



**“UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA”
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE TELECOMUNICACIONES**

**TRABAJO DE INTEGRACION CURRICULAR PREVIO A LA
OBTENCION DEL TITULO DE:
INGENIERO EN TELECOMUNICACIONES**

**OPTIMIZACIÓN DE INFRAESTRUCTURAS DE VIGILANCIA CCTV
MEDIANTE LA INTEGRACIÓN DE SISTEMAS HÍBRIDOS Y
SEGURIDAD AVANZADA DE REDES WI-FI 802.11AC/N.**

AUTORES

**MOREIRA PIGUAVE MICHAEL ANDRÉS
PANCHANA LIMONES WASHINGTON FABIAN**

PROFESOR TUTOR

ING. LUIS MIGUEL AMAYA FARIÑO

LA LIBERTAD – ECUADOR

2024

DECLARACIÓN AUTORÍA DEL ESTUDIANTE

El presente trabajo de Integración Curricular con el título **“Optimización de infraestructuras de vigilancia cctv mediante la integración de sistemas híbridos y seguridad avanzada de redes Wi-Fi 802.11ac/n.”** Declaramos que la Concepción, análisis y resultados del trabajo presentado son originales y le dan un aporte importante a la actividad educativa dentro del área telecomunicación.

Atentamente,



Sr. Moreira Piguave Michael Andres

C.I. 0928705110



Sr. Panchana Limones Washington Fabian

C.I. 2400011173

DECLARACIÓN DE DOCENTE TUTOR

En mi calidad de Docente Tutor del Trabajo de Integración Curricular, **“Optimización de infraestructuras de vigilancia CCTV mediante la integración de sistemas híbridos y seguridad avanzada de redes Wi-Fi 802.11ac/n.”**, elaborado por los señores Moreira Piguave Michael Andrés y Panchana Limones Washington Fabian, estudiantes de la Carrera de Telecomunicaciones, Facultad de Sistema y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniería en Telecomunicaciones, me permita declarar que, tras supervisar el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos. En consecuencia, lo considero acto en todos sus aspectos y listo para ser evaluado por el docente especialista.

Atentamente,



Ing. Luis Amaya Fariño, Mgtr

DOCENTE TUTOR

DECLARACIÓN DE DOCENTE ESPECIALISTA

En mi calidad de Docente Especialista del Trabajo de Integración Curricular, **“Optimización de infraestructuras de vigilancia cctv mediante la integración de sistemas híbridos y seguridad avanzada de redes Wi-Fi 802.11ac/n.”**, elaborado por los señores Moreira Piguave Michael Andrés y Panchana Limones Washington Fabian, estudiante de la Carrera de Telecomunicaciones, Facultad de Sistemas y Telecomunicaciones de la Universidad Península de Santa Elena, previo a la obtención del título de Ingeniera en Telecomunicaciones, me permito afirmar que, tras supervisar el desarrollo y estructura final de su trabajo, este cumple con los estándares académicos requeridos. En consecuencia, lo considero apto en todos sus aspectos y listo para la sustentación del trabajo.

Atentamente,



Ing. Daniel Jaramillo Chamba, Mgtr

DOCENTE ESPECIALISTA

TRIBUNAL DE SUSTENTACION DE TRABAJO DE INTEGRACIÓN
CURRICULAR



Ing. Ronald Rovira Jurado, Ph.D
DIRECTOR DE LA CARRERA



Ing. Daniel Jaramillo Chamba, Mgtr
DOCENTE ESPECIALISTA



Ing. Luis Amaya Fariño, Mgtr
DOCENTE TUTOR GUIA UIC



Ing. Corina Gonzabay De la A, Mgtr
SECRETARIA

DECLARACIÓN DE RESPONSABILIDAD

Quienes suscriban, **Moreira Piguave Michael Andrés** con C.I. **0928705110** y **Panchana Limones Washington Fabian** con C.I. **2400011173**, estudiantes de la carrera de Telecomunicaciones, declaramos que el trabajo de Titulación presentado a la unidad de Integración Curricular cuyo tema es **“Optimización de infraestructuras de vigilancia CCTV mediante la integración de sistemas híbridos y seguridad avanzada de redes Wi-Fi 802.11ac/n.”**, corresponde y es de exclusiva responsabilidad de los autores y pertenece al patrimonio intelectual de la Universidad Estatal Península de Santa Elena.

Atentamente,



Sr. Moreira Piguave Michael Andres

C.I. 0928705110



Sr. Panchana Limones Washington Fabian

C.I. 2400011173

AGRADECIMIENTO

Agradezco en primer lugar a Dios, cuya fortaleza y bendición me han guiado en cada paso de este camino, ya que este logro no hubiera sido posible sin su presencia. A mis padres, José y Teresita, les dedico mi más profundo agradecimiento, desde la infancia ellos me enseñaron el valor de la perseverancia y me inspiraron a enfrentar cada reto con determinación. Su apoyo incondicional han sido una pieza fundamental para cumplir esta meta académica.

Expreso mi más sincero agradecimiento a quienes han sido fundamentales en la realización del presente proyecto. En primer lugar, al Ing. Luis Miguel Amaya Fariño, mi docente tutor, cuya guía y mentoría han sido esenciales a lo largo de este camino, también agradecer a todos los ingenieros que compartieron sus enseñanzas para mi crecimiento académicos, personal y profesional.

También un agradecimiento profundo a mis compañeros Joel, Fabian, Estefanía y demás compañeros que han estado a mi lado, que su apoyo y amistad fueron incondicional, han sido fuente de fortaleza y motivación constante a lo largo del recorrido académico.

Michael Andrés Moreira Piguave

En primer lugar, mi más profundo agradecimiento es para Dios, fuente de sabiduría, fortaleza y guía en cada paso de este camino. Desde el inicio de mi vida universitaria, su presencia ha sido un faro que me ha iluminado en los momentos más oscuros, dándome esperanza cuando la incertidumbre y las dificultades parecían insuperables. En cada logro, en cada desafío superado, siento su mano sosteniéndome, y por ello le doy gracias infinitas porque sin su amor y gracia nada de esto habría sido posible.

A mis padres, Washington y Marjorie, les debo todo lo que soy. su apoyo incondicional, no solo durante este proceso universitario, sino a lo largo de toda mi vida, me ha dado los valores y la perseverancia necesarios para alcanzar mis sueños. Estoy profundamente agradecido por las enseñanzas que me inculcaron desde pequeño, ya que gracias a ellos he podido superar cada obstáculo y cumplir las metas que me propuse, a mis Tíos Félix y Janena por brindarme la mano cuando no necesitada en su hogar.

Extiendo mi gratitud a mi tutor, el Ing. Luis Miguel Amaya Fariño, por su paciencia, dedicación y valiosa orientación, pilares fundamentales para el desarrollo de este trabajo. De igual manera, agradezco al Ing. Daniel Armando Jaramillo Chamba, por su constante seguimiento, aportes y sugerencias, que enriquecieron este proceso.

No puedo dejar de mencionar a mis compañeros, Michael Moreira y Joel Mateo, quienes, además de ser grandes amigos, fueron un pilar fundamental durante este proceso. Con su apoyo, solidaridad y aliento, me impulsaron a seguir adelante en los momentos de incertidumbre y fatiga. Su amistad y compañerismo fueron vitales para mantenerme motivada y enfocada en mis objetivos, y siempre me alentaron a no rendirme. A Katherine Villón, le doy también un especial agradecimiento, cuya motivación, ánimo y apoyo incondicional me ayudaron a mantenerme firme, su presencia y su confianza en mí me dieron la fuerza necesaria para culminar este trabajo.

Washington Fabian Panchana Limones

DEDICATORIA

Este trabajo se lo dedico a mis padres, Teresita Piguave y José Moreira, por todo su amor incondicional, por el apoyo incansable y por enseñarme que el esfuerzo, la constancia y la dedicación siempre dan frutos. Gracias por ser mis guías y mis pilares fundamentales en cada paso de este camino.

A mis abuelos, Olga Parrales y Hugo Piguave, cuya sabiduría y fortaleza me han mostrado el verdadero valor del trabajo duro, también le agradezco cada consejo, cada sonrisa que me brindaron en este proceso.

A mis hermanos y amigos y compañeros por ser una fuente de inspiración, por recordarme siempre la importancia de la unión y el compañerismo, ya que estuvieron ahí brindándome su cariño y motivación para superar cada desafío académico.

A mi amigo José, que hoy nos acompaña desde otro lugar, ya que su amistad y su apoyo fueron fundamentales en todo este camino y aunque no este físicamente, su recuerdo y sus enseñanzas están en cada página de este trabajo. Gracias por ser parte de mi vida y de este logro.

Y a todos ustedes les doy las gracias por ser mi razón y mi motivación para poder llegar hasta aquí con humildad y gratitud.

Michael Andrés Moreira Piguave

Dedico este trabajo con todo mi corazón a mi querida madre, Marjorie Limones, cuyo amor incondicional y sacrificio han sido la base de cada uno de mis logros. Gracias, mamá, por estar siempre a mi lado, por brindarme tu apoyo constante en cada etapa de mi formación académica, y por no dejarme solo incluso en las largas noches de desvelo. Tus esfuerzos y enseñanzas no solo han sido una guía para mí, sino también una fuente de inspiración que me acompañará por el resto de mi vida. Este logro es tan tuyo como mío, porque sin tu dedicación y cariño, este camino habría sido mucho más difícil de recorrer.

A mi padre, Washington Panchana, le dedico también este logro con todo mi agradecimiento. Gracias, papá, por ser ese apoyo firme en los momentos en los que más lo necesité, por tus palabras de aliento que me motivaron a seguir adelante y por tu ejemplo de trabajo y perseverancia. Siempre estaré agradecido por todo lo que has hecho por mí, por demostrarme que con esfuerzo y determinación se puede superar cualquier obstáculo.

A mis hermanos, Cristian, Jorge y Marjorie, quienes han sido mi mayor motivación y una fuente constante de fuerza. Su confianza en mí, sus palabras de ánimo y su apoyo incondicional me han impulsado a superar los desafíos que encontré en este camino. En cada momento difícil, su compañía y su fe en mi capacidad me recordaron que no debía rendirme, y por ello les estaré eternamente agradecido.

A mis amigos y compañeros, quiero expresarles mi más sincero agradecimiento. Ustedes, con su apoyo, su motivación y su camaradería, hicieron que este viaje fuera más llevadero. Sus gestos, sus palabras de aliento y su amistad fueron un refugio en los momentos de presión y dificultad, y su presencia en este proceso significó más de lo que las palabras pueden expresar.

Finalmente, dedico este trabajo a todo el personal que conforma la carrera de Telecomunicaciones. Gracias por todos los años de enseñanza, por compartir conocimientos que van más allá de los libros y por fomentar en cada uno de nosotros una pasión por el aprendizaje.

Washington Fabian Panchana Limones

RESUMEN

El proyecto se centra en la optimización de infraestructuras de videovigilancia mediante la integración de sistemas híbridos además de la seguridad avanzada en redes Wi-Fi 802.11ac/n. Este trabajo aborda la necesidad de implementar sistemas de vigilancia que combinen tecnologías cableadas e inalámbricas, destacando la importancia de la convergencia de canales en redes Wi-Fi para mejorar la seguridad y la calidad de transmisión en ambientes como laboratorios de telecomunicaciones, también se plantea un estudio que combina elementos de videovigilancia y redes de datos, buscando desarrollar una arquitectura de infraestructura híbrida que aproveche las fortalezas de cada tipo de tecnología.

Además, existen distintos tipos de sistemas CCTV ya que su evolución desde analógicos a digitales ha sido exponencial y la comparación entre cámaras analógicas e IP en términos de capacidad y accesibilidad remota. También se discuten aspectos técnicos fundamentales como la transmisión de datos mediante cable coaxial, UTP, fibra óptica, y las conexiones inalámbricas, así como el uso de estándares de compresión de video H.264 y H.265 que optimizan el almacenamiento y transmisión de imágenes.

En la generación del desarrollo del proceso de los elementos céntricos, así se va trabajando en la elaboración de una infraestructura híbrida, es decir la combinación de diferentes tipos de redes, dentro del laboratorio de Telecomunicaciones, una herramienta a utilizar es el software SketchUp, con el fin de lograr un diseño específico para su realización de fácil entendimiento.

Se concluye con el análisis de los dispositivos empleados, tales como las cámaras, el NVR, routers y las diferentes antenas, además, se empleó un sistema de inhibición de señales, también la generación de ruido por medio de la tecnología Radio definida por Software (SDR), con el fin de facilitar la valoración, así obteniendo la optimización del sistema de CCTV

Palabras claves: CCTV, Cámara, NVR, antena, doble banda, escenario.

ABSTRACT

The project focuses on the optimization of video surveillance infrastructures through the integration of hybrid systems in addition to advanced security in 802.11ac/n Wi-Fi networks. This work addresses the need to implement surveillance systems that combine wired and wireless technologies, highlighting the importance of the convergence of channels in Wi-Fi networks to improve security and transmission quality in environments such as telecommunications laboratories, a study that combines elements of video surveillance and data networks is also proposed. seeking to develop a hybrid infrastructure architecture that takes advantage of the strengths of each type of technology.

In addition, there are different types of CCTV systems since their evolution from analogue to digital has been exponential and the comparison between analogue and IP cameras in terms of capacity and remote accessibility. Fundamental technical aspects such as data transmission via coaxial cable, UTP, fiber optics, and wireless connections are also discussed, as well as the use of H.264 and H.265 video compression standards that optimize image storage and transmission.

In the generation of the development of the process of the central elements, thus work is being done on the development of a hybrid infrastructure, that is, the combination of different types of networks, within the Telecommunications laboratory, a tool to be used is the SketchUp software, in order to achieve a specific design for its realization of easy understanding.

It concludes with the analysis of the devices used, such as the cameras, the NVR, routers and the different antennas, in addition, a signal inhibition system was used, also the generation of noise by means of Software Defined Radio (SDR) technology, to facilitate the assessment, thus obtaining the optimization of the CCTV system

Keywords: CCTV, Camera, NVR, antenna, dual band, scenery.

INDICE DE CONTENIDO

INDICE

DECLARACIÓN AUTORÍA DEL ESTUDIANTE	ii
DECLARACIÓN DE DOCENTE DE DOCENTE TUTOR.....	iii
DECLARACIÓN DE DOCENTE ESPECIALISTA.....	iv
TRIBUNAL DE SUSTENTACION DE TRABAJO DE INTEGRACIÓN CURRICULAR v	
DECLARACIÓN DE RESPONSABILIDAD.....	vi
AGRADECIMIENTO	vii
DEDICATORIA.....	ix
RESUMEN	xi
ABSTRACT.....	xii
INDICE DE CONTENIDO	xiii
ÍNDICE DE ILUSTRACIONES	xvii
ÍNDICE DE TABLA.....	xxii
ÍNDICE DE ABREVIATURAS.....	xxiii
INTRODUCCIÓN	1
CAPITULO I.....	3
1. GENERALIDAD DE LA PROPUESTA.....	3
1.1 Antecedentes.....	3
1.2 Contextualización	3
1.3 Planteamiento del problema	4
1.3.1 Identificación de problema.....	4
1.3.2 Justificación de problema.....	4
1.3.3 Descripción del proyecto.....	6
1.4 Objetivo General	6
1.5 Objetivo Específicos.....	6
1.6 Metodología.....	7
1.7 Resultado Esperado	10
CAPITULO II.....	11
2.1 Marco teórico	11
2.2 Circuito cerrado de televisión CCTV	11
2.2.1 Sistemas CCTV analógicos.....	11
2.2.2 Sistemas CCTV digitales (IP)	12

2.2.3	Característica de los sistemas de circuito cerrado de televisión CCTV IP..	13
2.3	Equipos que compone un sistema CCTV	14
2.3.1	Adquisición de imagen.....	14
2.3.2	Conexión cableada	16
2.3.3	Almacenamiento de recursos	18
2.3.4	Control de video.....	20
2.4	Estándar de compresión de video	21
2.4.1	H.264.....	21
2.4.2	H.256.....	22
2.5	Redes	23
2.5.1	Redes inalámbricas.....	23
2.5.2	Redes alámbricas.....	24
2.5.3	Redes híbridas	24
2.6	Topologías de redes	25
2.6.1	Topología de anillo.....	25
2.6.2	Topología de Bus.....	25
2.6.3	Topología de Estrella.....	26
2.6.4	Topología de Árbol.....	26
2.6.5	Topología de Malla.....	27
2.6.6	Topología Híbrida	27
2.7	Estándares de comunicación.....	28
2.7.1	IEEE 802.3.x	28
2.7.2	IEEE 802.11.x	28
2.8	Protocolo de servidores	29
2.8.1	DNS.....	29
2.8.2	Hypertext Transfer Protocol (HTTP)	30
2.8.3	Hypertext Transfer Protocol Secure (HTTPS)	32
2.8.4	Real-time Streaming Protocol (RTSP)	33
2.8.5	Open Network Video Interface Forum (ONVIF)	34
2.9	Ataques a redes inalámbricas	36
2.9.1	Ataque pasivo.....	36
2.9.2	Ataque activo	36
2.9.3	Ataques cibernéticos	37
2.10	Tecnología SDR.....	38
2.11	Recurso de software.....	40

2.11.1	Python	40
2.11.2	Modelo de aprendizaje Yolov5	40
2.11.3	GNU radio.....	42
CAPITULO III.....		43
3.1	DESARROLLO DE LA PROPUESTA.....	43
3.1.1	COMPONENTES DE LA PROPUESTA FÍSICOS	43
3.1.1.1	NVR Reolink	43
3.1.1.2	Reolink color Cam 510w	45
3.1.1.3	Ubiquiti NanoStation	47
3.1.1.4	Ubiquiti Loco M2	50
3.1.1.5	Ubiquiti NanoStation Loco 5AC	51
3.1.1.6	LiteBeam 5AC Gen2	53
3.1.1.7	Router Tenda Tx2 wifi6	55
3.1.1.8	HackRF One	57
3.1.1.9	Transceiver.....	58
3.1.1.10	Cable UTP cat6	60
3.1.1.11	Fibra Drop.....	61
3.1.1.12	Conector mecánico SC.....	62
3.1.1.13	Amplificador de señal wifi EPUP-AB049 4000mW	63
3.2	DISEÑOS DE PROPUESTA EN SKETCHUP	65
3.2.1	Escenarios planteados 1	67
3.2.2	Escenarios planteados 2	74
3.2.3	Escenarios planteados 3	77
3.3	IMPLEMENTACIÓN DEL DISEÑO DE LA PROPUESTA	81
3.3.1	Configuración e instalación de NVR Reolink.....	81
3.3.5	Rendimiento de medios de transmisión	84
3.3.2	Implementación escenario 1	48
3.3.3	Implementación escenario 2.....	73
3.3.4	Implementación escenario 3.....	91
3.3.5	Implementación de código en Python	99
3.3.5.3	Desarrollo de un generador de ruido en GNU Radio.....	170
3.3.6	Propuesta de generador de ruido en 5GHz en GNU radio.	181
3.4	PRESUPUESTO.....	184
CAPITULO IV		185
4	Análisis de resultado obtenidos.....	185

4.1	Análisis de resultado obtenido del escenario.....	185
4.1.1	Análisis de Rendimiento mediante Test de Ancho de Banda para el Dispositivo LOCO M2.....	185
4.1.2	Análisis de Rendimiento mediante Test de Ancho de Banda para el Dispositivo NanoStation M2.....	186
4.1.3	Análisis de Transmisión de Video de la Cámara 1 (Conectada a LOCO M2) 187	
4.1.4	Análisis de Transmisión de Video de la Cámara 2 (Conectada a NanoStation M2) 187	
4.1.5	Análisis e interpretación de datos obtenido mediante código de seguimiento de objetivos.	188
4.1.6	Análisis e interpretación al utilizar un generador de ruido para redes WLAN 2.4GHZ.	190
4.2	Análisis de resultado obtenido del escenario 2.....	192
4.2.1	Análisis de rendimiento de la antena emisora LiteBeam 5AC.....	192
4.2.2	Análisis de Rendimiento de la antena receptora 1 Loco 5AC.....	193
4.2.3	Análisis de Rendimiento de la antena receptora 2 Loco 5AC.....	193
4.2.4	Análisis de Rendimiento y calidad de transmisión de video de la Cámara 1 194	
4.2.5	Análisis de Rendimiento y calidad de transmisión de video de la Cámara 2 195	
4.2.6	Análisis e interpretación de datos obtenido al ejecutar código de seguimiento de objetivos en tiempo real para frecuencia de 5GHZ	195
4.3	Análisis de resultado obtenido del escenario 3.....	198
4.3.1	Análisis e interpretación de datos obtenido mediante el medio de transmisión wireless.....	198
4.3.2	Análisis e interpretación de datos obtenido mediante el medio cableado UTP 207	
4.3.3	Análisis e interpretación de datos obtenido mediante el medio de fibra óptica 212	
4.4	Resultado obtenido al ejecutar código de distancia en base a círculos de referencia.....	216
	CONCLUSIONES GENERALES.....	218
	RECOMENDACIONES.....	219
	ANEXOS	220
	Anexos 1	220
	Anexos 2	221
	Anexos 3	226
	Referencias.....	227

