartida Previamente.
TKIP	Temporal Key Integrity Protocol / Protocolo de Integridad de Clave Temporal.
MIC	Message Integrity Codes / Códigos de Integridad de Mensajes.
MAC	Media Access Control / Control de Acceso a Medios.
CCMP	Counter Mode CBC-MAC Protocol / Protocolo CBC-MAC en Modo Contador.
FIPS 140-2	Federal Information Processing Standard 140-2 / Estándares Federales de Procesamiento de la Información.
SAE	Simultaneous Authentication of Equals / Autenticación Simultánea de Iguales.
OWE	Opportunistic Wireless Encryption / Cifrado Inalámbrico Oportunista.
AP	Access Point / Punto de Acceso.
IP	Internet Protocol / Protocolo de Internet.
TCP/IP	Transmission Control Protocol / Internet Protocol / Protocolo de Control de Transmisión / Protocolo de Internet.
VTR	Video Tape Recorder / Grabadora de Video.
BNC	Bayonet Neill-Concelman / Bayoneta Neill-Concelman.
UTP	Unshielded Twisted Pair / Par Trenzado sin Blindaje.
TVI	Transport Video Interface / Interfaz de Transporte de Video.
CVI	Composite Video Interfase / Interfase de Video Compuesto.
SDI	Serial Digital Interface / Interfaz Serie Digital.

MPEG-4 Moving Picture Experts Group 4 / Grupo de Expertos en Imágenes en Movimiento 4.

MJPEG Motion Joint Photographic Experts Group / Grupo de Expertos de Articulación de Imágenes en Movimiento.

NVR Network Video Recorder / Grabador de Video en Red.

RJ45 Registered Jack 45 / Jack Registrado 45.

Khz Kilo Hertz / Kilo Hercio**.**

STP Spanning Tree Protocol / Protocolo de Arbol de Expansión.

CAPÍTULO 3:

CCTV Closed Circuit Television / Circuito Cerrado de Televisión.

IP Internet Protocol / Protocolo de Internet.

TCP/IP Transmission Control Protocol / Internet Protocol / Protocolo de Control de Transmisión / Protocolo de Internet.

DVR Transmission Control Protocol / Internet Protocol / Protocolo de Control de Transmisión / Protocolo de Internet.

WiFi Wireless Fidelity / Fidelidad Inalámbrica.

IR Infrared Radiation / Radiación Infrarroja.

ONVIF Open Network Video Interface Forum / Foro de Interfaz de Video en Red Abierta.

LED Light Emitting Diode / Diodo Emisor de Luz.

CMOS Complementary Metal Oxide Semiconductor / Semiconductor de Óxido de Metal Complementario.

NAS Network Attached Storage / Almacenamiento Conectado a la Red.

HTTPS Hyper Text Transfer Protocol Secure / Protocolo de Transferencia de Hipertexto Seguro.

ARP Address Resolution Protocol / Protocolo de Resolución de Dirección.

RTSP Real Time Streaming Protocol / Protocolo de Transmisión en Tiempo Real.

RTP Real Time Transport Protocol / Protocolo de Transporte en Tiempo Real.

UDP User Datagram Protocol / Protocolo de Datagrama de Usuarios.

SMTP Simple Mail Transfer Protocol / Protocolo Simple de Transferencia de Correo.

FTP File Transfer Protocol / Protocolo de Transferencia de Archivos.

DHCP Dynamic Host Configuration Protocol / Protocolo de Configuración de Huésped Dinámico.

DNS Domain Name System / Sistema de Nombres de Dominio.

DDNS Dynamic Domain Name System / Sistema de Nombres de Dominio Dinámico.

NTP Network Time Protocol / Protocolo de Tiempo de Red.

UPnP Universal Plug and Play / Conestor y Reproductor Universal.

PSIA Physical Security Interoperability Alliance / Alianza de Interoperabilidad de Seguridad Física.

CGI Common Gateway Interface / Interfaz de Entrada Común.

BLC Back Light Compensation / Compensación de Luz de Fondo.

HLC High Light Compensation / Compensación de Luz Alta.