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Circuito Cerrado de televisión CCTV.	11
Ilustración 2. Sistema CCTV de forma análoga.....	12
Ilustración 3. Sistema CCTV mediante componentes inalámbricos.	13
Ilustración 4. Cámaras analógicas.....	15
Ilustración 5. Cámaras con tecnología IP.....	15
Ilustración 6. Medio de transmisión por cable coaxial.	16
Ilustración 7. Medio de transmisión por cable UTP.....	17
Ilustración 8. Dispositivo de grabación DVR.	18
Ilustración 9. Dispositivo de grabación NVR.....	19
Ilustración 10. Arquitectura en forma anillo.	25
Ilustración 11. Arquitectura en forma bus.....	26
Ilustración 12. Arquitectura en forma estrella.....	26
Ilustración 13. Arquitectura en forma árbol.	27
Ilustración 14. Arquitectura en forma malla.	27
Ilustración 15. Arquitectura en forma híbridas.	28
Ilustración 16. Diagrama de bloque de la tecnología SDR.	39
Ilustración 17. NVR Reolink RLN12W.....	44
Ilustración 18. Cámara Reolink Color.....	46
Ilustración 19. Ubiquiti NanoStation M2.....	48
Ilustración 20. Ubiquiti NanoStation Loco M2.....	51
Ilustración 21. Ubiquiti NanoStation Loco 5AC.	52
Ilustración 22. Equipo LiteBeam 5AC Gen2.	54
Ilustración 23. Router Tenda Tx2 wifi6.	56
Ilustración 24. HackRF One.	58
Ilustración 25. Transceiver TP-link MS110CS.	59
Ilustración 26. Cable UTP Cat6.	60
Ilustración 27. Fibra drop de 2 hilos.	62
Ilustración 28. Conector Mecánico pulido SC.	63
Ilustración 29. Amplificador EP-AB049.....	64
Ilustración 30. Opciones de descargar para Sketchup.....	65
Ilustración 31. Pantalla de instalación de Sketchup.....	66
Ilustración 32. Instalación completada de sketchup.....	66
Ilustración 33. Pantalla de inicio de sketchup.....	67
Ilustración 34. Selección de espacio de trabajo dentro de Sketchup.....	68
Ilustración 35. Presentación de espacio de trabajo.....	68
Ilustración 36. Modelado de equipo utilizado dentro del modelado.	69
Ilustración 37. Réplica del laboratorio de la facsistel dentro de sketchup.	70
Ilustración 38. Elección del punto de instalación de la cámara para el punto 1.....	71
Ilustración 39. Ubicación de la última cámara.....	71
Ilustración 40. Ubicación del router y NVR Reolink dentro del Rack.	72
Ilustración 41. Conexiones del router hacia cada equipo.....	73
Ilustración 42. Visión panorámica de las ubicaciones de las cámaras y sus conexiones. .	74

Ilustración 43. Modelado de equipo a utilizar.....	74
Ilustración 44. Ubicación de la antena emisora y conexión de la antena mediante PoE. .	75
Ilustración 45. Ubicación de la primera antena receptora conjuntos a la primera cámara.	76
Ilustración 46. Ubicación de la segunda antena receptora conjunto a su cámara.	76
Ilustración 47. Conexión del router hacia la antena receptora y NVR.....	77
Ilustración 48. Vista panorámica de las ubicaciones de antenas en los alrededores del edificio de los laboratorios de Facsistel.	77
Ilustración 49. Modelado de equipos utilizado en el 3 escenario.....	78
Ilustración 50. Ubicación de la primera cámara y conexión mediante Transceiver.	79
Ilustración 51. Segunda ubicación en base a medio inalámbrico.....	79
Ilustración 52. Ultima ubicación median cableado UTP.....	80
Ilustración 53. Conexión del NVR hacia las diferentes cámaras.	80
Ilustración 54. Vista panorámica del desarrollo del tercer escenario.....	81
Ilustración 55. Configuración de parámetros generales del NVR.....	82
Ilustración 56. Parámetros de red del NVR	83
Ilustración 57. Habilitar y asignación de puertos del NVR	83
Ilustración 139. Descargar el archivo ffmpeg en formato ZI.	43
Ilustración 140. Carpeta ffmpeg lista para configurar el punto Path	44
Ilustración 141. Selecciones de Variables de entorno para entrar al apartado de PATH. ..	45
Ilustración 142. Agregar la ruta de FFmpeg dentro de PATH.....	45
Ilustración 143. Verificación de instalación de FFmpeg.....	46
Ilustración 58. Inicio de sesión en Router Tenda.	49
Ilustración 59. Direccionamiento de Gateway y su mascara.	50
Ilustración 60. Cambio de configuración de adaptadores de red del equipo portátil.	51
Ilustración 61. Parámetros de la red inalámbrica.....	52
Ilustración 62. Ingreso del navegador por IP de default.	52
Ilustración 63. Interfaz de inicio de equipo Ubiquiti Loco M2.....	53
Ilustración 64. Asignación de parámetros.....	54
Ilustración 65. Asignación de IP estática conjunto con puerta de enlace.....	55
Ilustración 66. Parámetros del equipo NanoStation M2 en el apartado Wireless.	56
Ilustración 67. Asignación de IP para el acceso al equipo y el acceso al internet.....	57
Ilustración 68. Asignación automática de IP dentro del router.	58
Ilustración 69. Ingreso mediante el navegador con la dirección IP.....	59
Ilustración 70. Inicio de sección e ingreso de credenciales de la cámara RLC-510WA. ..	59
Ilustración 71. Selección de la red Wi-Fi donde se conectará la cámara e ingreso de SSID y contraseña.	60
Ilustración 72. Cambio de configuración de red a estática.	61
Ilustración 73. Configuración de servidor y puerto de conexión.	63
Ilustración 74. Conexión establecida de la cámara y visualización de imagen.....	64
Ilustración 75. Proceso de instalación de la aplicación Reolink mediante la Play Store. .	64
Ilustración 76. Inicio de sesión de la aplicación Reolink y primeras configuraciones dentro.	65
Ilustración 77. Configuración de red Wi-FI mediante la aplicación Reolink.....	66
Ilustración 78. Verificación de información de la red y IP para posterior configuración..	67
Ilustración 79. Inicio de sesión mediante el navegador con la IP obtenida de la ilustración 78	68

Ilustración 80. Configuración de los servidores.....	68
Ilustración 81. Configuración de puerto de conexión.	69
Ilustración 82. Etiquetado de cableado desde el PoE.....	70
Ilustración 83. Resultado final de instalación de la primera cámara.....	71
Ilustración 84. Etiquetado de PoE correspondiente a la segunda ubicación.	72
Ilustración 85. Instalación final de la segunda cámara.	72
Ilustración 86. Cambio de protocolo IPv4 dentro del equipo portátil.....	74
Ilustración 87. Ingreso por medio del navegador por IP de default.	75
Ilustración 88. Inicio de sesión dentro del equipo.	75
Ilustración 89. Configuración en el apartado Wireless.	76
Ilustración 90. Asignación de IP dentro de la sección network.....	78
Ilustración 91. Conexión con el Wi-Fi del equipo para acceder a sus configuraciones.	79
Ilustración 92. Inicio de sesión en el equipo Loco 5AC.	80
Ilustración 93. Escaneo de señal emisora.....	80
Ilustración 94. Configuración restante dentro de Wireless.	82
Ilustración 95. Configuración del equipo en su apartado network.....	83
Ilustración 96. Enlace establecido entre los equipos.....	84
Ilustración 97. Asignación de IP dentro de la sección network.....	85
Ilustración 98. Verificación de estado de conexión entre la emisora y el punto b.	85
Ilustración 99. Cambio de red dentro a 5Ghz de la cámara RC-510WA	86
Ilustración 100. Etiquetado del Poe de antena emisora.....	88
Ilustración 101. Instalación de antena emisora.	88
Ilustración 102. Instalación completada correspondiente a la primera ubicación del escenario2.	89
Ilustración 103. Etiquetado de conexiones del PoE 2.	89
Ilustración 104. Etiquetado de conexiones del PoE 3.	90
Ilustración 105. Instalación completada correspondiente a la última ubicación del escenario2.	90
Ilustración 106. Configuración de red actualizado para 3° escenario.	92
Ilustración 107. Actualización de IP para la segunda cámara.	93
Ilustración 108. Actualización de conexión inalámbrica cámara 1.....	94
Ilustración 109. Actualización de conexión inalámbrica cámara 2.....	94
Ilustración 110. Ubicación de la primera cámara del último escenario.	95
Ilustración 111. Ubicación de la segunda cámara del último escenario.....	95
Ilustración 112. Instalación de cámara con medio de transmisión de cable UTP.....	96
Ilustración 113. Conexiones UTP de las cámaras en el NVR	96
Ilustración 114. Conexión del transceiver B para conectar a la cámara.....	98
Ilustración 115. Conexión entre el NVR y el Transceiver para la primera cámara.....	98
Ilustración 116. Conexión de la cámara 2 mediante UTP después de haber Utilizado el transceiver B.	98
Ilustración 117. Segunda conexión por medio de transceiver para la cámara 2.....	98
Ilustración 118. Proceso de instalación de Python.	99
Ilustración 119. Aceptación de termino en el proceso de instalación de Visual Studio Code.	100
Ilustración 120. Ubicación del Archivo Visual Studio Code.	100
Ilustración 121. Creación de acceso directo.....	101

Ilustración 122. Finalización del proceso de instalación.	101
Ilustración 123. Instalación de extensiones de Python dentro de visual studio code.	102
Ilustración 124. Instalación de librería OpenCV.	42
Ilustración 125. Instalación de librería Numpy.	167
Ilustración 126. Proceso de instalación de librería PyTorch.	168
Ilustración 127. Proceso de instalación de librería Pandas.	168
Ilustración 128. Instalación de Librería matplotlib.	168
Ilustración 129. Pantalla de inicio de GNU radio.	171
Ilustración 130. Diagrama de bloque del generador de ruido baso en redes WLAN de 2.4GHZ.	177
Ilustración 131. Configuración del bloque Options.	177
Ilustración 132. Configuración del bloque WX GUI Slider.....	178
Ilustración 133. Configuración del bloque WX GUI Chooser.....	179
Ilustración 134. Configuración del bloque Noise Source.	179
Ilustración 135. Configuración del bloque WX Fosphork Sink.....	180
Ilustración 136. Configuración del bloque Osmocon Sink.	180
Ilustración 137. Configuración del bloque WX GUI FFT Sink.	181
Ilustración 138. Esquema propuesto de conexiones física para el generador de ruido en 5Ghz.	182
Ilustración 144. Análisis de ancho de banda mediante test de velocidad.....	186
Ilustración 145. Estudio de ancho de banda mediante tes de velocidad en la antena NanoStation M2.	186
Ilustración 146. Visualización de cámara 1 sin interrupción de transmisión.	187
Ilustración 147. Visualización de cámara 2 con interrupciones en la transmisión.....	188
Ilustración 148. Visualización de ejecución de código de seguimiento en tiempo real. .	189
Ilustración 149. Ejecución del código de seguimiento en tiempo real en la cámara 2....	190
Ilustración 150. Ejecución de generador de ruido optimizado a antena emisora de cámara 1.	191
Ilustración 151. Verificación de intervención efectiva en la red.	191
Ilustración 152. Rendimiento de transmisión de antena emisora.....	193
Ilustración 153. Rendimiento de tasa de transmisión de la primera antena receptora. ...	193
Ilustración 154. Rendimiento de tasa de transmisión de la segunda antena receptora....	194
Ilustración 155. Visualización de cámara 1 desde el NVR mediante el radio enlace PTM.	194
Ilustración 156. Visualización de cámara 1 correspondiente al segundo escenario analizado	195
Ilustración 157. Visualización de ejecución del código de seguimiento en la banda de 5GHZ.	197
Ilustración 158. Visualización de ejecución del código de seguimiento en la banda de 5GHZ.	198
Ilustración 159. Captura de paquete mediante wireshark para banda de 2.4GHz.....	199
Ilustración 160. Captura de paquete mediante wireshark para banda de 2.4GHz en estándar H.265	200
Ilustración 161. Captura de paquete mediante wireshark para banda de 5GHz en estándar H.264.....	201
Ilustración 162. Captura de paquete mediante wireshark para banda de 5GHz en estándar H.265.....	201

Ilustración 163. Captura de paquete mediante wireshark por medio UTP.	207
Ilustración 164. Captura de paquete mediante wireshark por medio UTP en compresión H.265.....	208
Ilustración 165. Captura de paquete mediante wireshark por medio fibra óptica.....	212
Ilustración 166. Captura de paquete mediante wireshark por medio de fibra óptica en compresión H.265.....	213
Ilustración 167. Ejecución del segundo código de medición entres cámaras.	217

ÍNDICE DE TABLA

Tabla 1. Comparación entre protocolos y el Http	32
Tabla 2. Funciones básicas de un diagrama SDR.	39
Tabla 3. Especificaciones dada por el proveedor de NVR RLN12W.	44
Tabla 4. Especificaciones dada por datasheet de Reolink Color Cam.	46
Tabla 5. Ficha técnica de equipo Ubiquiti NanoStation.	48
Tabla 6. Valores de tasa de transmisión en base a la potencia de salida. Fuente:.....	49
Tabla 7. Ficha técnica de equipo Ubiquiti NanoStation Loco M2.	51
Tabla 8. Ficha técnica de equipo Ubiquiti NanoStation Loco 5AC.	52
Tabla 9. Ficha técnica de la antena LiteBeam 5AC Gen2.	55
Tabla 10. Ficha técnica de Router Tenda Tx2 wifi6.	56
Tabla 11. Ficha técnica del HackRF One.	58
Tabla 12. Ficha técnica del equipo Transceiver.	59
Tabla 13. Ficha técnica de cable UTP Cat6.	60
Tabla 14. Datos técnicos del conector mecánico.	63
Tabla 15. Tabla de datos técnico de amplificador.	64
Tabla 16. Inventario de equipos utilizado con respectivos usuario y contraseña.	72
Tabla 17. Inventario de equipos utilizado con respectivos usuario y contraseña del segundo escenario.	91
Tabla 18. Presupuesto para el desarrollo de la propuesta.	184
Tabla 19. Recurso utilizado del laboratorio de telecomunicaciones.	184
Tabla 20. Valores obtenidos de cálculo de latencia y retardo.	202
Tabla 21. Valor obtenido del análisis de ancho de banda mediante wireshark.	203
Tabla 22. Valores obtenidos para análisis de estabilidad.	1
Tabla 23. Valores obtenidos del cálculo de eficiencia de almacenamiento.	206
Tabla 24. Valores de ancho de bando de cableado UTP.	208
Tabla 25. Valores obtenidos para análisis de estabilidad del medio UTP.	211
Tabla 26. Valores obtenidos del cálculo de eficiencia de almacenamiento.	212
Tabla 27. Valores de ancho de bando de fibra óptica.	214
Tabla 28. Valores obtenidos para análisis de estabilidad del medio fibra óptica.	215
Tabla 29. Valores obtenidos del cálculo de eficiencia de almacenamiento en el medio de fibra óptica.	216

ÍNDICE DE ABREVIATURAS

AAC: Advanced Audio Coding - Codificación de audio avanzada.

ADC: Analog-to-Digital Converter - Convertidor de analógico a digital.

ADD: Add-drop multiplexer - Multiplexor de adición y eliminación.

AP: Access Point - Punto de acceso.

AVC: Advanced Video Coding - Codificación de video avanzada.

B&W: Black and White - Blanco y negro.

BSS: Basic Service Set - Conjunto de servicios básicos.

CCTV: Closed-Circuit Television - Circuito cerrado de televisión.

CGI: Common Gateway Interface - Interfaz de Puerta de enlace común.

CMOS: Complementary Metal-Oxide-Semiconductor - Semiconductor complementario de óxido metálico.

CPU: Central Processing Units - Unidad Central de Procesamiento.

CSMA/CD: Carrier Sense Multiple Access/Collision Detection - Detección de colisiones y acceso múltiple Carrier Sense.

CSTV: China Satellite Televisión - Televisión satelital de China.

DBI: Decibels Isotropic - Decibelios Isotrópicos.

DBM: Decibel Milliwatt - Decibelios Milivoltio

DCT: Discrete Cosine Transform - Transformada discreta de coseno.

DDC: Digital Down Converter - Convertidor digital hacia abajo.

DDOS: Distributed Denial of Service - Denegación de servicio distribuida.

DHCP: Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de host.

DNS: Domain Name System - Sistema de Nombres de Dominio.

DOS: Denial of Service - Denegación de servicio.

DS: Digital Signal - Señal digital.

DUC: Digital Up Converter - Convertidor digital ascendente.

DVR: Digital Video Recorder - Grabadora de video digital.

EP: End Point - Punto final.

FFT: Fast Fourier Transform - Transformada rápida de Fourier.

FPGA: Field-Programmable Gate Array - Matriz de puertas programables en campo.

FPS: Frames Per Second - Fotogramas por Segundo.

FTP: File Transfer Protocol - Protocolo de transferencia de archivos.

GBPS: Gigabits per Second - Gigabits por Segundo.

GHZ: Gigahertz - Gigahercios.

GNU: GNU's Not Unix

HD: High Definition - Alta definición.

HEVC: High-Efficiency Video Coding - Codificación de vídeo de alta eficiencia.

HTML: Hypertext Markup Language - Lenguaje de marcado de hipertexto.

HTTP: Hypertext Transfer Protocol - Protocolo de transferencia de hipertexto.

HTTPS: Hypertext Transfer Protocol Secure - Protocolo de transferencia de hipertexto Seguro.

IEEE: Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos.

IP: Internet Protocol - Protocolo de Internet.

ISO: International Organization for Standardization - Organización Internacional de Normalización.

ISP: Internet Service Provider - Proveedor de servicios de Internet.

LAN: Local Area Network - Red de área local.

LNA: Low Noise Amplifier - Amplificador de bajo ruido.

MAC: Media Access Control - Control de acceso a los medios.

MHZ: Megahertz – Megahercio.

MIMO: Multiple Input, Multiple Output - Múltiples Entradas, Múltiples Salidas.

MITM: Man in the Middle - Hombre en el medio.

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

NVR: Network Video Recorder - Grabadora de vídeo en red.

ONVIF: Open Network Video Interface Forum - Foro abierto de interfaz de vídeo en red.

PC: Personal Computer - Ordenador personal.

POE: Power over Ethernet - Alimentación a través de Ethernet.

PSK: Phase-Shift Keying - Modulación por desplazamiento de fase.

PTM: Point-to-Multipoint - Punto a Multi-Punto.

PTP: Point-to-Point - Punto a punto.

QOS: Quality of Service - Calidad de servicio.

RF: Radio Frequency – Radiofrecuencia.

RFC: Request for Comments - Solicitud de comentarios.

RTMP: Real-Time Messaging Protocol - Protocolo de mensajería en tiempo real.

RTSP: Real-Time Streaming Protocol - Protocolo de transmisión en tiempo real.

SD: Standard Definition - Definición estándar.

SDR: Software-Defined Radio - Radio definida por software.

SFP: Small Form-factor Pluggable - Factor de forma pequeño conectable.

SGV: Sistema de Gestión de Video

SLAAC: Stateless Address Autoconfiguration - Configuración automática de direcciones sin estado.

SQL: Structured Query Language - Lenguaje de consulta estructurado.

SSID: Service Set Identifier - Identificador de conjunto de servicios.

SSL: Secure Sockets Layer - Capa de sockets seguros.

TDMA: Time Division Multiple Access - Acceso múltiple por división de tiempo.

TDT: Televisión Digital Terrestre.

TLS: Transport Layer Security - Seguridad de la capa de transporte.

TV: Televisión.

TX: Transmit - Transmitir.

UHD: Ultra High Definition - Ultra alta definición.

UIT-T: Sector de normalización en telecomunicaciones de la Unión Internacional de Telecomunicaciones.

UNIX: Sistema operativo multiusuario y multitarea.

UNMS: Ultra High Definition - Ultra alta definición.

URL: Uniform Resource Locator - Localizador Uniforme de Recursos.

UTP: Unshielded Twisted Pair - Par trenzado sin blindaje.

VMS: Value Stream Mapping - Mapa de flujo de valor.

WAN: Wide Área Network - Red de Área Amplia.

WDR: Wide Dynamic Rang - Amplio Rango Dinámico.

WIFI: Wireless Fidelity - Fidelidad Inalámbrica.

WISP: Wireless Internet Service Provider - Proveedor Servicio de Internet.

WWW: Word wide web - Web Mundial.

INTRODUCCIÓN

Este proyecto se enfocó en la implementación de una infraestructura de videovigilancia a través de un sistema de circuito cerrado de televisión (CCTV), de manera híbrida donde estarán combinadas las redes cableadas al igual que las inalámbricas, para asegurar una correcta cobertura y transmisión en un entorno controlado como lo es el laboratorio de telecomunicaciones. Esta estrategia tecnológica tiene en consideración la creciente necesidad de seguridad por lo cual se propone la integración de nuevas soluciones para poder emplear las ventajas de las redes híbridas, mediante el uso de estándares avanzados en redes en específico el IEEE 802.11ac/n, esta infraestructura está diseñada para abordar las limitaciones de un sistema convencional de videovigilancia en el cual ofrecerá una cobertura más eficiente y robusta en diferentes escenarios que se planteen en el transcurso del proyecto.

El estudio realizado se fundamenta para conocer sobre sistema CCTV, en sus inicios han mejorado de manera exponencial los sistemas de cámaras de seguridad, anteriormente la tecnología que utilizaban estos sistemas solo era de manera analógica además, no poseían demasiada capacidad, en la actualidad con las nuevas generaciones de cámaras con las nuevas redes de conexión llegaron al mercado las cámaras digitales, la videovigilancia ha evolucionado mejorando las calidades de imágenes, así mismo dando una facilidad de poder controlarlas desde cualquier parte de la ciudad, provincia o país gracias al internet. Con estas tecnologías se incorporan grabadores de vídeo en red o en tiempo real llamados comúnmente (NVR), lo que permite una mayor capacidad de almacenamiento y gestión de la transmisión de vídeo.

Dentro de la propuesta, se observa el desarrollo de diferentes topologías de red que logran optimizar la distribución de los equipos, permitiendo una adecuada adaptación del sistema de video vigilancia de acuerdo con la disposición del espacio. Las topologías destacadas incluyen configuraciones tipo estrella, malla y estructuras híbridas, lo cual adecua soluciones ante eventuales desperfectos en un nodo como flexibilidad para futuras ampliaciones de la red. Por esta razón, se

considera la implementación de protocolos de transmisión seguros y eficientes que minimicen el riesgo de interferencias garantizando una transmisión estable en diferentes entornos controlados, un aspecto importante a tratar son las distintas programaciones de los sistemas de videovigilancia para diversos escenarios en cuestión, como el reconocimiento y medición de proximidad de objetos.

Así mismo, el proyecto analizará la eficacia de los medios de transmisión inalámbricos y alámbricos, que incluyen tanto a la fibra óptica como también al cable UTP, tomando en cuenta la capacidad para transmitir vídeo en tiempo real, en la correcta elección de los medios representa a la necesidad de equilibrio con el costo de la calidad de transmisión, garantizando que cada tecnología esté empleado con las características de un entorno controlado, con la mayor seguridad que requiere el caso..

CAPITULO I

1. GENERALIDAD DE LA PROPUESTA

1.1 Antecedentes

El primer uso de un circuito cerrado de televisión o CCTV se realizó en el año de 1942 por parte del ejército alemán. Pero en su momento los sistemas utilizados eran básicos en B&W ya que eran más utilizados para la observación de ensayos de misiles para ataques a gigantescas distancias [1].

En los tiempos para este sistema de circuito cerrado tendría que ser supervisado por el ente humano logre operar y que cumpla su función, en el año de los 60's esta actividad fue lo más común y dentro de eso a pasar los años hemos visto como locales, escuelas, empresas y banco son muy utilizados [1].

Estos circuitos cerrados o CCTV van a estar compuestos por dos o más cámaras de vigilancia, donde van a estar conectadas a televisores o monitores donde las imágenes serán presentadas a través de los dispositivos antes ya mencionados. Tomando en cuenta que siempre se va a poder actualizar todo el sistema [2].

Mediante las investigaciones que se han realizado a través del tiempo se procedió a explicar que la seguridad o CCTV ha experimentado grandes avances con las nuevas eras de digitalización, por tal motivo las nuevas tecnologías en las redes y en los sistemas de comunicación ya que han dado cabida a los videos de vigilancia IP, esto ayuda a muchos temas como lo son la seguridad y mantener el orden dentro de la zona delimitada [3].

1.2 Contextualización

Un sistema de videovigilancia es un conjunto de elementos que interactúan entre sí, la videovigilancia implica la instalación de cámaras en una red que es opción para guardar en grabadora digital o ver transmisión en vivo desde la pantalla el céntrico. El circuito cerrado de televisión, también denominado por las abreviaturas CCTV, es un sistema de vídeo vigilancia, dónde sus funciones están basadas en la transmisión y visualización de espacios con poco acceso en tiempo real, con la facilidad de poseer un control visual de manera remota. Su nombre proviene del hecho de que la transmisión de imágenes grabadas por cámaras de seguridad está destinada a un número limitado de pantallas o usuarios.

Un Circuito Cerrado de Televisión, también conocido como CCTV, es una de las tecnologías que se enfoca en la vigilancia por video que ha sido diseñada para monitorear diferentes lugares y actividades. Se le denomina "circuito cerrado" debido a que está destinado a ser visto únicamente por un número limitado de espectadores autorizados. Dentro del sistema de video vigilancia, el CCTV debe incluir cámaras, monitores y dispositivos de almacenamiento de video, los dispositivos que se usan para eso son los DVR (Digital Video Recorder) y NVR (Network Video Recorder). [4]

El control de las cámaras puede lograrse mediante hardware, como un teclado, o mediante software instalado en un ordenador. Además, estos sistemas de vigilancia por video pueden incorporar tecnologías complementarias, como reconocimiento facial o lentes teleobjetivo, que mejoran aún más el sistema.

Actualmente, los sistemas de CCTV (Circuito Cerrado de Televisión) se pueden encontrar en establecimientos comerciales, universidades, empresas públicas y privadas, e incluso en los hogares. La aplicación de este sistema es casi ilimitada no solo para la monitorización de salas, sino también para: sondas médicas y cámaras en miniatura, monitorización del tráfico, monitorización de procesos industriales o análisis facial. [5]

1.3 Planteamiento del problema

1.3.1 Identificación de problema

La falta de conocimiento sobre sistema basado en CCTV, ya que no se han enfocado en ampliar la base sobre el tema y sus derivaciones que posee tales como la infraestructura de red híbrida como también sus vulnerabilidades y sus aplicaciones a diferentes estándares.

1.3.2 Justificación de problema

En el aumento de los sistemas de seguridad de vídeo vigilancia (CCTV), tiene una exigencia de encontrar nuevas soluciones eficientes y peculiares en diversos contextos, en particular los laboratorios de telecomunicaciones requieren una solución de infraestructura de cámaras de vídeo vigilancia, con el fin de asegurar la seguridad y el control en los procesos de experimentación

Para sistemas de seguridad de cámaras o también conocidos como CCTV (Circuito Cerrado de televisión) poseen la cualidad de poder monitorear con ayuda de una pantalla externa para así captar las imágenes en tiempo real de las cámaras conectadas. Es uno de los sistemas necesarios en los lugares donde se necesite de supervisión o vigilancia ya sea para el cuidado de personas o de bienes. Es un sistema de vigilancia crucial que exigen una supervisión en lugares muy frecuentados donde la importancia de salvaguardar bienes o personas. Este sistema de CCTV tiene las habilidades y capacidades de poder adaptarse a la necesidad del cliente y sus circunstancias donde serán implementadas además, deja una cualidad de poder implementar una topología híbrida. [6]

Los ajustes en los canales 802.11 n/ac logran presentar diferentes obstáculos o desafíos sustanciales en la implementación y configuraciones de un sistema de CCTV, esto podría generar diferentes tipos de problemas en la transmisión de vídeo, dándonos como resultado una caída en la calidad de la imagen. Las configuraciones preinstaladas suelen dar lugar a una asignación automática de frecuencia o canal, esto puede restringir una correcta transmisión de datos, uno de los principales errores es la falta de conocimiento de los participantes sobre los canales más adecuados conectados a su red.

Así mismo es vital el ajustar los sistemas híbridos para poder gestionar la convergencia de los saltos del canal 802.11 n/ac, con el fin para asegurar una excelente calidad de transmisión de vídeo y una eficacia en las soluciones del sistema de CCTV.

De igual manera se debe de tomar en cuenta los ajustes del sistema híbrido ya que puede permitir una mayor adaptabilidad y escalabilidad en la implementación de soluciones frente a la infraestructura CCTV, puede ser relevante en diversos contextos en donde la videovigilancia es de manera eficaz y de excelente calidad, asimismo es pertinente para los mayores entendedores y expertos que buscan aplicar diferentes soluciones para los sistemas de CCTV, incluyendo los laboratorios de telecomunicaciones.

Los sistemas de videovigilancia con el paso de los años se han encargado de procesar información en video que suelen ser guardado en dispositivos externo como un NVR (Network Video Recorder) [7].

1.3.3 Descripción del proyecto

Para la elaboración de este proyecto va a adaptar sistemas híbridos para la implementación de una infraestructura CCTV que va a estar basada en la tecnología de convergencia en cambios de canales 802.11 ac/n.

Se sabe que los sistemas híbridos se enfocan en la combinación de tecnologías de cableado y tecnologías inalámbricas, así aprovechando las fortalezas de cada una para lograr una solución eficiente.

Para poder empezar con este proyecto se va a llevar a cabo un estudio exhaustivo de los sistemas híbridos existentes y de las tecnologías de convergencia en cambio de canales 802.11 ac/n. Esto va a incluir una revisión especializada, el análisis de casos de estudio y evaluación de las mejores prácticas e implementación de infraestructura CCTV.

A continuación, se va a proponer una arquitectura para la infraestructura CCTV híbrida adaptada que combine elementos de cableado e inalámbricos, se van a definir los componentes necesarios tales como cámaras de vídeo punto de acceso inalámbricos sistemas de almacenamiento y dispositivos de visualización para que este proyecto sea ejecutable.

Se va a realizar un diseño detallado de la infraestructura, considerando aspectos como la ubicación y distribución de las cámaras además la cobertura de la red inalámbrica, con eso la capacidad de almacenamiento y la integración del sistema de monitoreo centralizado.

1.4 Objetivo General

Adaptar sistemas híbridos para realizar una implementación en base a una infraestructura CCTV aplicando convergencia y seguridad en la topología esto aplicado al cambio de canales 802.11ac/n, realizado en los laboratorios de telecomunicaciones de la Universidad Estatal Península de Santa Elena.

1.5 Objetivo Específicos

- ✚ Diseñar la arquitectura de sistemas híbrido CCTV de manera detallada utilizando el software SketchUp para garantizar una implementación segura.
- ✚ Implementar el diseño propuesto mediante el equipamiento específico para incrementar la seguridad en las proximidades del laboratorio de telecomunicaciones.

- ✚ Adaptar escenarios propuestos utilizando adecuadamente el equipamiento, con el fin de analizar detalladamente dichos escenarios.
- ✚ Configurar eficazmente protocolos de regulación de saltos de frecuencia en bandas licenciadas para optimizar la utilización del espectro electromagnética.
- ✚ Elaborar un sistema de programación mediante software libre que facilite el cálculo y visualización de la cobertura entre 2 cámaras IP con el fin de identificar áreas y posibles zonas ciegas
- ✚ Desarrollar un sistema de inhibición de señales basado en tecnología (SDR), incorporando código específico en GNU Radio para identificar, intervenir y neutralizar eficazmente transmisiones basadas en el estándar de comunicaciones inalámbricas.
- ✚ Estudiar el funcionamiento práctico de los bloques de procesamiento de la tecnología SDR utilizando GNU radio.
- ✚ Analizar y evaluar las vulnerabilidades del ancho de banda en el sistema híbrido CCTV, cuál es el objetivo de incrementar y optimizar su rendimiento.

1.6 Metodología

En el desarrollo de este proyecto se tomó en cuenta utilizar los diferentes tipos de metodologías:

Metodología Exploratoria

Para el desarrollo de esta metodología se recopiló diversos repositorios académicos, artículos científicos, bibliografías, así obteniendo temas relacionados como: Implementación de Sistemas CCTV, Redes Híbridas, sistemas y monitoreos de centros CCTV mediante cámaras IP, Vulnerabilidades de los sistemas de videovigilancia, Uso de tecnología SDR, etc.

Metodología Experimental Aplicada

Como conocimiento general la metodología aplicada utiliza técnicas para resolver problemas específicos en los cuales busca mejorar la calidad de vida, este proyecto se basa en desarrollar un sistema de video vigilancia para garantizar la seguridad y el monitoreo de un ambiente controlado, como metodología aplicada se usará en

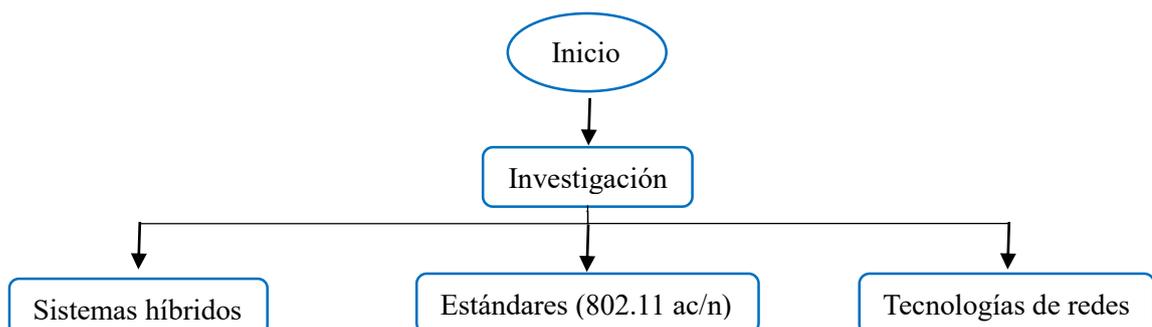
base al planteamiento de seguridad y control y en cómo se planificará para resolverlo en la cual se implementará las herramientas necesarias para solucionar cada etapa del problema.

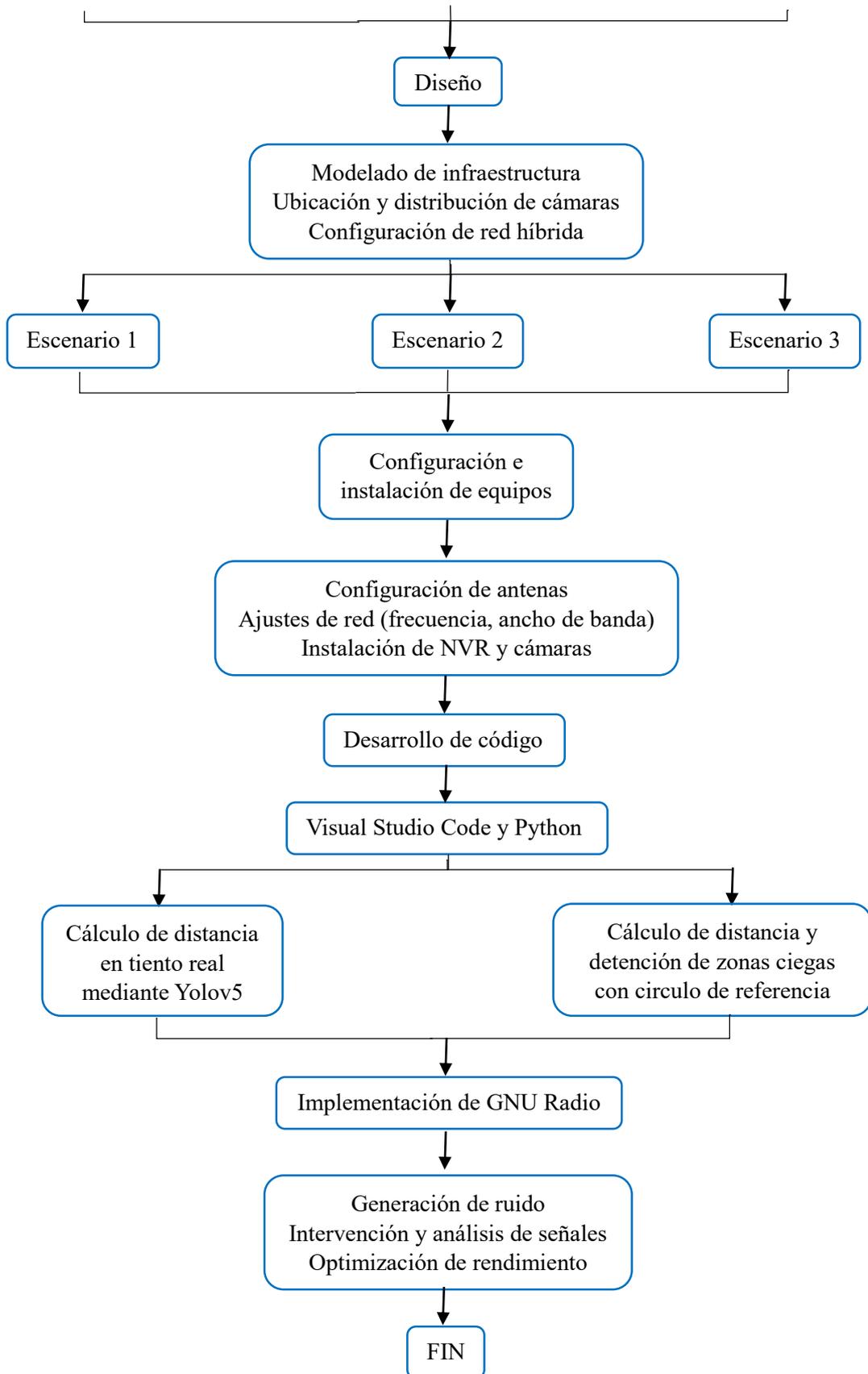
Este proyecto se enfocará en la implementación de una infraestructura híbrida de videovigilancia que se basará en sistemas CCTV por lo cual integrará tecnologías alámbricas e inalámbricas para lograr optimizar la seguridad y cobertura en entornos controlados en este caso sería el laboratorio de telecomunicaciones, como metodología aplicativa busca estudiar distintos métodos en los cuales permite seleccionar el más adecuado para determinar qué tipo de tecnología ya sea alámbrica e inalámbrica es la adecuada para llegar al resultado esperado.

Un método de gran ayuda para el progreso de este proyecto es la herramienta de SketchUp que permitirá crear modelos tridimensionales que representen el laboratorio y los equipos en el cual permite tener medidas y simulaciones que minimicen los errores para así asegurar la implementación eficiente por esta razón se instalarán equipos de cámaras Reolink, NVRs y routers en puntos estratégicos analizados mediante simulación basados en diferentes escenarios de uso.

Este tipo de metodología esta encargada de pautar procedimientos necesarios para realizar una indagación formal por lo cual esta metodología es una de las más utilizadas ya que es eficaz y asegura que la indagación sea coherente y que sus resultados sean precisos, por consiguiente debido a la aplicación de este método se conseguirá una mayor seguridad y eficiencia en la transmisión de datos mediante la convergencia de canales Wi-Fi, se identificará los puntos ciegos además de lograr optimizar el posicionamiento de las cámaras en conjunto con un análisis detallado de un ancho de banda y rendimiento de los medios de transmisión a utilizar.

Diagrama de Flujo de la propuesta tecnológica





1.7 Resultado Esperado

El desarrollo de la propuesta de implementar una infraestructura híbrida dentro de un sistema CCTV en los laboratorios de telecomunicación, esperando obtener los siguientes resultados significativos que demuestren la viabilidad y eficiencia de la solución propuesta.

-  Analizar el costo de los equipos a utilizar dentro del proyecto para poder así mantener un presupuesto correcto.
-  Con el diseño preciso y detallado de una arquitectura del sistema híbrido CCTV, una visualización tridimensional clara y comprensible del desarrollo propuesto identificar y mitigar el de posibles problemas de implementación.
-  Implementar una red híbrida para las conexiones de las antenas con el propósito de mantener la conectividad en tal caso que suceda fallos en algunas de ellas, así asegurando una comunicación interrumpida y eficiente.
-  Realizar un estudio de las diferentes tecnologías de redes híbridas disponible, para posterior seleccionar la mejor opción que se acople en la realización de este proyecto.
-  Analizar y comparar las distintas de localización de las cámaras de vigilancia con el fin de calcular la pérdida de comunicación.
-  Obtener un cálculo preciso de la cobertura de las cámaras y poder tener una visualización intuitiva de las áreas cubiertas y las zonas ciegas.
-  Llevar a cabo un análisis de las posibles interferencias en la infraestructura de la red mediante el uso de dispositivo generador de ruido.
-  Establecer nuevas ideas para nuevos conocimientos para futuras implementaciones o investigaciones similares a este proyecto.

CAPITULO II

2.1 Marco teórico

2.2 Circuito cerrado de televisión CCTV

Los sistemas que son encaminador en la gestión de video (SGV), son conocidos como CCTV es un acrónimo al referirse a “Closed Circuit Television” que al traducirlo se conoce como “Circuito Cerrado de Televisión”. Es un sistema en base en la transmisión y visualización de imágenes en movimiento con la finalidad de controlar y supervisar.

El sistema puede estar configurado con una o más cámaras de seguridad, que se conectan a uno o varios monitores o televisores para visualizar las imágenes capturadas. Estas imágenes poseen la opción de ser almacenadas al mismo tiempo en formatos analógicos o digitales, según las preferencias del usuario. Los elementos que componen este circuito incluyen cámaras, conmutadores matriciales analógicos y grabadores digitales. [8]

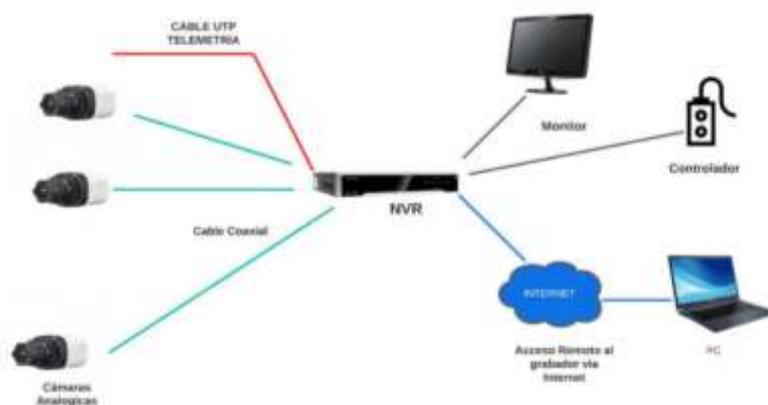


Ilustración 1. Circuito Cerrado de televisión CCTV.

Fuente: Elaboración propia.

En la actualidad, los sistemas de CCTV están presentes prácticamente en todas partes ya que son muy comunes en centros comerciales, edificios y mucho otros lugares. En el ámbito comercial, estos sistemas no solo se utilizan para prevenir robos, sino que también se aprovechan para diversos fines, como obtener evidencias de incidentes o combatir reclamaciones fraudulentas. [9]

2.2.1 Sistemas CCTV analógicos

Estos tipos de sistemas data sus orígenes en los años 50s, de lo cual para la época se usaba cable coaxial de 75 ohm. Se conoce por ser una conexión cableada de

varias cámaras, estos dispositivos en cuestión deben conectarse a un multiplexor para su alimentación, este multiplexor se encuentra ubicado en los cuartos de controles de las centrales. Es posible visualizar las imágenes en tiempo real utilizando varios monitores o único monitor como una función de cambio de cámaras para seleccionar la que se desea observar. [10]

El sistema cuenta con una capacidad de almacenamiento limitada, adecuada sólo para una pequeña cantidad de datos. Los costos asociados a la grabación de pequeños lapsos de video eran elevados, al igual que los datos relacionados con las instalaciones de estaciones de monitoreo. Además, la reubicación de cámaras representa un desafío de vídeo a la necesidad de realizar un tendido de cable completamente nuevo. [10]

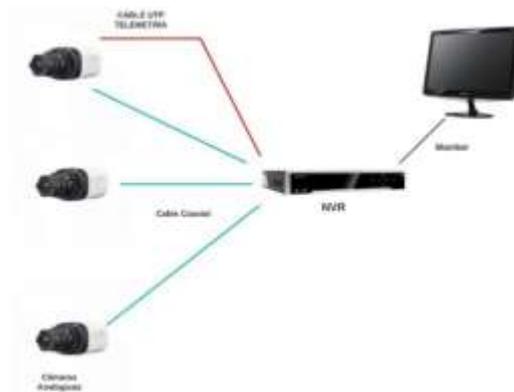


Ilustración 4. Sistema CCTV de forma analógica.

Fuente: Elaboración propia.