WDR Wide Dynamic Range / Amplio Rango Dinámico.

DNR Digital Noise Reduction / Reducción de Ruido Digital.

NVR Network Video Recorder / Grabador de Video en Red.

GOP Group Of Pictures / Grupo de Imágenes.

ROI Region Of Interest / Región de Interés.

DMSS Digital Mobile Surveillance System / Sistema de Vigilancia Móvil Digital.

ANR Automatic Network Reset / Reinicio Automático de la Red.

HDMI High Definition Multimedia Interface / Multimedia de Interfaces en Alta Definición.

VGA Video Graphics Array / Matríz de Gráficos de Video.

LAN Local Area Network / Red de Área Local.

AP Access Point / Punto de Acceso.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Wilson Alejandro Madrid Pacheco**, con C.C: # **0704237163** autor/a del trabajo de titulación: **Diseño de un sistema de seguridad CCTV mediante una red WIFI para el monitoreo y control en el edificio de la Gobernación de la Provincia de El Oro,** previo a la obtención del título de **Magíster 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, 9 de noviembre de 2020

Wilson Alejandro Madrid Pacheco

C.C: 0704237163

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN		
TÍTULO Y SUBTÍTULO:	Diseño de un sistema de seguridad CCTV mediante una red WIFI para el monitoreo y control en el edificio de la Gobernación de la provincia de El Oro	
AUTOR(ES)	Wilson Alejandro Madrid Pacheco	
REVISOR(ES)/TUTOR	MSc. Edgar Quezada Calle; MSc. Luis Córdova Rivadeneira / MSc. Manuel Romero Paz	
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil	
FACULTAD:	Sistema de Posgrado	
PROGRAMA:	Maestría en Telecomunicaciones	
TITULO OBTENIDO:	Magister en Telecomunicaciones	
FECHA DE PUBLICACIÓN:	9 de noviembre de 2020	**No. DE PÁGINAS: 100**
ÁREAS TEMÁTICAS:	Redes Inalámbricas, Estándar Inalámbrico IEEE 802.11, Seguridad en redes WiFi, Sistema de Seguridad de Circuito Cerrado de Televisión, Diseño de un Sistema CCTV	
PALABRAS CLAVES/ KEYWORDS:	WLAN, CCTV, DVR, Cámara de Video Vigilancia, Switch, WiFi	
RESUMEN/ABSTRACT: El presente proyecto se enfoca en el diseño de un sistema de seguridad de circuito cerrado de televisión CCTV para el monitoreo y control de las actividades diarias que se desarrollan en el edificio donde funciona actualmente la Gobernación de la Provincia de El Oro, utilizando cámaras con protocolo IP que manejan estándares de tecnología inalámbrica para monitorear las oficinas, pasillos y demás departamentos u oficinas en el edificio. La comunicación entre los equipos que conforman el sistema de seguridad CCTV se la realizará mediante una red Wireless, la cual estará conformada mediante dispositivos de Puntos de Acceso (Access Point); es decir equipos que utilizan radiofrecuencia a través de antenas omnidireccionales. Además, estos equipos que pertenecerán a la red Wifi podrán ser usados para que determinados funcionarios puedan tener acceso o salida al internet. El capítulo 1, describe las generalidades del proyecto donde se justifica la propuesta de innovación tecnológica ante un problema palpable dentro de la Institución. El capítulo 2, describe una fundamentación teórica amplia e investigativa correspondiente a los sistemas de circuito cerrado de televisión CCTV y a las tecnologías inalámbricas, sirviendo como herramientas de control, monitoreo y seguridad. El capítulo 3, describe la parte física y el diseño de un sistema de circuito cerrado de televisión CCTV a través de una red Wifi, considerando su funcionalidad basada en la seguridad. Finalmente, se presentan las conclusiones y recomendaciones que surgen de este proyecto.		
ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO AUTOR/ES:	**Teléfono:** +593-986726250	**E-mail:** wamp_86@outlook.com
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	**Nombre:** Romero Paz Manuel de Jesús **Teléfono:** +593-994606932 **E-mail:** manuel.romero@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):		