2.2.2 Sistemas CCTV digitales (IP)

En la siguiente fase en la transición del analógica digital es la vigilancia IP ofrece la posibilidad de mejorar significativamente. El rendimiento de las redes de datos en las empresas como ya que permite transportar vídeos y audios a través de la misma infraestructura de la red de datos. [11]

Es posible configurar las cámaras de red y los codificadores para acceder a ellos de manera remota, lo que habilita a distintos usuarios autorizados para visualizar video en tiempo real y grabaciones en cualquier ubicación conectada a la red, sin importar su lugar en el mundo, uno de los equipos que llegó junto con ese sistema es el NVR el cual nos permitirá el almacenamiento y transmisión lo cuales se podrá ver en tiempo real en base a la red de datos que esté conectado este sistema. [11]



Ilustración 7. Sistema CCTV mediante componentes inalámbricos.

Fuente: Elaboración propia.

2.2.3 Característica de los sistemas de circuito cerrado de televisión CCTV IP

La característica y funcionalidad que tiene un sistema CCTV en base a tecnología IP se mencionaran a continuación:

- **Accesibilidad remota:** El avance de las tecnologías en base a protocolos IP, se ha logrado utilizar una función que permite a los usuarios autorizados acceder y visualizar contenido en tiempo real desde cualquier rincón que se encuentra simplemente conectándose a una red de internet. esta característica ha transformado la forma de interactuar con información y nos brinda una nueva perspectiva para la gestión y monitoreo de datos visuales. [12]
- ✚ **Procesamiento digital de imagen:** Esta característica nos permite realizar grabaciones programas basada en eventos como la detención de movimientos o señales externos de sistemas de alarma, además, esta tecnología. Evita la subjetividad del ojo humano a las 3 automáticamente en tiempo real la información pertinente solicitada esto facilita considerablemente el trabajo del operador alta en acceso a datos más precisos y relevante de la grabación.
- ✚ **Infraestructura de la red:** Un sistema de CSTV pasado en la tecnología IP aprovecha el cableado estructurado la red y no requiere de instalaciones específicas para su alimentación, ya que aprovecha la tecnología PoE (Power Over Ethernet). Además, las redes IP Tanto como cableadas como las inalámbricas son opciones más económicas a comparación del cableado

coaxial o de la fibra óptica que se han utilizado en la parte de sistemas analógicos ya que estos necesitarán una fuente de alimentación externa.

2.3 Equipos que compone un sistema CCTV

Es el procedimiento de poder capturar o recolectar contenido audiovisual de manera en tiempo real, mediante el uso de los dispositivos externos tales como cámara, escáner u otros dispositivos, la precisión de la calidad en la obtención de las imágenes ya que son elementos fundamentales para garantizar una supervisión eficaz y fiable.

2.3.1 Adquisición de imagen

El accidente de imagen nos referimos al proceso en el cual se encarga de capturar o recopilar imágenes visuales En tiempo real utilizando dispositivos externos como cámara, escáner u otros dispositivos. La calidad y precisión de la adquisición de imagen son aspectos fundamentales para garantizar una vigilancia efectiva y confiable.

2.3.1.1.1 Cámara analógica

Las cámaras análogas son conocidas por su extraordinaria facilidad de uso, pues no implican la necesidad de configuraciones complicadas como administración, direcciones IP, programación o software adicional. Así mismo, se destacan por ofrecer una resolución más baja en comparación con otras alternativas tecnológicas. Esta simplicidad en su funcionamiento las convierte en una opción accesible y práctica para aquellos que buscan una solución de videovigilancia sin complicaciones. A pesar de su menor resolución, estas cámaras aún pueden cumplir con eficacia funciones básicas de vigilancia en diversos entornos. [13]

Una característica importante de estas cámaras es que utilizan una conexión punto a punto para transferir la información al video grabador a través de un cable coaxial. Actualmente, se pueden utilizar adaptadores de impedancia para transmitir tanto el voltaje de alimentación (12V C.C) como el video obtenido por la cámara. [14]

A diferencia de las cámaras digitales, el tráfico de video analógico no está expuesto a riesgos de la red. Además, estas cámaras son perfectamente compatibles con los DVR sin requerir adaptaciones o incompatibilidades.



Ilustración 10. Cámaras analógicas

Fuente: Elaboración propia.

2.3.1.1.2 Cámaras IP

Las cámaras IP o también conocida como cámaras de Red, Son dispositivos que se interconectan a través de internet con la finalidad de transmitir vídeo en una alta definición. Estos dispositivos suelen ser económicos, de instalación y mantenimiento accesibles. Además, Cuenta con la habilidad de poder conectarse a un ordenador o cualquier dispositivo móvil lo que nos permite tener la información en cualquier momento y lugar. [15]

Son cámaras de vídeos digitales que mediante las conexiones de un switch o router en un área local (LAN) con acceso al internet son posibles permitir las transmisión y recepción de información de vídeo. Estos equipos cuentan con CPU propio Tiene transformar en microcomputadoras autónomas gracias a listo les permite procesar De manera independiente a la información. [16]



Ilustración 13. Cámaras con tecnología IP

Fuente: Elaboración propia.

Medios de transmisión

En la actualidad, existen diversas opciones de medios de transmisión uno de ellos el más sencillo tenemos el cable coaxial, el cual es comúnmente utilizado en sistemas CCTV de corto alcance. Sin embargo, para aplicaciones que requiera una mayor tasa de transmisión de datos se recurre a la fibra óptica ya que es un medio

que posibilita la transmisión de tasa de información mucho más grande sin tener ningún retraso en la comunicación. En situaciones donde el topografía e infraestructura limita la instalación de fibra óptica, se suele optar por implementar sistemas inalámbricos como una alternativa a estos casos. [17]

2.3.2 Conexión cableada

2.3.2.1 Cable de coaxial

La conexión promedio de cable coaxial consiste en un número de conductores de cobre que rodea una malla de hilo del mismo material. Entre dos conductores se encuentra un conductor de plástico que su función es de separar y mantener sus propiedades eléctricas con el fin de evitar cualesquiera emisiones de energía ya que todo el cable se cuenta recubierta con protectores de aislamiento para que no suceda problemas. [18]

Dentro de los sistemas de CCTV, el medio de transmisión en este caso siendo el cable coaxial que nos permite transmitir las señales de vídeo análogas, de igual forma este medio es comúnmente utilizado para la distribución de señales de televisión, así brindando un servicio en casas, edificios y residencias, incluyendo el uso de los sistemas de vídeo vigilancia y la programación de televisión por cable, también el cable coaxial logra transmitir frecuencias de radio y muchas aplicaciones más.. [15]



Ilustración 16. Medio de transmisión por cable coaxial.

Fuente: [15]

2.3.2.1.1 Cable UTP

El cable Utp o también parte par trenzado el cual se encuentra construido en ocho hilos de cobre aislado, agrupando emparejos y trenzado. Esta disposición se realiza con la finalidad de evitar que los dos alambres con una antena simple, lo que podría generar interferencia. al trenzar los alambres las ondas se cancelan entre sí esto hace que la interferencia es disminuya y lo que permita que la tasa de transmisión de datos sea más eficiente. [19]

Frecuentemente empleado en comunicaciones telefónicas y en las más avanzadas conexiones Ethernet, el tipo más comúnmente utilizado es el cable UTP. Este se compone de cuatro pares de hilos conductores de cobre que se cruzan entre sí con el propósito de disminuir las interferencias electromagnéticas que puedan surgir en un canal de comunicación o causar atenuación de la señal. Estos pares de hilos habilitan la transmisión de señales de video, datos, audio o incluso corriente a través del mismo cable. [20]

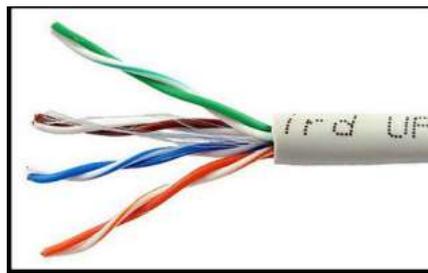


Ilustración 19. Medio de transmisión por cable UTP.

Fuente:[20]

2.3.2.2 Conexión Inalámbrica

La vinculación se efectúa mediante las líneas de la infraestructura de cableado estructurado, con el propósito de llevar a cabo la transferencia de datos y energía. Esto conlleva a la reducción de los gastos relacionados con la instalación de redes suplementarias necesarias en los sistemas analógicos tradicionales. Este modo de suministro es conocido como PoE (siglas en inglés de Power over Ethernet). La potencia proporcionada se encuentra regulada por la norma IEEE 802.3af. [21]

Las cámaras IP a menudo emplean los estándares 802.11g/b/n para su funcionamiento. Las versiones b y g utilizan el espectro de frecuencia de 2,4-2,5 GHz. Los dispositivos inalámbricos que se utilizan para establecer conexión con otros dispositivos similares son el Punto de Acceso (AP) y el Punto de Extensión (EP). Los AP, por lo general, poseen la función principal de facilitar la conectividad a la red, mientras que la tarea de enrutamiento y direccionamiento recae en servidores, routers y switches. Por otro lado, los AP amplían el alcance de la red inalámbrica al retransmitir las señales entre un equipo o Punto de Acceso y otro punto de extensión. La cobertura de estos dispositivos depende de los obstáculos presentes, como edificios, paredes y puertas, pero suele ser de alrededor de 100 metros en interiores y 300 metros en exteriores. [22]

2.3.3 Almacenamiento de recursos

En el almacenamiento de los recursos implica reconocer múltiples recursos vinculado a la conversión de dispositivo de grabación ya la calidad de imagen que son proporcionados mediante una cámara de vídeo. En esta sección sea abarcará la relación entre la resolución y el tamaño digital del archivo, se examinará las capacidades de grabador que imponen restricción de al almacenamiento.

2.3.3.1.1 DVR

El Sistema DVR debe contar con una entrada analógica para cada cámara que haya sido instalada. La resolución de la imagen depende de cómo el DVR digitaliza la señal del video compuesto, y también de las condiciones técnicas de la cámara, como el tipo de lente, el iris (fijo o automático), el balance de blancos, el control de ganancia, WDR, entre otros factores. La transmisión se efectúa mediante un cable coaxial. Es el propio DVR el que establece el límite de cuadros por segundo (FPS) con los cuales generará y registrará el video digital. Los DVR pueden realizar la compresión tanto por software como por hardware.

El DVR tiene la capacidad de conectarse a la red, lo que permite la visualización de las grabaciones desde cualquier PC que esté conectado a esa red. Los datos en formato digital se desplazan comprimidos en formatos de compresión ampliamente utilizados (como MPEG, MPEG4 y H.264), de manera similar a como ocurre en una instalación de CCTV IP. [23]



Ilustración 22. Dispositivo de grabación DVR.

Fuente: Elaboración propia.

2.3.3.1.2 NVR

La abreviatura NVR representa "Network Video Recorder" en inglés, o "Grabador de Video de Red" en español. Este dispositivo físico o software que se instala en una computadora guarda similitudes con un DVR, con la distinción de que el DVR digitaliza, graba y gestiona las imágenes provenientes de cámaras de seguridad

analógicas. Por el contrario, un NVR registra y administra imágenes que ya son digitales, estas son transmitidas desde cámaras IP a través de una red. [8]

Una de las fortalezas distintivas del NVR en comparación con el DVR es su capacidad para emplear imágenes digitales que han sido comprimidas previamente por las cámaras IP. Estos archivos por lo general están comprimidos para posteriormente ser enviados al NVR, esto conlleva a la disminución de manera notable del peso sobre el procesamiento que ejerce sobre la unidad central de procesamiento también conocido como (CPU). [18]

Estos rasgos ofrecen un gran avance evidente del desempeño y la eficacia del sistema hablado, una cosa muy importante es recalcar que facilita una gestión o administración del contenido audiovisual que son recolectados por las cámaras IP, por lo tanto se logrará una mejora en el tráfico de datos ya que reduce la carga laboral del CPU, dando como resultado un sistema veloz y eficaz en la gestión de la vigilancia y el almacenamiento. [24]



Ilustración 25. Dispositivo de grabación NVR

Fuente: [24].

2.3.3.1.3 NVR con conexión cableada

Un NVR de conexión cableada (Network Video Recorder) es un dispositivo que utiliza una conexión física con cable para grabar y administrar cámaras de seguridad en una red de área local (LAN). Los NVR son responsables de recibir y almacenar secuencias de video de cámaras de seguridad en varios lugares, como oficinas, almacenes o espacios al aire libre, utilizando conexiones Ethernet y cables de red. La conexión por cable también puede proporcionar más capacidad de ancho de banda que una conexión inalámbrica, lo cual es esencial para capturar y ver videos de alta definición y controlar de manera efectiva varias cámaras.

Frecuentemente el equipo NVR tienen incorporados puertos ethernet o más conocido como puertos de Power over ethernet (PoE), una cualidad es que la energía y la transmisión de datos pasan por un solo medio de transmisión llamado cable UTP lo que proporciona una fácil instalación.

2.3.3.1.4 NVR inalámbrico

El NVR también llamado (network video recorder) es un equipo plenamente utilizado para registrar, gestionar y guardar contenido audiovisual desde las cámaras de seguridad de manera inalámbrica, uno de los puntos más importante es que este enlazada con una red de área local ya sea por Wi-Fi o una red LAN. En contraste con los NVR convencionales, estos necesitan una conexión de cable de manera física ocupando mayor espacio, los NVR inalámbricos permiten una conexión de inalámbrica pero eficaz con las cámaras de seguridad

El dispositivo NVR inalámbrico tiene la particularidad de lograr trabajar con señales de radiofrecuencia además de realizar el debido procesamiento del contenido audiovisual que brinda las cámaras IP, también ofrece un soporte de adaptabilidad en la localización donde las cámaras serán ubicadas con el fin de reducir la cantidad de cables, la comunicación por la que transmiten las cámaras IP pueden ser a través de una conexión inalámbrica hacia el dispositivo NVR dónde se registrarán todo las grabaciones para su uso posterior según el caso lo amerite..

2.3.4 Control de video

El control de videovigilancia está relacionado con la acción de permitir controlar y vigilar imágenes en movimiento y de manera estáticas que son capturadas en tiempo real, todo mediante cámaras de videovigilancia junto a diversos dispositivos que logran realizar capturas visuales, este estudio realizado de manera experimental se pueden ser utilizados en diversos entornos con funcionalidades distintas, como la vulnerabilidad, custodia, inspección de procesos.

Dentro del monitoreo en proceso donde visualizado por operadores de seguridad, personal de control de calidad, administradores de redes, entorno personal de un individuo.

El monitoreo de video puede incluir funciones como:

- Vigilancia de seguridad: Ayuda a tener vigilancia en áreas restringidas, lugares de multitudes y para usos comerciales.
- Control de procesos: : Analiza la supervisión de diversos procesos tanto en áreas administrativas, industrias y sistemas mecanizados.
- Tráfico y transporte: Para poder gestionar y observar el flujo de tráfico en las calles, avenidas, con el fin monitorear eventos de congestión

vehicular. Entretenimiento: Observar eventos deportivos, conciertos, transmisiones en vivo u otras actividades de entretenimiento.

- Análisis de datos: Utilizar sistemas de monitoreo de video para recopilar información y datos sobre patrones de comportamiento

2.4 Estándar de compresión de video

2.4.1 H.264

El estándar H.264, también conocido como Advanced Video Coding (AVC), es una tecnología de compresión de video desarrollada conjuntamente por la Unión Internacional de Telecomunicaciones (UIT-T) y el Grupo de Expertos en Imágenes en Movimiento (MPEG) de la Organización Internacional de Normalización (ISO). Este estándar se ha convertido en una herramienta fundamental para la grabación, compresión y distribución de contenido de video en alta definición (HD) y ultra alta definición (UHD). [25]

Inicialmente, las nuevas técnicas de compresión y codificación de video se desarrollaron para mejorar la calidad de imagen en aplicaciones como la videoconferencia. Sin embargo, con el tiempo, estas técnicas se adaptaron para mejorar la capacidad de la Televisión Digital Terrestre (TDT). Una de las principales ventajas del estándar H.264 es su alta tasa de compresión, tanto de audio (AAC, parte 10) como de video (MPEG-4 parte 10). Esto significa que H.264 puede ofrecer videos de alta calidad con un uso eficiente del ancho de banda.

En principio los métodos de compresión h.264 cuando originalmente tenía como objetivo el poder mejorar la calidad visual en escenarios tales como videotelefonía, así se prioriza dos temas importantes tales como la nitidez y el rendimiento, además estos métodos o estos estándares de compresión fueron modificados dando nuevos dominios tales como la Televisión Digital Terrestre, así mejorando su adaptabilidad con esto nos asegura una correcta funcionalidad y eficacia, permitiendo así su aplicaciones en diversas plataformas digitales, así se puede acceder desde teléfonos inteligentes de transmisión en secuencia conectados en la misma red. [25]

Características Principales de H.264:

- Alta Eficiencia de Compresión: H.264 ofrece una alta eficiencia de compresión, lo que permite reducir significativamente el tamaño de los

archivos de video sin sacrificar la calidad. Esto se logra mediante técnicas avanzadas de predicción, transformada y cuantificación.

- ✚ Predicción Intra e Inter cuadro: El “Intra” trata de la predicción dentro en un cuadro de video, en cambio “Inter” está basado en la predicción lo que conlleva a diversos cuadros de video, para mejorar la compresión de video.
- ✚ Transformada de Coseno Discreta (DCT): Mediante la transformada de coseno discreta es la cargada de compresión, convirtiendo la señal de video en señal de frecuencia para fácil manejo al momento de comprimir.
- ✚ Perfiles y Niveles: H.264 define varios perfiles y niveles que permiten ajustar la complejidad y la eficiencia de codificación según las necesidades de la aplicación. Esto proporciona flexibilidad para utilizar H.264 en una amplia variedad de dispositivos y aplicaciones.
- ✚ Soporte para Diferentes Resoluciones: Posee la capacidad de gestionar una variedad de resoluciones comenzando con la definición estándar (SD), alta definición (HD) y ultra alta definición (UHD), lo que implica un diverso uso en aplicación como videoconferencias, transmisiones de televisión y Streaming en línea.

2.4.2 H.256

Este estándar comúnmente conocido HEVC es la representación más progresista en percepción de vídeo incrementando hasta la actualidad, este innovativo estándar ha alcanzado a regenerar de manera significativa la eficiencia de su antecesor, el estándar Advanced Video Coding con sus abreviaturas (AVC), esto al poseer y duplicar su disposición de compresión de contenido audiovisual. Por esta razón con HEVC se encuentra la posibilidad de sustentar el equivalente de calidad de vídeo mientras se logra disminuir el bit rate en un deslumbrante 50%, una de las primeras versiones completas fue el resultado de empeño y dedicación entre la colaboración de MPEG y el grupo experto de código de video (VCEG), donde recibieron la aprobación de las normas ITU-T en el año 2013. [26]

Este estándar ha aprovechado los avances en la capacidad de procesamiento de los dispositivos multimedia modernos, permitiendo así una entrega más eficiente de contenido de alta calidad, esta evolución es esencial para la expansión del contenido de video en alta definición y ultra alta definición, que requieren mayores

capacidades de compresión para ser transmitidos de manera eficiente a través de las redes actuales sin comprometer la calidad. [26]

Además, HEVC se ha adaptado a una variedad de aplicaciones, desde la transmisión de video en streaming hasta el almacenamiento en dispositivos físicos y la transmisión en tiempo real. Su diseño avanzado permite gestionar de manera efectiva las demandas de ancho de banda y almacenamiento, consolidándose como una herramienta indispensable para la industria del video digital en la era contemporánea.

2.5 Redes

Una red está basada en un sistema de comunicación donde va a permitir que cierta cantidad de equipos o dispositivos logren comunicarse entre ellos de una manera independiente, una de las cosas más importantes a mencionar es que la palabra Red o Redes no tan solo abarca una red computadoras, sino que también a los equipos de comunicación de datos, otro punto a considerar es que no hay un límite de nodos involucrados en una red mucho menos las separaciones de la red.

Para poder generar que tengan comunicación entre las redes, deberán establecer una conectividad mediante cableado, siempre y cuando se utilice el estándar Ethernet, que es utilizado en las conexiones de las redes LAN, todo es dentro de la tipología Bus con el mecanismo CSMA/CD, esto se refiere al protocolo de transmisión en orden de datos. [27]

2.5.1 Redes inalámbricas

Las redes inalámbricas tratan sobre la comunicación de medios no guiados por medio de ondas electromagnéticas, básicamente quiere decir que son redes que no necesitan de un medio físico (cable) para poder transmitir o recibir datos, esto también se debe tomar en cuenta que este tipo de redes suele ser la más vulnerable a ciertas situaciones donde el robo de información logra darse a través de una red inalámbrica, lo cual este tipos de casos puede llegar hacerse replantear si este tipo de redes es la mejor

Uno de los temas es que las redes inalámbricas es un tipo de tecnología que posee una buena velocidad de transmisión de datos siempre y cuando las condiciones de los lugares sean optimas, también es de fácil de instalación y configuración. [28]

2.5.2 Redes alámbricas

Una red alámbrica, es también conocida teóricamente como una red cableada, es básicamente un sistema de comunicación que va a utilizar cables físicos para poder transferir datos entre dispositivos y así el poder habilitar computadoras, servidores, impresoras y otros dispositivos que formen parte de la red de área local (LAN) o una red de área amplia (WAN), dentro de este tipo de redes alámbricas las más usadas o comunes son las siguientes:

- Ethernet: Es el tipo más utilizado en redes locales (LAN). Aquí utiliza cables de par trenzado o cables coaxiales para transmitir datos a velocidades de hasta Gigabits por segundo.
- Fibra Óptica: Utiliza cables de fibra óptica para transmitir datos mediante pulsos de luz, esto nos ofrece una mayor velocidad y capacidad de transmisión que el cable de cobre, una de sus ventajas es que puede recorrer largas distancias sin perder conexión.
- Cable Coaxial: este tipo de cableado en día ya no están utilizados, sin embargo, el cable coaxial solía ser utilizado en las redes de televisión por cable y en algunas redes LAN más antiguas.

2.5.3 Redes híbridas

Una red híbrida es un sistema complejo y de manera heterogénea donde abarca una gran variedad de nodos y diversas conexiones entre sí, siendo más factible para todo equipo lograr enlazarse con la red. Este planteamiento resalta la variedad en las arquitecturas de la red al contar con múltiples tipos de nodos y conexiones, como la calidad funcional que se logra al tener una red compuesta por múltiples nodos y relaciones, las diferentes particularidades son clave en un sistema híbrido de multimodo y multi relación donde se logra observar los aspectos importantes los cuales son: [29]

- La diversidad de los nodos que conlleva a derechos de autor palabras claves y documentos.
- La calidad de las conexiones que existen entre estos nodos ya que pueden manifestar como colaboración o cualquier otro tipo de correlación.

2.6 Topologías de redes

Dentro de la topología de redes se lo denomina el conjunto de dos o varios equipos (computadoras) que están conectadas a la misma red para así compartir información. Las composiciones de cualquier red van a estar compuesta por conexiones y nodos según el tamaño de la red, además esto lleva a una descripción esquemática sobre las posibilidades que nos da una red. [30]

2.6.1 Topología de anillo

Este tipo de topología va a estar compuesto de un aro o anillo cerrado, el cual está conformado por dos nodos como también de enlaces, algo a tomar en cuenta es que cada nodo debe estar conectado con solo dos nodos de manera adyacente, este tipo de topología no están recomendable utilizar ya que puede ocasionar varios problemas y que en el futuro donde exista un error en la conexión de un nodo la comunicación se perdería. [31]

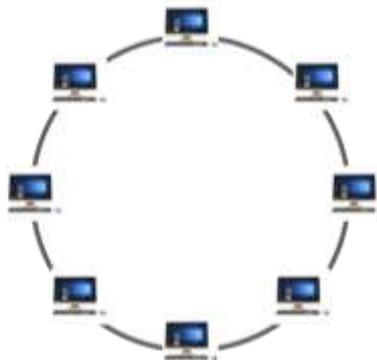


Ilustración 28. Arquitectura en forma anillo.

Fuente: Elaboración propia.

2.6.2 Topología de Bus

Este tipo de topología puede estar representado en una sola línea o cable donde van a ir conectados todos los hosts dentro del mismo cable. Una característica de este tipo de conexión permite conocer el tráfico del host. Este tipo de topología es más utilizado en redes pequeñas, además este tipo de redes por lo general suelen presentar ciertas colisiones y problemas de tráfico. [31]

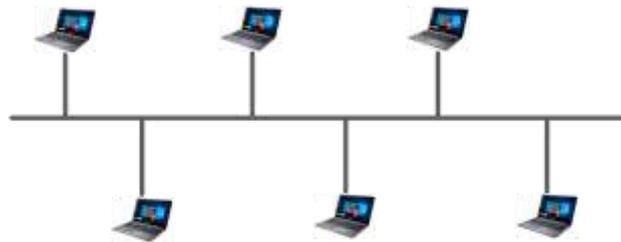


Ilustración 31. Arquitectura en forma bus.

Fuente: Elaboración propia.

2.6.3 Topología de Estrella

Una topología en estrella se la puede llegar a caracterizar por la disposición en el cual los dispositivos o periféricos y terminales van a estar interconectados directamente a un elemento central. Este tipo de topología o configuración patentiza su singularidad al poder brindar una visibilidad mejorada así dando las posibilidades de detección a posibles fallos o errores. [30]



Ilustración 34. Arquitectura en forma estrella

Fuente: Elaboración propia.

2.6.4 Topología de Árbol

Las topologías de árbol o jerárquica se logran distinguir por que constan de un único nodo comúnmente conocido como raíz, del cual se va a desplegar de una forma de árbol o también llamado ramificaciones nodales. Dentro de un esquema arbóreo, se va a distinguir de dos variantes notables los cuales son:

- **Árbol binario:** Estos son caracterizados por cada nodo donde se bifurcan en dos partes distintas.

- **Árbol genealógico:** Los enlaces entre nodos ramificados reflejan conexiones filiales simbolizando así un árbol genealógico. [32]



Ilustración 37. Arquitectura en forma árbol.

Fuente: Elaboración propia.

2.6.5 Topología de Malla

En una topología de red tipo malla, esta basada en todos los nodos que se encuentran interconectados de manera directa, esto va a implicar que cada nodo físico va a establecer una conexión con todos los demás nodos mediante vínculos adicionales. En ciertos casos de que algún enlace proceda a presentar algún fallo, el flujo de información persiste mediante la utilización de múltiples rutas alternativas con el cual si pueda llegar así a su objetivo. [32]



Ilustración 40. Arquitectura en forma malla.

Fuente: Elaboración propia.

2.6.6 Topología Híbrida

La topología híbrida es el resultado de la combinación de dos o más topologías diferentes en una sola estructura de red, uno de los ejemplos más comunes es cuando se mezcla los elementos de la topología estrella y la topología malla y eso

genera ya la topología híbrida esto da función a que ambas topologías funcionen simultáneamente. En este enfoque se va a poder aprovechar los beneficios junto con las características únicas de cada topología utilizada. [33]



Ilustración 43. Arquitectura en forma híbridas.

Fuente: Elaboración propia.

2.7 Estándares de comunicación

Un estándar de comunicaciones es un conjunto de reglas, protocolos y especificaciones técnicas diseñadas para garantizar una comunicación eficiente y compatible entre dispositivos y sistemas en una red. Estos estándares son fundamentales para garantizar la interoperabilidad y la coherencia en la transmisión de datos, voz, vídeo u otro tipo de información. Al seguir estándares comunes, diferentes fabricantes y proveedores de servicios pueden garantizar que sus dispositivos y aplicaciones puedan comunicarse sin problemas entre sí.

2.7.1 IEEE 802.3.x

El estándar IEEE 802.3 define varios aspectos de las redes Ethernet, como los medios físicos utilizados para la transmisión de datos, las velocidades de transmisión, el formato de tramas, el método de acceso al medio y la detección de colisiones. Algunas de las variantes comunes de Ethernet incluyen Ethernet 10BASE-T (10 Mbps sobre cable UTP), Ethernet 100BASE-TX (100 Mbps sobre cable UTP) y Ethernet 1000BASE-T (1 Gbps sobre cable UTP). [34]

2.7.2 IEEE 802.11.x

El estándar IEEE 802.11 introduce el concepto de Conjunto de Servicios Básicos (BSS), el cual se compone de dos o más nodos o estaciones inalámbricas que albergan la capacidad de identificarse mutuamente y establecer comunicación para la transferencia de información. En otras palabras, un BSS representa un grupo de

dispositivos inalámbricos que pueden reconocerse e interactuar dentro de una red inalámbrica, permitiendo la transmisión de datos y comunicación entre ellos de manera efectiva. [35]

2.7.2.1.1 IEEE 802.11ac

Este tipo de estándar es también conocido como la tecnología Wi-fi 5, es una especificación de red inalámbrica de alta velocidad, este estándar va a estar representada con mejoras significativas ante su predecesor, este estándar trabaja en la frecuencia de 5 GHz y con las funciones de MIMO esto nos va a permitir una mayor cantidad de canales y una menor interferencia en comparación con las que operan con la frecuencia de 2.4 GHz. [36]

2.7.2.1.2 IEEE 802.11n

El Wi-Fi 4 Como comúnmente se lo conoce al estándar IEEE 802.11 n, está basado en una individualización de red inalámbrica que fue debutada en el año 2009, como dato interesante este tipo de red también logra operar en las bandas de frecuencia de 2.4 y 5 GHz con el fin de brindar una mayor acomodación y afinidad con los diferentes dispositivos que trabajan de manera inalámbrica y a su vez operen en ambas bandas antes mencionadas. Debido a su gran innovación en este tipo de estándar utiliza una tecnología muy peculiar conocida como MIMO, lo que quiere decir esta terminología es que utiliza múltiples antenas como su nombre lo señala, tanto como para el punto de acceso como para los dispositivos de destino. Este tipo de tecnología ha sido empleado para poder mejorar la eficiencia y calidad de las conexiones inalámbricas tomando como ejemplo siendo utilizado en las grandes metrópolis de diferentes países del primer mundo. [36]

2.8 Protocolo de servidores

2.8.1 DNS

Esto comienza en los inicios del internet con esto las direcciones se gestionaban mediante la única tabla centralizada, durante la década del 70 la empresa ARPANET que es la precursora del internet estaba formada de muchas máquinas las cuales iban a depender de un solo archivo denominado HOSTS.TXT, este archivo era el único que guardaba toda la información sobre las máquinas lo cual permitía la resolución de los nombres a las direcciones IP, existían otros sistemas lo cual se basaban en realizar copias periódicas de la información que contenía el archivo para poder tener

la coherencia y la actualización de la información ya que todo esto se realizaba como método centralizado de la gestión, esto a medida de que si iba creciendo la red exponencialmente el sistema es centralizado llegó a su capacidad lo cual mostraba su limitación por ende se llevó el desarrollo del sistema de nombres de dominio denominado como (DNS). [37]

El Sistema de nombres de dominio (Domain Name System), está basado en un sistema de nomenclatura jerárquica de manera estandarizada según las normas RFC 1034 y RFC 1035, este sistema permite a la asociación de información con nombres de dominio el poder facilitar la localización y el respectivo acceso a los recursos de la red, uno de sus principales funciones es el poder mapear nombres de dominio elegibles para los humanos en direcciones IP, este mismo en ciertos casos suelen ser difíciles de memorizar por eso este sistema permite utilizar una tabla para poder así tener todas las direcciones de la red y así tener un control del mismo. [37]

También al proporcionar de manera los nombres significativos y comprensibles a las direcciones IP, el DNS simplifica el acceso a los sitios web y otros servicios en línea, todo esto mediante la estructura jerárquica antes mencionada ya que permite a los usuarios el poder utilizar nombres fáciles de recordar, traduciéndose a nombre de dominios amigables con las correspondientes elecciones y así facilitar la navegación y la administración de las redes a nivel global

2.8.2 Hypertext Transfer Protocol (HTTP)

El protocolo de transferencia de hipertexto (HTTP) es un protocolo de comunicación sencilla ya que es de tipo cliente servidor lo que regula el intercambio de información entre los navegadores web y entre los servidores http, la explicación completa del protocolo http se encuentra detallada en la norma del RFC 1945, ya que fue desarrollado por Tim-Berners Lee para poder satisfacer las necesidades del sistema global de distribución de información como lo es la Word wide web (www). [38]

También una de las perspectivas de las comunicaciones de HTTP está apoyada en los servicios de conexión de TCP/IP ya que opera de manera similar a otros servicios comunes dentro de los entornos UNIX, el procedimiento del servidor escucha en un puerto de comunicación TCP y espera solicitudes de conexión de los clientes web, una vez que esté establecida la conexión el protocolo TCP se encarga

de mantener la comunicación asegurando un intercambio de datos sin errores, ya que el funcionamiento del HTTP se basa en las operaciones simples de solicitud y respuesta donde un cliente inicia una conexión con un servidor y envía un mensaje con los datos de la solicitud por ende el servidor llega a responder con un mensaje similar que incluya el estado de la operación y el resultado posible todas estas operaciones pueden incluir un objeto o recurso específico sobre el cual están actuando y se entrega como un documento en HTML o un archivo multimedia o una aplicación CGI que es identificado por su URL. [38]

Las características que presenta el protocolo de transferencia de hipertexto (HTTP) Es fundamental para las comunicaciones en la web, dónde a continuación se mostrará algunas de sus características claves:

- ✚ Cliente-Servidor: El HTTP es un protocolo basado en un modelo cliente servidor donde los clientes envían solicitudes a los servidores web los cuales responden a los recursos solicitados.
- ✚ Conexión sin estado: Cada solicitud de HTTP es de manera independiente y no conserva información sobre solicitudes anteriores lo cual simplifica que el protocolo puede requerir mecanismos adicionales para mantener las sesiones.
- ✚ Métodos de Solicitud: HTTP soporta varios métodos de solicitud como GET, POST, DELETE, HEAD, OPTIONS y PATCH, cada uno diseñado para realizar diferentes tipos de operaciones
- ✚ Uso de URLs: HTTP utiliza UNIFORM RESOURCE IDENTIFIERS para identificar recursos lo que permite la localización de recursos de manera unificada y estandarizada
- ✚ Seguridad: HTTP puede ser utilizado sobre TLS para formar HTTPS, que proporciona confidencialidad, integridad y autenticación de la comunicación
- ✚ Código de Estado: Las respuestas basadas de HTTP incluyen códigos de estado que informan sobre el resultado de la solicitud.

De la siguiente tabla se muestra la diferencia entre los diferentes protocolos y el mencionado.

Tabla 1. Comparación entre protocolos y el Http

Fuente: [39]

Características	HTTP	HTTPS	FTP	SMTP
Modelo	Cliente-Servidor	Cliente-Servidor	Cliente-Servidor	Cliente-Servidor
Puerto x defecto	80	443	21	25
Estado	Stateless	Stateless	Stateless	Stateless
Seguridad	No cifrado	Cifrado con TLS	Opcional (FTPES/FTPS)	Opcional (STARTTLS)
Propósito	Transferencia de Hipertexto	Transferencia de Hipertexto	Transferencia de archivos	Envío de correo electrónico
Métodos	GET, POST, PUT, DELETE	GET, POST, DELETE, PUT	USER, PASS, RETR, STOR	HELO, MAIL, RTCP, DATA
Uso Principal	Navegación Web	Navegación Web	Transferencia de archivos	Envío de correos electrónicos
Persistencia	No	No	No	No
Encabezados	Si	Si	No	No
Soporte de Contenidos	Si	Si	No	No

2.8.3 Hypertext Transfer Protocol Secure (HTTPS)

El protocolo HTTPS (Hypertext Transfer Protocol Secure) es la versión más segura del protocolo http, lo que incorpora el protocolo SSL (Secure Sockets Layer), el SSL fue propuesto por Netscape en 1994 con el apoyo de Verisign y sus Microsystems y fue lanzado oficialmente ese mismo año con el objetivo principal del protocolo HTTPS es poder garantizar la seguridad en la transmisión de datos especialmente en las aplicaciones que manejan información confidencial tanto como lo puede llegar a ser el comercio electrónico las transacciones bancarias contraseñas y datos privados entre muchos servicios que se ofrecen en la red, este protocolo se considera único aunque sea en la unión de 2 protocolos por lo tanto es necesario usar en el URL como “https://” ya que ahí ejecuta a la llamada de una página con seguridad a diferencia del protocolo HTTP, una de las diferencias principales entre el protocolo HTTP y el HTTPS es que tiene un símbolo de un candado con el cual se entiende de que la página a la que se está accediendo es segura. [39]

El protocolo SSL ha ido evolucionando con el tiempo TSL ya que fue diseñado para proporcionar una capa adicional de seguridad en las comunicaciones dentro de internet estos protocolos SSL/TLS cifra los datos transmitidos entre el cliente y el servidor asegurando de que toda la información intercambiada no puede ser interceptada o manipulada por terceros los cuales no están autorizados a tener dicha

información, con esto las transferencias de datos entre los navegadores y los servidores, bajo el protocolo son cifradas, una de las partes principales es que el uso del puerto de este de este protocolo es el 443. [39]

Características del HTTPS

- ✚ Cifrado: el protocolo HTTPS utiliza de seguridad al TSL (transport Layer security) y su predecesor SSL (Secure sockets Layer), ya que estos sirven para cifrar los datos transmitidos entre el cliente y el servidor
- ✚ Autenticación: el HTTPS asegura que el cliente esté comunicándose con el servidor legítimo mediante el uso de certificados digitales emitidos por las autoridades de la certificación con el fin de poder prevenir ataques de suplantación de identidad.
- ✚ Puerto por Defecto: los puertos por defecto de HTTPS es generalmente el 443 a diferencia de http que utiliza el puerto 80.

2.8.4 Real-time Streaming Protocol (RTSP)

El Protocolo RTSP (Real-time Streaming Protocol) básicamente está diseñado para realizar la gestión del flujo de datos en tiempo real ya sea entre un cliente y un servidor, así operando al nivel de la aplicación que se le valla a dar, a diferencia de los demás protocolos que están orientados a la conexión, el RTSP no permite o no establece una conexión constante ya que va a estar definido al momento que envía la información de manera eficiente y así eliminar las interrupciones. [40]

Este protocolo es muy esencial para poder garantizar de manera correcta la entrega de datos durante el streaming, ya que el contenido multimedia es muy sensible a la sincronización temporal, una de las cosas importantes es que el protocolo trabaja como servidores multimedia, dando el poder al usuario de manipular el medio mediante por comandos de los cuales son denominados como: play, pause y stop.

Este protocolo RSTP logra soportar diversas maneras de conexión, además, también define varios diversos requisitos con el fin de optimizar las transmisiones de datos a través de las redes IP, uno de sus objetivos principales es el poder de que sea seguro que las transferencia de datos sea de manera eficiente y que se pueda minimizar el nivel de latencia y así evitar las caídas e interrupciones, el protocolo RTSP logra establecer y controlar de que los datos estén sincronizados, también gestiona las sesiones con ayuda de identificadores para cada transmisión. [40]

Las diferentes características que posee el protocolo RSTP:

- ✚ Control de Sesiones: El RSTP permite a los clientes el poder controlar sesiones de transmisión Streaming.
- ✚ Multicasting y Unicasting: El RTPS logra manejar tantas transmisiones simultaneas en unicast y multicast con fin de aprovechar el máximo del ancho de banda.
- ✚ Extensible: Es compatible con versiones anteriores sin comprometer las nuevas funciones.
- ✚ Establecimiento y Terminación: Logra proporcionar mecanismos para iniciar, modificar y finalizar sesiones multimedia.

El protocolo es una herramienta esencial para la entrega y control de flujos de datos multimedia en tiempo real, además, sus características de control de sesiones, flexibilidad y compatibilidad lo hacen de manera ideal para una amplia variedad de aplicaciones como pueden ser videovigilancia, streaming ya que permite una alta interactividad al ajustarse a diferentes condiciones de red.

2.8.5 Open Network Video Interface Forum (ONVIF)

El estándar ONVIF está basado en un estándar abierto ya que fue creado para que los sistemas de seguridad física garanticen la interoperabilidad entre dispositivos de diferentes fabricantes con la premisa central de que este protocolo es el modelo de poder interactuar y comunicarse eficazmente con cualquier otro dispositivo que también cumpla con los estándares ONVIF, ya que el objetivo principal que se llevó a cabo para poder desarrollar es el poder eliminar las barreras entre los diferentes equipos de seguridad de diferentes proveedores permitiendo así una amplia integración de la manera más sencilla y eficiente dentro del sistema de vídeo vigilancia controles de accesos y otros aspectos en seguridad física, también que este estándar nos permite tener un marco común que facilita la interoperabilidad así asegurando que los dispositivos como las cámaras IP, grabadores de vídeo de red y sistema de gestión de vídeo puedan trabajar juntos y sin problemas y de manera independiente del fabricante. [41]

Estructura de estándar Onvif

La estructura del estándar ONVIF se organiza mediante diversas especificaciones que pueden agruparse en perfiles conocidos como perfiles ONVIF con el fin de que

este producto sea considerado compatible con ONVIF debe cumplir con varios requisitos o al menos con uno de los perfiles que van a ser mencionados en estos perfiles facilitan la identificación de cómo los dispositivos y clientes compatibles pueden interactuar y ser inter pero hables entre sí con el fin de que puedan trabajar juntos de manera eficaz. [41]

Además, de las funciones obligatorias cada perfil ONVIF puede incluir características condicionales ya que estas son funciones adicionales que pueden ser implementadas por un dispositivo o cliente hombre si son soportadas por dicho dispositivo ya que proporciona una flexibilidad a los fabricantes para añadir características avanzadas manteniendo la compatibilidad básica por el perfil, a continuación, los perfiles ONVIF:

- ✚ Perfil A: Esta enfocado en la configuración de permisos de acceso físico, además soporta las configuraciones de las políticas de acceso y gestión de credenciales
- ✚ Perfil G: Esta enfocado en la grabación, búsqueda y reproducción de datos en dispositivos de almacenamiento.
- ✚ Perfil M: Esta enfocado en la gestión de metadatos y la integración de analítica avanzada, además, soporta la transmisión y gestión de metadatos.
- ✚ Perfil S: Está diseñado para el manejo de video y audio en Streaming, además, de soportar el control de transmisión de video, audio bidireccional y metadatos.

Aplicaciones del Protocolo ONVIF

- ✚ Videovigilancia: Integración de cámaras IP, NVR y VMS para la monitorización y grabación de video en tiempo real.
- ✚ Control de Acceso: Incorpora lectores de tarjetas, cerraduras electrónicas y diferentes tipos de gestión de acceso, para mejorar el control del sistema de acceso.
- ✚ Gestión de Tráfico y Transporte: Monitoreo y control de tráfico y sistemas de transporte público, mejorando la seguridad y eficiencia operativa.

2.9 Ataques a redes inalámbricas

2.9.1 Ataque pasivo

Los ataques pasivos se centran en la interceptación y el monitoreo de la información transmitida a través de la red sin alterar los datos ni afectar el funcionamiento del sistema. El propósito principal de los ataques pasivos es obtener información confidencial o sensible sin ser detectados, estos ataques suelen ser difíciles de identificar ya que no generan alteraciones visibles en los sistemas o redes afectados., ya que aparentemente no producen daño, pero atacan en donde estén los puntos más flacos de seguridad para en un futuro poder hacer daño. [42]

Algunos ataques pasivos son:

- ✚ **Eavesdropping (Escucha Clandestina)**
- ✚ **Sniffing (Olfateo de Paquetes)**
- ✚ **Traffic Analysis (Análisis de Tráfico)**

2.9.2 Ataque activo

Los ataques activos, por otro lado, implican la alteración directa de los datos, la interrupción de los servicios, o el acceso no autorizado a los sistemas, estos ataques son más agresivos y pueden causar daños significativos a las redes y sistemas afectados. Los ataques activos buscan no solo robar información, sino también manipular, ya que el atacante escucha los mensajes transmitidos en la red y los reenvía al destinatario legítimo. [42]

Algunas características y ejemplos de ataques activos incluyen:

- ✚ **Denial of Service (DoS) y Distributed Denial of Service (DDoS):** Estos ataques intentan sobrecargar un sistema o red con tráfico excesivo para interrumpir o denegar el servicio a los usuarios legítimos.
- ✚ **Inhibidor de señal:** Un bloqueador de frecuencia o inhibidor de señal, ejecuta ataques de denegación de servicio al controlar el espectro electromagnético para que éste se vuelva inaccesible. Este dispositivo es capaz de interrumpir las comunicaciones inalámbricas como sistemas de seguridad, Bluetooth, telefonías móviles y redes Wi-Fi. Al interferir con señales de frecuencia específica los inhibidores pueden desconectar servicio

al bloquear las señales de frecuencias específicas, lo que puede tener serias repercusiones en situaciones de emergencia. [43]

- ✚ **Phishing y Spear Phishing:** Utiliza correos electrónicos o mensajes fraudulentos para engañar a los usuarios y obtener sus credenciales de acceso o información personal sensible.
- ✚ **Malware (Software Malicioso):** Se encarga de robar información mediante infectando los equipos con virus, gusanos, troyanos y ransomware.

2.9.3 Ataques cibernéticos

Los ciberataques son métodos deliberadamente diseñados para explotar vulnerabilidades o debilidades presentes en una red, sistema o aplicación con el objetivo de causar algún tipo de daño, interrumpir servicios, robar información, o comprometer la integridad y confidencialidad de los datos. Estos ataques pueden clasificarse en dos categorías principales: ataques pasivos y ataques activos, cada uno con sus propias características y mecanismos. [42]

Los ciberataques pueden lograr tener consecuencias grandes y devastadoras para las diferentes organizaciones importantes las cuales sufren daños en todos los sentidos como también a los individuos ya que nadie esta salvo de este tipo de delincuencia a continuación. Para las organizaciones, los ciberataques pueden resultar en la interrupción de sus operaciones diarias, pérdida de datos críticos, compromisos de seguridad y costosas recuperaciones, las brechas de seguridad pueden exponer información confidencial, lo que puede llevar a multas regulatorias, litigios y una pérdida de confianza por parte de clientes y socios comerciales. Además, la restauración de sistemas comprometidos y la implementación de medidas de seguridad adicionales pueden suponer un costo financiero significativo. los grandes impactos que ocasiona estos tipos de ataques:

- ✚ **Pérdida de Datos:** Información valiosa y sensible puede ser robada, comprometida o destruida.
- ✚ **Daño a la Reputación:** Las infracciones de seguridad pueden debilitar la confianza de clientes y socios, impactando la reputación y la confiabilidad de la entidad.

- ✚ **Compromiso de Seguridad:** La integridad y confidencialidad de los datos se ven comprometidas, lo que puede tener implicaciones legales y de cumplimiento normativo.

2.10 Tecnología SDR

El software Defined Radio es renombrado como una de las tecnologías de radio excesivamente versátiles y adaptables esto se debe a que sus capacidades se determinan fundamentalmente a través de software, por lo cual esta peculiaridad permite que el hardware sea diseñado y operado para ejercer múltiples funciones en diversos momentos, cabe recalcar que esto tiene lugar según las necesidades que se meriten durante su uso, el SDR brinda una estructura en gran medida flexibles por lo que facilita la innovación y modernización de sus debidas capacidades en tiempo real... [44]

El SDR (Software Defined Radio) está basado en el sistema de comunicaciones lo que utiliza el software con la ayuda del software para el procesamiento de las señales de radio. Este hardware empleado en un sistema de radio definida por software (SDR) generalmente consiste en una tarjeta de Radiofrecuencia, la tarjeta posee la capacidad de poder convertir las señales de radio analógicas en señales digitales como también de manera inversa, además, de transformar las señales digitales en señales de radios analógicas, con esto de tener una comunicación eficiente. [45]

Este dispositivo posee todas las funciones de procesamiento de señales basadas en la transposición de frecuencia, además, incluye filtrado y demodulación, los cuales se realizan en el hardware, evitando así afectar el diseño, esta tecnología fue desarrollada inicialmente en los Estados Unidos con el propósito de permitir la comunicación en diversas bandas utilizando un solo equipo, este avance ha sido significativo, ya que actualmente se emplea para múltiples fines. [44]

Además, existen varias aplicaciones del SDR:

- ✚ Comunicaciones Militares
- ✚ Radioaficionados
- ✚ Comunicaciones Móviles
- ✚ Radiodifusión
- ✚ Vigilancia y Seguridad

La estructura de un SDR puede llegar a variar considerablemente ya que esta baso en dos formas como Software y Hardware, también de la aplicación que se le valla a dar, la estructura está diseñada para poder permitir la configuración y reconfiguración de los componentes de manera dinámica, ajustándose a as necesidad que requiera el usuario. [45]

En la siguiente ilustración 16, se muestra la estructura típica del diagrama de bloques de un equipo SDR, además, de sus funciones las cuales son muy importantes para el desarrollo de proyecto.

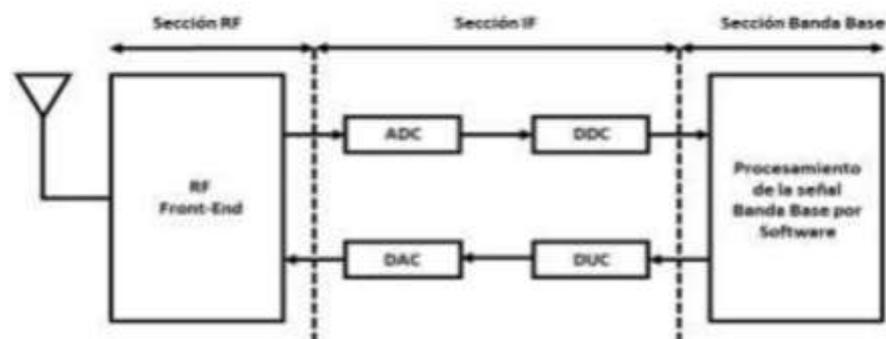


Ilustración 46. Diagrama de bloque de la tecnología SDR.

Fuente: [43]

Dentro de la tecnología SDR tenemos funciones básicas de la misma:

Tabla 2. Funciones básicas de un diagrama SDR.

Fuente: [43]

Sección	Función
RF (Radiofrecuencia)	<ul style="list-style-type: none"> • Esta encargada de la Transmisión y en la recepción de señales de Radiofrecuencia. • Ejecuta el paso de las señales RF a señales IF. • Realiza técnicas de modulación y o u amplificación junto a un LNA.
IF (Frecuencia Intermedia)	<ul style="list-style-type: none"> • Posee convertidores tales como (ADC/DAC) y (DDC/DUC). • Ejecuta el paso de Frecuencia Intermedia a banda base. • Posee convertidor Analógico Digital (ADC). • Posee convertidor Digital Analógico (DAC). • Posee convertidor Descendente Digital (DDC). • Posee convertidor Ascendente Digital (DDU).
Banda Base	<ul style="list-style-type: none"> • Dentro de la transmisión se realiza la extracción de la señal de manera digital en banda base luego de ser manipulada mediante la App o programa en el ordenador. • Luego en la recepción es, al contrario.

2.11 Recurso de software

2.11.1 Python

Python es un lenguaje de programación que se originó como un proyecto de código abierto y actualmente es supervisado por la organización Python Software Foundation.

Guido Van Rossum, el fundador de Python le otorgó el nombre debido a la administración hacia los comediantes británicos Monty Python, un tema más importante es el lenguaje de programación con el que maneja Python se encuentra en la escala de scripting y también disputa determinadamente con Perl, una particularidad que es muy visible de Python es su eficiencia para poder fraccionar un programa en varias secciones con eso permite de que sea aprovechado al máximo con una variedad de programas que fueron desarrollados con el mismo lenguaje de programación que utiliza Python, de igual manera posee una gran lista de diferentes módulos los que permiten desarrollar diversos trabajos de entrada y salida de archivos, llamadas y poder generar interfaces gráficas ya que esto permite tener una excelente interacción con el programador.. [46]

2.11.2 Modelo de aprendizaje Yolov5

La primera versión de YOLO fue presentada en 2015, y la más reciente, la versión 5, se introdujo en 2020, en las versiones sucesivas, como YOLOv3 y YOLOv4, se han implementado diversas mejoras, incluyendo el uso de conexiones residuales y redes piramidales convolucionales (Features Pyramid Network, FPN). Estas mejoras han permitido aumentar la precisión y eficiencia del modelo en la detección de objetos. [47]

La versión más reciente, YOLOv5, que se emplea en este proyecto, está implementada en el framework PyTorch. PyTorch es una biblioteca basada en Python diseñada para realizar cálculos a través de tensores. Estos tensores se ejecutan en la GPU, lo que permite reducir significativamente los tiempos de entrenamiento y ejecución en comparación con la ejecución en la CPU, gracias a su flexibilidad y eficiencia, PyTorch se ha convertido en una de las herramientas más populares para el desarrollo de aplicaciones de inteligencia artificial, junto con Tensor Flow y Keras.

El Yolov5 es un prototipo de localización de objetos de avanzada generación ya que sus puntos de destacar son por su rapidez y precisión en el cual es empleado en detectar objetos en vídeos e imágenes todo esto en tiempo real y hace que sea posible el poder procesar los datos capturados de la misma manera antes mencionada, esto ya hace que sea esencial para desarrollar servicios que requieren recurrir a la detección rápida y oportuna, un ejemplo claro está desarrollado en la actualidad como lo pueden ser en la conducción autónoma donde necesita un buen equilibrio entre la rapidez y la precisión este modelo viene en diverso tamaños como lo son:

-  Versión S
-  Versión M
-  Versión L
-  Versión X

También presenta un cúmulo de datos personalizados por lo que se aporta distintas técnicas de aumento y gran ajuste de parámetros ya que posee peculiaridades donde permiten que sea adaptable a diferentes tareas donde nos deja un gran margen de aprendizaje ya que simplifica la fusión con otros proyectos basados en el mismo lenguaje PyTorch. a sus predecesores, por ejemplo, ha mejorado el anclaje automático, que optimiza la detección de objetos de diferentes tamaños, y ha refinado la estrategia de data, lo que ayuda a aumentar la robustez del modelo frente a variaciones en los datos de entrada. Además, la comunidad de usuarios y desarrolladores de YOLOv5 ha crecido, proporcionando una amplia gama de recursos y soporte para aquellos que implementan y experimentan con este modelo en sus proyectos de visión por computadora. [47]

Características del módulo YOLOv5

-  Velocidad y Eficiencia: está diseñado para ser extremadamente rápido, así permitiendo la detección de objetos a tiempo, también utiliza la potencia del GPU para acelerar significativamente los tiempos.
-  Facilidad de uso: tiene la implementación del framework que, conocido por su flexibilidad y fácil uso, además este módulo viene con scripts preconfigurados, fáciles de usar.

- ✚ Modelos Preentrenados: ofrece varios modelos preentrenados con diferentes tamaños, capacidades ya que el solo cuenta diversos formatos

2.11.3 GNU radio

El GNU Radio es un entorno de desarrollo de software de manera gratuita, como también de código abierto donde ofrece una amplia gama de bloques de procesamiento de señales que están diseñados para lograr una implementación de radio definida como lo es el SDR (Software Defined Radio), este software está integrado con el hardware de Radiofrecuencia de manera externa. También el GNU Radio está altamente valorado y siendo utilizado en diversos ámbitos tales como: [45]

- ✚ Entornos Académicos
- ✚ Radioaficionados
- ✚ Sectores comerciales

Este software permite a todos los desarrolladores el poder crear diferentes aplicaciones de SDR con lo que puedan transmitir y recibir señales de radio, lo cual se realiza de diferentes tipos que pueden ser el de Hardware de Radiofrecuencia, tarjetas de sonido, dispositivos USB y de tarjetas (Field Programables Gate Array)

CAPITULO III

3.1 DESARROLLO DE LA PROPUESTA

La actual propuesta tiene como fin el poder formalizar la Optimización de infraestructura de CCTV mediante sistemas híbridos y seguridad en redes avanzadas de WIFI, mediante a los estudios realizados para poder alcanzar todos los objetivos propuestos, además, se va a dividir en tres escenarios donde se van a demostrar diferentes características y demostrar cual es la mejor, también los equipos a utilizar son de marcas líderes en tecnología Wifi, Radio Frecuencia y de video vigilancia, tales como Ubiquiti y Reolink, estos equipos poseen compatibilidades con otros equipos y así mejoran sus uso como también sus interfaces de manejo para su entendimiento de una mejor manera.

El desarrollo de esta propuesta se va a ejecutar en un ambiente controlado del laboratorio de telecomunicaciones y a los alrededores, dentro de este mismo va a quedar implementado para sus futuros usos, luego se le dará el uso al dispositivo llamado HackRF One para poder medir las interferencias ocasionadas por este equipo, por tal motivo va a quedar una guía para practicas dentro de un módulo educativo.

3.1.1 COMPONENTES DE LA PROPUESTA FÍSICOS

3.1.1.1 NVR Reolink

El componente Reolink están diseñados para poder grabar toda las imágenes o videos grabadas mediante las cámaras y posee cuatro antenas que van en la parte trasera del NVR para poder una alta ganancia para así potencia la señal del RLN12W, uno de sus puntos fuertes es que cubre un área total de 1000 metros cuadrados, también unas de sus funciones principales es que trabaja con la tecnología WIFI 6 donde trabaja con las más ultima encriptación WPA 3, para poder así proteger los datos y privacidad del sistema, con la transmisión inalámbrica va a estar más segura, también puede conectarse con diversas marca de videocámaras de seguridad siempre y cuando cumplan o tengan los mismos protocolos de conectividad. [48]



Ilustración 49. NVR Reolink RLN12W.

Fuente: Elaboración propia.

Tabla 3. Especificaciones dada por el proveedor de NVR RLN12W.

Fuente: [48]

Entrada de video/Audio	
Entrada de Video IP	UP to 12 IP cameras
Entrada de Audio	Cameras with built-in mic
Salida de Video / Audio	
Salida de Video	VGA, HDMI
Resolución de la pantalla	HDMI: 3840x2160, 1920x1080, 1280x1024, 1280x720, 1024x720 VGA: 1920x1080, 1280x1024, 1280x720
Salida de audio	1-channel, RCA
Descodificación	
Compresión de Video	H.265/H.264
Formato de Video	7680x2160, 4608x1728, 4512x2510, 4096x3072, 3840x2160, 2560x1920, 2560x1440, 2048x1536, 2340x1296, 1080p, 720p
Reproducción Simultanea	Up to 4 channels
Almacenamiento	
SATA	1xSATA interfaz (1x2TB HDD)
Capacidad	Up to 16 TB
Interfaz Interna	
Interfaz USB	2xUSB 2.0
Interfaz de red	4xRJ 45, 10/100 Mbps self-adaptive 1x RJ45, 10/100 Mbps self-adaptive
Wi-Fi	
Estándar inalámbrico	IEEE 802, 110a/ac/ax/b/g/n
Frecuencia de Funcionamiento	2.4 GHz/ 5 GHz
Seguridad inalámbrica	WPA/WPA2/WPA3
Red	
Protocolos de Red	HTTPS, TCP/IP, UDP, DHCP, P2P, UONP, RTMO, RTSP, SMTP, SSL/TLS, DNS, DDNS, NTP, FTP

Navegadores compatibles	Edge, Firefox, Chrome, Safari
OS Compatible	PC: Windows, Mac OS; Smartphone: IOS, Android
Max Acceso de Usuarios	Max. 20 users (1 admin & 19 users) Max. 12 simultaneous (10 sub & 2 mainstreams)
General	
Fuente de Alimentación	DC 12V/2A
Consumo de energía	10w (with 2TB HDD)
Entorno de Funcionamiento	Temperatura: -10 C-+45 C
Dimensiones	255mm(W)x 49.5mm(H)x222.7mm(D)
Peso	1.4 Kg
Garantía	
Garantía Limitada	2-year limited warranty

3.1.1.2 Reolink color Cam 510w

La Reolink Color Cam 510W es una cámara de seguridad inalámbrica Wi-Fi diseñada para proporcionar una solución completa para la seguridad del hogar y la vigilancia, posee herramientas tecnológicas mejoradas a cámaras y atributos innovadores, lo cual hace que esta cámara sobresalga en el sector de cámaras de videovigilancia.

Una de las cualidades a destacar de la cámara utilizada es la capacidad hora de conectarse a redes wireless de bandas duales (2.4/5GHz), esto garantiza una conexión fiable y estable, garantizando que la transmisión de vídeo y las notificaciones se transmitan sin contratiempos. Además, la cámara dispone de una resolución HD de 5MP, asegurando así imágenes nítidas y detalladas durante el día como la noche.

En términos de funcionalidad, la Reolink Color Cam 510W está equipada con detección inteligente de personas y vehículos, lo que reduce las notificaciones falsas y permite a los usuarios centrarse en los eventos importantes. La detección de movimiento avanzada garantiza que la cámara capture cada movimiento sospechoso, mientras que la visión nocturna de alta calidad asegura que se puedan monitorear las actividades incluso en condiciones de poca luz. Otra característica destacada de la cámara es su micrófono incorporado, que permite capturar sonido ambiente. Esto es especialmente útil en situaciones donde el audio puede proporcionar información adicional sobre un incidente. Además, la Reolink Color

Cam 510W admite grabación continua las 24 horas, activada por movimiento y programada, lo que garantiza que nunca se pierda un momento importante. [49]



Ilustración 52. Cámara Reolink Color.

Fuente: Elaboración propia.

Tabla 4. Especificaciones dada por datasheet de Reolink Color Cam.

Fuente: [49]

Video & Audio	
Sensor de Imagen	Sensor CMOS de 1/2,7"
Resolución de Video	Predeterminado: 2560x1920 (5 megapíxeles) a 20 fotogramas/s
Objetivo	f= 4.0 mm fijo; F= 2.0, con corte IR
Compresión de video	H.264
Campo de visión	Horizontal: 80; Vertical: 42
Modo Dia/Noche	Filtro de corte IR con conmutación automática
Visión nocturna	30 metros (100 pies) (LED:18 pzas/14mil/850nm)
Audio	Grabación de audio
Alimentación	
Alimentación CC	DC 120, V; 1A; 12W
Interfaz	
Alimentación	Puerto de alimentación CC
Sistema	botón de reinicio
Ethernet	Mbps; Rj45
Almacenamiento	Ranura de tarjeta MicroSD
Audio	Micrófono incorporado
Características de Software	
Frecuencia de Imagen	Transmisión principal: 2fps-30fps, Transmisión secundaria: 4fps-15fps
Tipo de código	Transmisión principal: 1024 kbps - 8192 Kbps; Transmisión secundaria: 64 Kbps - 512 Kbps
Navegadores Compatibles	Edge, Firefox, Chrome, Safari
OS Compatibles	PC: Windows, Mac OS; Smartphone: IOS, Android

Alarma Inteligente	Grabación de movimiento/ detección de personas/detección de vehículos
Navegadores Admitidos	Grabación de movimiento; grabación programada; grabación 24/7
Protocolos y estándares	HTTPS, TCP/IP, UDP, DHCP, P2P, UONP, RTMO, RTSP, SMTP, SSL/TLS, DNS, DDNS, NTP, FTP
Max. Acceso de Usuario	20 users (1 cuenta de admin y 19 cuentas de users); admite 12 transmisiones de video simultaneo (10 transmisiones secundarios y 2 principales)
Funciona con	Google Assitant
Inalámbrico	
Estándar inalámbrico	IEE 802.11 a/b/g/n
Frecuencia de funcionamiento	2.4 GHz/5GHz
Seguridad inalámbrica	WPA-PSK/WPA2-PSK
Entorno de Funcionamiento	
Temperatura de Funcionamiento	Temperatura: -10 C-+55 C
Humedad de Funcionamiento	10 % - 90 %
Impermeabilidad	IP67
Tamaño & Peso	
Dimensión	67x186 mm
Peso	415 g
Garantía	
Garantía Limitada	Garantía Limitada de dos años

3.1.1.3 Ubiquiti NanoStation

El Ubiquiti NanoStation es un dispositivo inalámbrico diseñado para crear enlaces punto a punto de alta velocidad entre ubicaciones remotas. Algunas características clave del NanoStation incluyen:

Permite conectar dos ubicaciones remotas en una misma red, compartiendo la conexión a Internet entre edificios, disponible en modelos de 2.4 GHz (NanoStation M2) y 5 GHz (NanoStation M5), con potencias de salida de hasta 600 mW y velocidades de hasta 150 Mbps, incluye software web integrado AirOS para controlar la potencia, modo puente/AP, etc. [50]

Viene con inyector PoE y adaptador de CA de 240V, requiere dos unidades para crear un enlace inalámbrico punto a punto, puede configurarse como un punto de acceso Wi-Fi 802.11b/g/n de alto rendimiento y largo alcance. Completamente resistente a la intemperie para instalación permanente en ambientes difíciles, indicadores de intensidad de señal para alineación rápida y sencilla

Para una instalación óptima, se recomienda montar las unidades en el techo, altas y despejadas de obstrucciones, utilizando su soporte de montaje integrado para poste, también se recomienda usar protección contra sobretensiones y cable Ethernet Cat6 exterior.



Ilustración 55. Ubiquiti NanoStation M2.

Fuente: Elaboración propia.

Tabla 5. Ficha técnica de equipo Ubiquiti NanoStation.

Fuente: [50]

Nano Station	
Dimensions	294 x 31 x 80 mm (11.57 x 1.22 x 3.15")
Weight	400 g (14.11 oz)
Power Supply (PoE)	24V, 0.5A
Max. Power Consumption	BW
Power Method	Passive PoE
Operating Frequency	2412-2462 MHz
Gain	10.4-11.2 dBi
Networking Interface	(2)10/100 Ethernet Ports
Processor Specs	Atheros MPS 24Kc, 400MHz
Memory	32 MB SDRAM 8MB Flash
Frequency	2.4 GHz
Cross-pol Isolation	23 Db Minimum
Max. VSWR	1.6:1
Beamwidth	55°(H-pol) /53°(V-pol)/27°(Elevation)
Polarization	Dual Linear
Enclosure	Outdoor UV Stabilized Plastic
Mounting	Pole-Mount
Operating Temperature	30 to 75°C(-22to167°F)
Operating Humidity	5 to 95% Noncondensing
Wireless Approvals	FCC Part 15.247, IC RS210, CE
RoHS Compliance	Yes
Shock & Vibration	ETSI300-019-1.4

Tabla 6. Valores de tasa de transmisión en base a la potencia de salida. Fuente:

Fuente: [50]

Output Power: 23 dBm							
5 GHz TX Power Specifications				5 GHz RX Power Specifications			
Modulation	Data Rate/MCS	Avg. TX	Tolerance	Modulation	Data Rate/MCS	Sensitivity	Tolerance
11a	6-24 Mbps	23 dBm	± 2dB	11a	6-24 Mbps	-83 dBm	± 2dB
	36 Mbps	21 dBm	± 2dB		36 Mbps	+80 dBm	± 2dB
	48 Mbps	19 dBm	± 2dB		48 Mbps	-77 dBm	± 2dB
	54 Mbps	18 dBm	± 2dB		54 Mbps	-75 dBm	± 2dB
11n/airMAX	MCS0	23 dBm	± 2dB	11n/airMAX	MCS0	-96 dBm	± 2dB
	MCS1	23 dBm	± 2dB		MCS1	-95 dBm	± 2dB
	MCS2	23 dBm	± 2dB		MCS2	-92 dBm	± 2dB
	MCS3	23 dBm	± 2dB		MCS3	-90 dBm	± 2dB
	MCS4	22 dBm	± 2dB		MCS4	-86 dBm	± 2dB
	MCS5	20 dBm	± 2dB		MCS5	-83 dBm	± 2dB
	MCS6	18 dBm	± 2dB		MCS6	-77 dBm	± 2dB
	MCS7	17 dBm	± 2dB		MCS7	-74 dBm	± 2dB
	MCS8	23 dBm	± 2dB		MCS8	-95 dBm	± 2dB

	MCS9	23 dB m	± 2 dB		MCS9	-93 dBm	± 2 dB
	MCS10	23 dB m	± 2 dB		MCS10	-90 dBm	± 2 dB
	MCS11	23 dB m	± 2 dB		MCS11	-87 dBm	± 2 dB
	MCS12	22 dB m	± 2 dB		MCS12	-84 dBm	± 2 dB
	MCS13	20 dB m	± 2 dB		MCS13	-79 dBm	± 2 dB
	MCS14	18 dB m	± 2 dB		MCS14	-78 dBm	± 2 dB
	MCS15	17 dB m	± 2 dB		MCS15	-75 dBm	± 2 dB

3.1.1.4 Ubiquiti Loco M2

El Ubiquiti NanoStation Loco M2 (LocoM2) es un dispositivo inalámbrico compacto y resistente diseñado para crear enlaces punto a punto de alta velocidad entre ubicaciones remotas en la banda de 2.4 GHz [50]

A continuación, diversas características importantes del LocoM2 incluyen:

Antena direccional doble polarización MIMO integrada de 8 dBi de ganancia, velocidad de transferencia real de hasta 150 Mbps. Tecnología TDMA (Time Division Múltiple Access) que permite conectar a más de 300 clientes con baja latencia, procesador Atheros MIPS 4KC de 400 MHz con 32 MB de SDRAM y 8 MB de flash, Interfaz Ethernet 10/100 con alimentación PoE pasivo (pares 4-5+, 7-8-), rango de hasta 10 km dependiendo del WISP, línea de vista y entorno.

Modos de operación: AP, cliente, WDS, Traffic Shopping, QoS, puente transparente o enrutamiento, completamente resistente a la intemperie para instalación permanente en ambientes difíciles, Indicadores de intensidad de señal para alineación rápida y sencilla.

Para una instalación óptima, se recomienda montar el LocoM2 en el techo, alto y despejado de obstrucciones, utilizando su soporte de montaje integrado para poste,

también se recomienda usar protección contra sobretensiones y cable Ethernet Cat6 exterior. [50]



Ilustración 58. Ubiquiti NanoStation Loco M2.

Fuente: Elaboración propia.

Tabla 7. Ficha técnica de equipo Ubiquiti NanoStation Loco M2.

Fuente: [50]

Specifications	
Dimensions	161x31x80 mm (6.31x1.22x3.15")
Weight	180g (6.35 oz)
Power Supply	24V, 0.5 A
Max. Power Consumption	5.5W
Power Method	Passive PoE
Gain	8.5 dBi
Networking interface	10/100 Ethernet Port
Bandwidths	60 °/ 60°/ 60°
Processor Specs	Atheros MIPS 24Kc, 400MHz
Memory	32 MB SDRAM, 8 MB Flash
Cross-pol Isolation	20 dB Minimum
Max. VSWR	1.4:1
Polarization	Dual Linear
Enclosure	Outdoor UV Stabilized Plastic
Mounting	Pole-Mount (Kit Included)
Operating Temperature	Temperature -35 to 75° C (-22 to 167°F)
Operation Humidity	5 to 95 % Noncondensing
RoHS Compliance	Yes
Shock & Vibration	ETSI300-019-1.4
Wireless Approvals	FCC Part 15.247, IC RS210, CE

3.1.1.5 Ubiquiti NanoStation Loco 5AC

El Ubiquiti NanoStation Loco 5AC (Loco5AC) es un dispositivo inalámbrico compacto y resistente diseñado para crear enlaces punto a punto de alta velocidad entre ubicaciones remotas en la banda de 5 GHz.

A continuación, algunas características del Loco 5 AC incluyen:

Antena direccional doble polarización integrada de 13 dBi de ganancia, velocidad de transferencia real de hasta 450 Mbps gracias a la tecnología 802.11ac, tecnología TDMA (Time Division Múltiple Access) que permite conectar a más de 300 clientes con baja latencia, procesador Atheros MIPS de 560 MHz con 64 MB de DDR2, Interfaz Ethernet Gigabit con alimentación PoE pasivo. [51]

Rango de hasta 5 km dependiendo del WISP, línea de vista y entorno, Modos de operación: AP, estación, WDS, Traffic Shopping, QoS, puente transparente o enrutamiento, completamente resistente a la intemperie para instalación permanente en ambientes difíciles.

Indicadores de intensidad de señal para alineación rápida y sencilla, para una instalación óptima, se recomienda montar el Loco5AC en el techo, alto y despejado de obstrucciones, utilizando su soporte de montaje integrado para poste, también se recomienda usar protección contra sobretensiones y cable Ethernet Cat5e o superior apantallado con drenaje a tierra. [51]



Ilustración 61. Ubiquiti NanoStation Loco 5AC.

Fuente: Elaboración propia.

Tabla 8. Ficha técnica de equipo Ubiquiti NanoStation Loco 5AC.

Fuente: [51].

Specifications	
Dimensions	179x77.5x59.1 mm (7.05x3.05x2.33")
Weight	180g (6.35 oz)
Power Supply	24V, 0.3A Gigabit PoE Supply
Max. Power Consumption	7W
Power Method	Passive PoE 2-Pair
Gain	13 dBi
Networking interface	10/100/1000 Mbps Ethernet Port

Channel Bandwidths	10/20/30/40/50/60/80 MHz
Processor Specs	Atheros MIPS 74Kc, 560MHz
Memory	64 MB DDR2
Cross-pol Isolation	20 dB Minimum
Max. VSWR	1.8:1
Beamwidth	45°(H-pol) / 45° (V-pol) / 45° (Elevation)
Polarization	Dual Linear
Enclosure	Outdoor UV Stabilized Plastic
LEDs	(1) Power
Mounting	Pole-Mount (Kit Included)
Operating Temperature	Temperature -40 to 70° C (-40 to 158°F)
Operation Humidity	5 to 95 % Noncondensing
RoHS Compliance	Yes
ESD/EMP Protection	±24kV Contact/Air
Shock & Vibration	ETSI300-019-1.4
Certifications	CE, FCC, IC

3.1.1.6 LiteBeam 5AC Gen2

Este dispositivo de banda ancha inalámbrica para exteriores, este modelo ha sido diseñado específicamente para ser una solución viable y accesible con respecto a costo/rendimiento para generar puentes de banda ancha inalámbrica de larga distancia por lo cual es de gran ayuda para lograr uno de los objetivos de este proyecto, como característica principal el LiteBeam es un dispositivo de puente inalámbrico punto a punto perteneciente a Ubiquiti Networks, además de esto incluye una antena direccional de alta ganancia que permite mejorar la fuerza y el alcance de la señal que se estaría generando como tecnología en cuestión posee una tecnología airMAX ac soportando el protocolo de esta tecnología lo que permite ofrecer un mejor rendimiento de la red y una menor latencia. [52]

La antena LiteBeam está equipada con una radio Wi-fi secundaria para una configuración y una gestión más sencilla a través de una aplicación móvil, está integrado en el feedhorn (estructura física que dirige las ondas electromagnéticas hacia la antena) de la antena por lo que así elimina la necesidad de conectores de cable. LiteBeam 5AC Gen 2 opera en el rango de frecuencia de 5 GHz proporcionando 23dBi de ganancia para una conectividad de larga distancia y utiliza un patrón de antena direccional para mejorar la inmunidad al ruido, posee una polarización Dual-linear lo que ayuda a mejorar la resistencia a la interferencia y el rendimiento en condiciones ambientales adversas, como patrón de radiación el

diseño de la antena esta optimizado para enfocar la señal en una dirección específica y así logra minimizar la pérdida de la señal. [52]

Al hablar del radio de frecuencia de la antena esta oscila en la banda de 5Ghz por lo cual permite un rango de canales disponibles entre 5150-5875MHz. El LiteBeam 5AC Gen 2 ofrece varias herramientas y métodos para gestionar y monitorear el dispositivo de manera eficiente, como herramienta de gestión utiliza la Ubiquiti Network Management System (UNMS) esta plataforma permite monitorizar y gestionar los distintos dispositivos Ubiquiti además de contar con una aplicación móvil UISP en la cual permite la configuración y gestión del dispositivo por lo que facilita la instalación y el mantenimiento en campo.



Ilustración 64. Equipo LiteBeam 5AC Gen2.

Fuente: Elaboración propia.

Seguridad

El LiteBeam 5AC Gen 2 incluye varias características de seguridad para proteger la red y datos las cuales son:

- ✚ **Cifrado WPA2:** WPA2 actúa como un guardián invisible, los datos viajan cifrados como un código secreto que solo el administrados y los dispositivos autorizados pueden descifrar, es decir, es como una fortaleza para la red Wi-fi que la resguarda de accesos no autorizados.
- ✚ **Firewall Integrado:** Firewall o también conocido como cortafuegos funciona como un monitorea supervisando el flujo de entrada y salida de los datos, examinando cada paquete de datos. Esto facilita el tráfico de información relevante y bloquea cualquier posible amenaza

- ✚ **Autenticación de Usuario:** Soporta autenticación avanzada para garantizar que solo usuarios autorizados puedan acceder al dispositivo y realizar configuraciones. [52]

Tabla 9. Ficha técnica de la antena LiteBeam 5AC Gen2.

Fuente: [52]

Dimensiones	362 x 273 x 203 mm (14,25 x 10,75 x 7,99")
Peso	907 g (2,00 libras)
Supervivencia del viento	Plástico estabilizado UV al aire libre
Kit de montaje	Kita de montaje en poste (incluido)
Consumo máximo de energía	7 vatios
Fuente alimentación	Adaptador PoE Gigabit de 24 V, 0,3 A (incluido)

3.1.1.7 Router Tenda Tx2 wifi6

El Router Tenda TX2 es un dispositivo de conexión de vanguardia que integra la conexión Wi-Fi 6 para brindar un desempeño sobresaliente y una experiencia de red inalámbrica de excelente calidad. A continuación, se detallará con exactitud las principales características y beneficios que posee el siguiente equipo: [53]

Tecnología Wi-Fi 6

Al poseer la tecnología Wi-Fi 6 este router Tenda TX2 representa la evolución en la conectividad inalámbrica ofreciendo velocidades superiores, una capacidad amplia y una eficiencia superior en relaciones con versiones anteriores de Wi-Fi la más reciente Wi-Fi 5 que brindaba un ancho de banda de mayor capacidad que facilitaba el manejo de grandes capacidades de datos. Esto resulta en una conexión más ágil y constante para una amplia gama de dispositivos conectados, lo que es ideal para espacios donde existen varios dispositivos conectados y necesita de alta velocidad ya sea empresas o condominios.

Doble Banda

El router Tenda TX2 al funcionar en ambas bandas de 2.4GHz y 5GHz, facilitando la distribución inteligente de dispositivo asignando una frecuencia exacta y adecuada para cada dispositivo, con el fin de garantizar un rendimiento óptimo y un fluido de ancho de banda al poseer la capacidad de doble banda mejora la conexión inalámbrica y disminuye la pérdida de ancho de banda, ofreciendo una experiencia de red más fluida y eficaz

Ethernet Gigabit

En el router Tenda TX2 cuenta con tres puertos LAN Ethernet Gigabit con capacidad de transmisión de hasta 1G de ancho de banda cada uno y un puerto WAN Ethernet Gigabit para el acceso a internet, brinda la opción de conexiones a dispositivos cableado para obtener una conexión de internet de alta velocidad y confiable.

Esta característica es ideal para actividades que requieren una conexión estable y de alto rendimiento, como juegos en línea, transmisión de video en 4K y transferencia de archivos grandes.



Ilustración 67. Router Tenda Tx2 wifi6.

Fuente: Elaboración propia.

Tabla 10. Ficha técnica de Router Tenda Tx2 wifi6.

Fuente: [54].

Hardware features	
Standards & Protocols	IEEE802.3, IEEE802.3u, IEEE802.3ab
Interface	10/100/1000Mbps WAN Ports 1 10/100/1000Mbps LAN Ports 3
Antena	4*6dbi External Antennas
Button	1* WPS/Reset Button
Power	Input: AC 100-240 -50/60 Hz Output: DC 12 V 1 A
LED indicator	1* LED
Wireless Features	
Wireless Standard	5GHz: IEEE 802.11 ax/ac/a/n 2.4 GHz: IEEE802.11 b/g/n
Frequency	2.4 GHz & 5 GHz
Data Rate	5GHz: 1201 Mbps 2.4 GHz: 300Mbps
Functions basics	OFMDA, MU-MIMO, Beamforming Signal Directional Transmission Technology

Wireless security	WPA-PSK/WPA2-PSK, Wireless Encryption Disable and Enable, WPS Connection
Software Features	
Tipo de connection an internet	PPPOE, Dynamic IP, Static IP, PPPoE, PPTP, L2TP Unify, Maxxis, Maxxis-special, Celcom, Digi
Network Protocol	IPv4, IPv6
Modo de operation	Wireless Router Mode Relay Mode Wireless AP mode
DHCP	DHCP Server List IP Address DHCP Client DHCP Static
Security	Client Filter Control Management Parental Remote Web
Security system	DHCP UDP WAN Ping from Internet TCP Forbid
DDNS	Support Dyn DNS TRO069 Unify 2.4GHz&5GHz Guest Network IPTV IPv6 Smart Power Bandwidth Control MAC Address
Features	System Log Web Management Backup Restore Configurations Remote Tenda APP Firmware Upgrade
VPN	IPsec Pass Through L2TP Pass Through PPTP Pass Through
Other Features	
Temperature	Temperature: 0 C - 40 C
Humidity	Humidity: 10 % - 90 %
Certifications	CE, RoHS, FCC
Supported pages	Default access address: tendawifi.com
Package content	Wireless Router, Ethernet Cable, Power Adapter, Installation Guide

3.1.1.8 HackRF One

El dispositivo HackRF One es un SDR este equipo permite la función de poder recibir y transmitir diferentes señales de radio dentro de un rango de 1 Mega Hertz hasta 6 Giga Hertz, posteriormente este dispositivo fue desarrollado y elaborado por “Great Scott Gadgets” con el fin del estudio y así desarrollar nuevos métodos

para las nuevas generaciones de la radio moderna, este equipo tiene diferentes formas de poder configurarse para sus funciones requeridas. [45]



Ilustración 70. HackRF One.

Fuente: Elaboración propia.

Tabla 11. Ficha técnica del HackRF One.

Fuente: [44]

HackRF One	
Rango de Frecuencia	1 MHz hasta 6 GHz
Funciona como un transmisor y receptor llamado transceptor, se comunica Semidúplex	
Total, de muestras por segundo	20 millones de muestras
Logra obtener 8 muestras en cuadratura I y Q con sus respectivos 8 bits	
Software Compatibles	SDR & GNU Radio
Ganancia TX & Rx puede ser configurado por medio del software simulando el filtro de banda base.	
Power	3.3 V, 50 mA
Tiene un conector SMA hembra	
Posee botones prácticos para el desarrollo de la programación.	
Posee un puerto USB 2.0 de gran velocidad	
Alimentación USB	
Sincronización de entradas y salidas reloj SMA	
Puerto de la antena es controlado	

3.1.1.9 Transceiver

Un transceiver es un dispositivo electrónico utilizado en comunicaciones para transmitir y recibir señales. Está compuesto por un transmisor y un receptor combinados en un solo circuito o carcasa. La función del 3 mi sol es transformar señales eléctricas o digitales en señales apropiadas para su transmisión mediante un medio de comunicación, ya sea por medio de cables, fibra óptica o en el aire en el caso de comunicaciones inalámbricas. En cambio, el receptor cumple la función inversa recibiendo la señal proveniente del medio de comunicación y las reconvierte en información entendible para el dispositivo receptor. [55]

En el caso de las comunicaciones por fibra óptica, el transmisor modula la señal de datos para su transmisión a través del cable, mientras que el receptor demodula la señal recibida, extrayendo así la información transmitida

Los transceiver se clasifican según la velocidad de transmisión y el alcance:

- ✚ Módulos SFP: Brindan velocidades de 100 Mbps a 4 Gbps con alcances de 500 m a 100 km.
- ✚ Módulos CFP: Son capaces de transmitir hasta 100 Gbps a distancias de 1000 km, perfectas para utilizar en redes WAN y remotas.

La versatilidad del transceiver lo hace indispensable en aplicaciones como telefonía móvil, redes de datos, transmisión de video y audio, y en entornos LAN e infraestructuras de telecomunicaciones para garantizar conectividad y transmisión fiable de datos. [55]



Ilustración 73. Transceiver TP-link MS110CS.

Fuente: Elaboración propia.

Tabla 12. Ficha técnica del equipo Transceiver.

Fuente:

Características de Transceiver	
Estándar & Protocolos	IEEE 802.3, IEEE 802.3u, IEEE 802.3x
Funciones básicas	Incorpora tecnología WDM Transferencia Half-Duplex/Full Link Fault Pass-rough & Far En Fault Amplia alcance de fibra hasta 20km
Puertos	1 puerto SC a 100 Mbps 1 RJ45 a 100 Mbps (MDI/MDIX)
Longitud de Onda	Transmisión 1550 nm/recepción 1310 nm
Transmisión WDM	1550 nm
Recepción WDM	1310 nm
M. red 10BASE-T	UTP cat 3,4,5 (100 m. max), EIA/TIA-568 100 Ω STP
M. red 100BASE -T	UTP cat 5, 5e (max 100m), cat 6, EIA/TIA-568 100Ω STP
M. red 100BASE-FX	Fibra monomodo

Indicadores LED	PWR, FDX/Col, Enlace /Act, SPD
Dimensiones	3.7x2.9x1.1 "
Fuente de Alimentación	Adaptador Corriente externo
Consumo max. energía	2.49 W
Seguridad y emisiones	FCC, CE, RoHS
Contenidos Paquete	Convertidores medios MC111CS Adaptador de corriente Guía de instalación
Ambiente	Temperatura de Funcionamiento: 0°C - 40°C Temperatura de Almacenamiento: -40°C-70°C Humedad de Funcionamiento: 10%-90% Humedad de Almacenamiento: 5% - 90%

3.1.1.10 Cable UTP cat6

El cable categoría utp 6 es también conocido con un par trenzado he utilizado en redes de áreas locales para poder transmitir datos a velocidades de hasta 1000 megabits por segundo entre las funciones de este cable tenemos que tiene un mayor ancho de banda a comparación con el cable de categoría 5, puede transferir datos a mayores velocidades además también de vídeo con alta definición, además, opera entre las frecuencias de hasta 250 MHz en cada par y una velocidad de 1Gbps lo que permite una transmisión de datos más rápida y confiable. [56]

Otra de las cualidades es que al ser de par trenzado ayuda a reducir la diafonía y mejora la calidad de la señal especialmente en entornos con interferencias eléctricas o electromagnéticas, también cumple con los estándares requeridos como lo son ANSI TIA EIA-568-B-2-1, los cuales garantizan su rendimiento y compatibilidad con diferentes equipos, también trabaja con los estándares 10BASE-T, 100BASE-TX Y 1000BASE-TX. [56]



Ilustración 76. Cable UTP Cat6.

Fuente: Elaboración propia.

Tabla 13. Ficha técnica de cable UTP Cat6.

Fuente: [56]

Cable UTP CAT 6	
Característica de Construcción	
Conductor	23 AWG Cobre Solido
Aislamiento	Polietileno
Formación	2 conductores aislados trenzados haciendo un par
Cableado	4 pares trenzados colectivamente con relleno en forma de estrella
Cubierta Exterior	Free de halógenos
Características Técnicas	
Diámetro exterior	6.2 ± 0.3 mm
T de servicio	0° C a +60°C
V. de Propagación	69%
Radio Curvatura min	F: 4xD; I: 8xD
Peso	4.10 Kg/100m
Normativa & Propiedades	
Norma Diseño Ref.	TIA/EIA-B.2-1, EN50173-1, ISO/IEC 11801
N. Propagador de llama	IEC 60332, IEC 60754
Free Halógenos	UNE-EN 60754
Baja Emisión	EN50399, IEC 61034
Clasificación CPR	EN 50575:2014 A1:2016

3.1.1.11 Fibra Drop

Una "fibra drop" se refiere a un tipo de cable de fibra óptica utilizado en redes de telecomunicaciones de última milla para conectar un punto de acceso principal a un punto de acceso secundario o final, como una casa o un negocio. Este tipo de cable se utiliza en redes de acceso de fibra óptica, donde se proporcionan servicios de Internet de alta velocidad, televisión por cable y servicio telefónico a los clientes. Es el cable de fibra óptica que se conecta desde el poste del proveedor hasta nuestras casas. La "fibra drop" corresponde a un cableado especial, el cual emplea en proximidades de transformadores y líneas de alta tensión, es dieléctrico, hp versátil y duradero, lo que facilita las conexiones en diferentes escenarios

Una de las características de la Fibra drop es que consta del denominado cable de Fibra Óptica monomodo, también es elaborado para las instalaciones al aire libre, otras de sus características es que soportas grandes distancias que sería hasta 1000 metros.

Además, la fibra está protegida por fibra de vidrio, como también el alambre de acero para que tenga una alta resistencia, también tiene una mínima sensibilidad a la flexión ya que esto permite una mayor flexibilidad en el momento de la respectiva

instalación y tiene diversas funcionalidades al momento de la transmisión de datos.
[57]



Ilustración 79. Fibra drop de 2 hilos.

Fuente: Elaboración propia.

3.1.1.12 Conector mecánico SC

Los conectores de fibra óptica son componentes esenciales que permiten la conexión precisa y confiable entre dos o más fibras ópticas, son piezas clave para establecer enlaces ópticos y son indispensables para el funcionamiento de las redes de fibra óptica, lo que hace que los adaptadores sean importante en una conexión es que poseen una alineación precisa ya que garantizan que los núcleos de las fibras ópticas estén perfectamente alineados, lo que es crucial para una transmisión de luz óptima. Referente a la conexión temporal y repetitiva esto permite conectar y desconectar las fibras ópticas de forma sencilla, sin dañarlas, lo que facilita el mantenimiento y la reconfiguración de la red. En este caso, los adaptadores están específicamente diseñados para su uso con fibra monomodo, que es el tipo de fibra que se utiliza para las conexiones de larga distancia.

Ventajas de los conectores mecánicos:

- ✚ Instalación Rápida: no requiere herramientas especiales ni equipos de fusión, lo que permite una instalación rápida y sencilla.
- ✚ Costo efectivo: menor costo inicial comparado con los equipos de fusión.
- ✚ Portabilidad: fáciles de transportar y usar en campo.
- ✚ Flexibilidad: Pueden ser utilizados en una variedad de aplicaciones y con diferentes tipos de fibra.

Desventajas de los conectores mecánicos:

- ✚ Pérdida de inserción: Los conectores mecánicos generalmente tienen una pérdida de inserción más alta comparada con las fusiones.

- ✚ Mantenimiento: Se necesita revisiones y cuidados periódico para garantizar que las conexiones se conserven limpias y operativas.
- ✚ Durabilidad: No poseen la misma durabilidad que las uniones fusionadas y pueden sería menos resistentes a condiciones ambientales severas



Ilustración 82. Conector Mecánico pulido SC.

Fuente: Elaboración propia.

A continuación, se elaborará una tabla con especificaciones técnicas del conector SC

Tabla 14. Datos técnicos del conector mecánico.

Fuente: Elaboración propia.

Dimensiones	362 x 273 x 203 mm (14,25 x 10,75 x 7,99")
Peso	907 g (2,00 libras)
Supervivencia del viento	Plástico estabilizado UV al aire libre
Kit de montaje	Kita de montaje en poste (incluido)
Consumo máximo de energía	7 vatios
Fuente alimentación	Adaptador PoE Gigabit de 24 V, 0,3 A (incluido)
Temperatura de Funcionamiento	-40 a 70 ° C (-40 a 158 ° F)

3.1.1.13 Amplificador de señal wifi EPUP-AB049 4000mW

El amplificador EDUP EP-AB019, es un amplificador de señal que opera en la banda 5725 – 5850 GHz, con esto ofrece una potencia de salida de 4000 W, el pinto principal de este dispositivo es el poder incrementar y mejorar la señal inalámbrica tanto de transmisión y de recepción, además, tiene diferentes usos como las comunicaciones de largo alcance, drones, etc. Uno de sus puntos

positivos es que son compatibles con las frecuencias de 2400 – 2500 MHz, también soporta los estándares IEEE 802.11b/g/n.

El funcionamiento se basa en conectar el Router o un Access Point con una antena extra, con el fin de poder amplificar la señal emitida por el Router, estas posibilidades que brinda este dispositivo que es muy útil en entornos donde la señal llega débil con esto se cubre áreas extensas.



Ilustración 85. Amplificador EP-AB049.

Fuente: Elaboración propia.

Se elaboro una tabla con las especificaciones técnicas del amplificador.

Tabla 15. Tabla de datos técnico de amplificador.

Fuente: Elaboración propia

Especificaciones	
Rango de Frecuencia	5725 - 5850 GHz
Voltaje de Funcionamiento	6 - 16 V
Recepción de Ganancia	15 dB
Ganancia de Transmisión	19 dB
Potencia de salida máxima	36 dBm
Potencia del disparador de entrada	Min: 3 dBm Max: 20 dBm
EVM	3% 28 dBm 802.11a a 54 Mbps OFDM 64QAM BW 20MHz
Figura de Ruido	3.0 dB
Fuente de Corriente	485 mA 12 V
Retraso del tiempo del interruptor	1 us
Indicador Led	Transmisor: verde, Receptor: rojo
Temperatura de Funcionamiento	22 to 158
Temperatura de almacenamiento	40 to 302
Humedad de funcionamiento	95 %de humedad
Conector RF	SMA-K; RP-SMA-K
Toma de Corriente	0.098 * 0.028 DC
Tamaño de la carcasa	76.6*35*14(mm)
Material de la Carcasa	Aluminio

3.2 DISEÑOS DE PROPUESTA EN SKETCHUP

Con el objetivo de tener una visualización más precisa y clara de los diseños de la red y posteriormente facilitar su implementación, se elaboraron 3 escenarios detallados que representa la arquitectura de la red. Los escenarios elaboraron tienen la finalidad de brindar un bosquejo que será fundamental, para una futura implementación de la red y tener detallado las rutas y componentes a utilizar.

Para la elaboración de estos escenarios se utilizó el software de sketchup, es un software que nos permite visualizar y además nos brinda herramientas para realizar un modelado en 3D, gracias a esto nos permite visualizar de manera precisa y eficiente el lugar dónde serán instalada y los componentes de la red en conjuntos a sus interconexiones.

Instalación del software sketchup

Para obtener este software de modelado debemos dirigirnos a la página oficial de Sketchup o al siguiente link para proceder con la descarga <https://help.sketchup.com/es/downloading-sketchup>.

Después de seleccionar el link, se nos abre una ventana donde se presenta dos opciones de descarga para dos sistemas operativos.

- [Download for SketchUp Pro 2024 for MacOS](#)
- [Download for SketchUp Pro 2024 for Windows](#)

Ilustración 88. Opciones de descargar para Sketchup.

Fuente: Elaboración propia.

Una vez teniendo el archivo “SketchUp-2024-0-553-221” procedemos a dar clic derecho sobre el archivo y seleccionar la opción de “ejecutar como administrador”. Esta acción hace que el archivo se ejecute e inicie el proceso de instalación del programa.

Se abre una ventana de sketchup donde se muestra los diferentes programas que viene dentro del paquete del instalador, además la ruta donde se encontrara el archivo despuesto de la instalación, despuesta de ya tener definido estos datos procedemos a seleccionar el botón de instalar para continuar con el proceso.

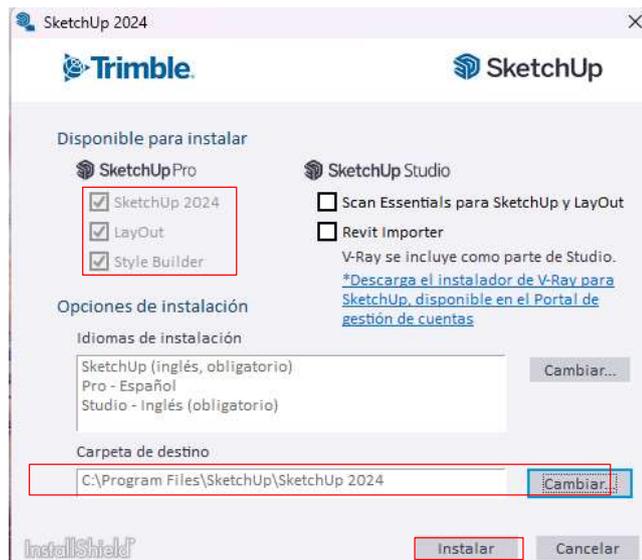


Ilustración 91. Pantalla de instalación de Sketchup.

Fuente: Elaboración propia.

Llegado a este punto después de espera el proceso de instalación nos muestra en la ilustración 31, la finalización de la instalación de sketchup.



Ilustración 94. Instalación completada de sketchup.

Fuente: Elaboración propia.

Una vez ya teniendo instalado el programa procedemos a abrir la cual nos presenta una interfaz de bienvenida que se muestra en la ilustración 28, donde debemos iniciar sesión para acceder a trabajar en el programa para ellos debe de tener en cuenta el siguiente aspecto:

- 🚦 El inicio de sesión con cuenta tanto con Gmail, Outlook y Apple, debe tener en cuenta que al iniciar con esta cuenta solo se concede un periodo de prueba de 7 días.
- 🚦 Inicio de sesión mediante código de activación de licencia.



Ilustración 97. Pantalla de inicio de sketchup.

Fuente: Elaboración propia.

3.2.1 Escenarios planteados 1

En el primer escenario, el edificio del laboratorio de telecomunicaciones y los laboratorios cercanos de la facultad de Sistemas y Telecomunicación de la Universidad Estatal Península de Santa Elena fueron replicado con exactitud para facilitar al momento de la implementación de los equipos. En el proceso de réplica del edificio no sólo abarcó la estructura física del laboratorio, si no también todos los detalles necesarios para construir escenario de referencia en el proceso de instalación y colocación de equipos, con el fin de garantizar una instalación eficaz y un corto tiempo.

En el edificio, se diseñó la infraestructura y todos los equipamientos necesarios, para el desarrollo del tema propuesto, los cuales son necesarios para tener una base de lo que incluye una instalación de sistema CCTV.

Además, se consideraron cuidadosamente los aspectos de diseño para asegurar que el entorno replicado fuera funcional y realista, proporcionando así un espacio adecuado para la enseñanza y la práctica en telecomunicaciones. A continuación, se explicará en detalle el proceso de diseño, abordando cada uno de los componentes mencionados y su integración en el proyecto global. Este análisis incluirá desde la planificación inicial hasta la implementación final, asegurando que todos los elementos funcionen de manera cohesiva y efectiva

Antes de comenzar, es esencial tener instalado previamente el programa SketchUp en nuestro ordenador, una vez asegurada la instalación procedemos a abrir el software. Al hacerlo, nos encontramos con una ventana de inicio que nos brinda diversas opciones, dentro de esta plantilla inicial podemos elegir varias plantillas diseñadas para adaptarse a diferentes requerimientos del proyecto. Para nuestro

propósito específico, optamos por seleccionar la plantilla denominada “Sencillo”, lo cual utiliza medidas en metros.



Ilustración 100. Selección de espacio de trabajo dentro de Sketchup.

Fuente: Elaboración propia.

Seleccionado la plantilla de trabajo, se desplegará una ventana en la que se mostrará las distintas herramientas requeridas para elaborar el diseño propuesto. Esta interfaz está diseñada para facilitar la obtención de todas las funciones necesarias posibilitando que los usuarios se relacionan eficazmente con el software. En esta área de trabajo, se encuentran herramientas para dibujar, modelar y modificar además de contar con herramientas para poder visualizar y ajustar detalles técnicos y medidas apropiadas de los edificios replicado para el desarrollo del tema propuesto.

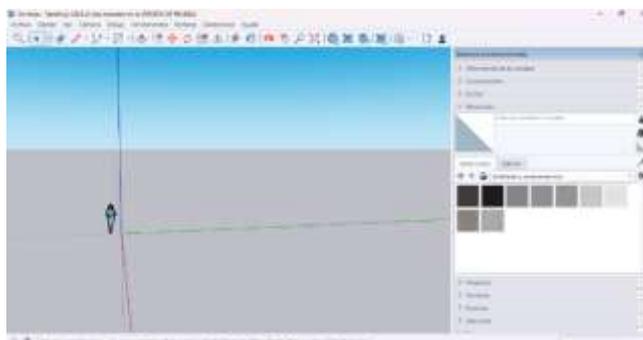


Ilustración 103. Presentación de espacio de trabajo.

Fuente: Elaboración propia.

A continuación, se procedió a modelar los equipos que se utilizarán para la infraestructura CCTV que se implementará en los exteriores del laboratorio de telecomunicaciones. De los cuales son los siguientes componentes:

- ✚ Cámara de seguridad que se asemeja a la utiliza de la propuesta.
- ✚ Ubiquiti NanoStation Loco M2
- ✚ Monitor

- ✚ Router Tenda
- ✚ NVR Reolink
- ✚ Ubiquiti NanoStation M2



Ilustración 106. Modelado de equipo utilizado dentro del modelado.

Fuente: Elaboración propia.

Una vez finalizado el diseño de los equipos, procedimos a la elaboración del diseño arquitectónico del edificio que alberga el laboratorio de telecomunicaciones, la sala de automatización y la sala de investigación. Asimismo, se realizó un diseño detallado del laboratorio de cisco tanto en sus aspectos exterior como interior, especificando minuciosamente de los componentes que integran cada laboratorio. Para asegurar la precisión y eficacia del diseño, se resaltó particularmente la réplica realizada de la estructura y organización de los laboratorios previamente mencionado, dentro del diseño se elaboraron el equipamiento específico de cada laboratorio. Con el objetivo de realizar esta réplica a detalle es proporcionar una ilustración visual exacta y minuciosa que facilite la identificación de los componentes esenciales de la propuesta.

El propósito de este enfoque es minimizar cualquier posible inconveniente durante la fase de instalación, especialmente es lo que respecta a la ubicación de la infraestructura CCTV. Al tener un diseño que refleje fielmente las características y las configuraciones de los laboratorios, se puede planificar con mayores énfasis la instalación de cámaras de seguridad, antenas y el sistema de cableado estructurado, garantizando así una implementación eficiente y sin errores.



Ilustración 109. Réplica del laboratorio de la facsistel dentro de sketchup.

Fuente: Elaboración propia.

En el desarrollo de instalación del sistema CCTV dentro de los laboratorios, se determinó las ubicaciones de cada cámara iniciando con el primer punto de instalación situado al lado derecho de laboratorio. Esta ubicación facilitará obtener una vista destacada de laboratorio de cisco y de laboratorio de suelos vinculados con la carrera de ingeniería civil, proporcionando una cobertura completa de los sectores fundamentales.

Además, dentro del diseño se situó una antena NanoStation M2 junto a la cámara RLC-510AW. Dicha antena fue colocada de manera que funcione como una receptora de señal, lo cual es una parte primordial dentro del sistema para evitar pérdida de vídeo o imágenes, entre el lapso de la cámara hacia el reproductor NVR. Esta configuración garantiza que las imágenes capturadas mediante la cámara en medio de las transmisiones se han imágenes de alta calidad y libre de congelación de píxeles lo cual es esencial para la vigilancia y seguridad del área.

Mediante el diseño se recalcó varias medidas fundamentales para el momento de la instalación, unos de los datos atamanes cuenta es un medio de conexión conectado a la antena, para antena es cuestión está conectado mediante cableado UTP. El cableado que conecta la antena con el router, dicho router se encuentra ubicado estratégicamente dentro del laboratorio de telecomunicaciones. Garantizando una transmisión de datos eficiente y segura.

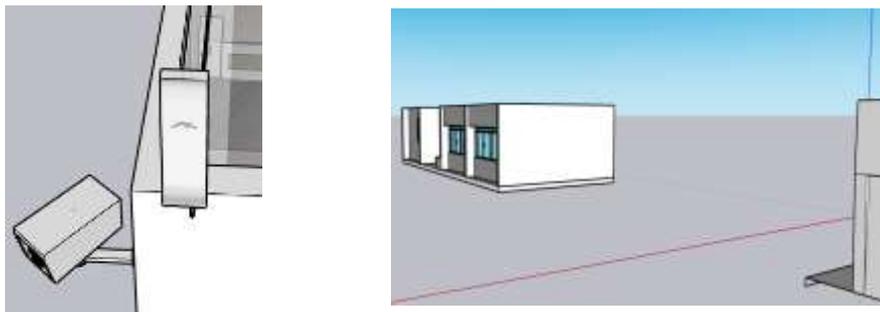


Ilustración 112. Elección del punto de instalación de la cámara para el punto 1.

Fuente: Elaboración propia.

Para la segunda ubicación, se ha elegido estratégicamente la parte trasera del bloque, específicamente en el costado izquierdo. Al igual que en las instalaciones anteriores, esta cámara también estará equipada con una antena Ubiquiti NanoStation Loco M2, siguiendo la misma línea de configuración que las cámaras previas para asegurar una uniformidad en el sistema de vigilancia.

Dentro de la ubicación elegida se logran visualizar de manera efectiva los sectores del estacionamiento conectado al laboratorio de Cisco, así como la entrada y salida correspondiente del laboratorio. Dicha selección de esta ubicación nos permite el monitoreo de zonas de alto tráfico, garantizando una mayor seguridad y una observación continua y detallada de los movimientos tanto vehiculares como peatonales. En conjunto con la instalación y la configuración de los equipos garantiza una gestión del entorno más segura y regulada, lo cual es esencial para evitar incidentes y de misma manera poder responder eficazmente ante cualquier regularidad presentada en las áreas de cobertura de esta cámara.

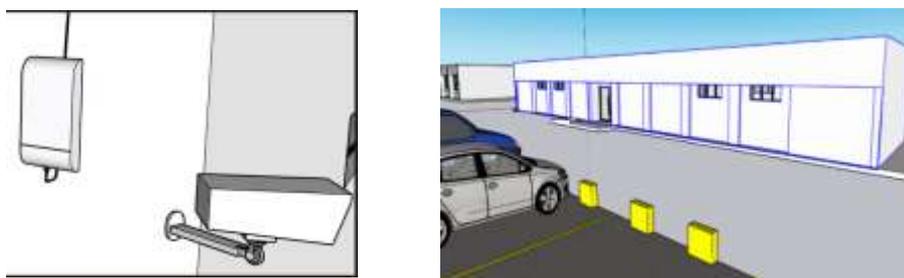


Ilustración 115. Ubicación de la última cámara.

Fuente: Elaboración propia.

La configuración actual muestra la ubicación estratégica del router principal y cómo se organiza el recorrido del cableado UTP desde este punto hacia las diversas antenas y hacia el NVR. Cabe recalcar que el NVR está ubicado en la bandeja la

inferior de dónde se encuentra colocado el router principal, la ubicación escogida logró optimizar el espacio maximizando de esta manera el aprovechamiento de cada bandeja ubicada en el rack así mismo permite una conexión cableada directa sin tanto recorrido entre el NVR y el router, sin embargo, el equipo puede situarse en cualquier lugar de laboratorio siempre y cuando sea de una forma cableada y respetando los estándares mi norma de cableado estructurado mediante un UTP que es la forma de conexión del NVR para acceder al internet.

Cuando el NVR se encuentra en diferentes redes domésticas o empresariales Y se necesita visualizar las cámaras enlazada a la NVR Sea con configuraciones especiales como reenvío de puertos en ambos routers, con el fin de poder conectar ambas redes y poder visualizar en todo tiempo las cámaras conectadas al NVR. Mientras el NVR se encuentre conectado de manera directa al router se podrá visualizar el NVR mediante la aplicación o desde el lugar físico ubicado en el NVR, en cambio si las cámaras se encuentran conectadas de manera directa al NVR para visualización de ellas se conecta a la red interna de NVR ya que no se podrán visualizar desde la red principal en este punto entra los mencionados anteriormente con el reenvío de puertos para la visualización de las cámaras en diferentes direccionamiento de redes.



Ilustración 118. Ubicación del router y NVR Reolink dentro del Rack.

Fuente: Elaboración propia.

En la ilustración 41, se logra visualizar las diferentes conexiones realizadas de los equipamientos mediante cableado UTP en el router Tenda, iniciando con la conexión WAN la cual permite el acceso al internet del router proveniente del switch HP principal el cual se encargar de proporcionar internet a todos los

equipamientos del laboratorio, el siguiente puerto de conexión del router se extiende hacia el NVR de manera cableada.

Las tres entradas restantes en el router están meticulosamente ocupadas por conexiones a tres antenas, cada una dedicada a mejorar el acceso y la estabilidad de la red para las cámaras de seguridad. Esta configuración asegura que las cámaras puedan operar de manera eficiente y sin interrupciones, facilitando una vigilancia continua y de alta calidad. Además, esta disposición de las conexiones en el router facilita la administración y el mantenimiento del sistema, proporcionando una plataforma robusta para la gestión de la seguridad del laboratorio

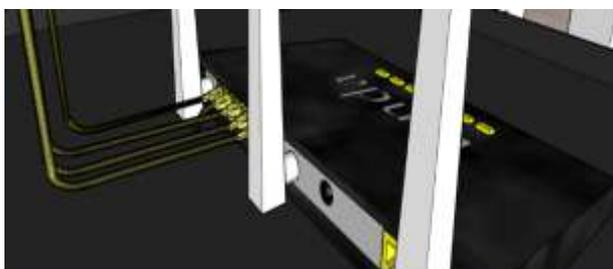


Ilustración 121. Conexiones del router hacia cada equipo.

Fuente: Elaboración propia.

Para finalizar, una vista panorámica permite apreciar las ubicaciones estratégicas de las cámaras a lo largo del bloque de laboratorios. Desde esta perspectiva, se puede observar claramente cómo cada cámara ha sido colocada para maximizar la cobertura y la eficiencia del sistema de vigilancia.

Adicionalmente se aprecia en la ilustración 42, el recorrido detallado en el exterior de laboratorio el cual se verifica de una conexión directa entre el router principal y las antenas ubicadas en sus posiciones correspondiente, la ejecución del cableado de manera correcta garantiza una transmisión de datos eficiente y sin interrupción red sistema de videovigilancia planteado.

El diseño realizado muestra las ubicaciones y el recorrido del cableado que deben realizarse el momento de la implementación del escenario, la realización al detalle del diseño permite tener una idea clara al momento de la ejecución de escenario, lo cual garantiza una correcta instalación y ahorro de tiempo.

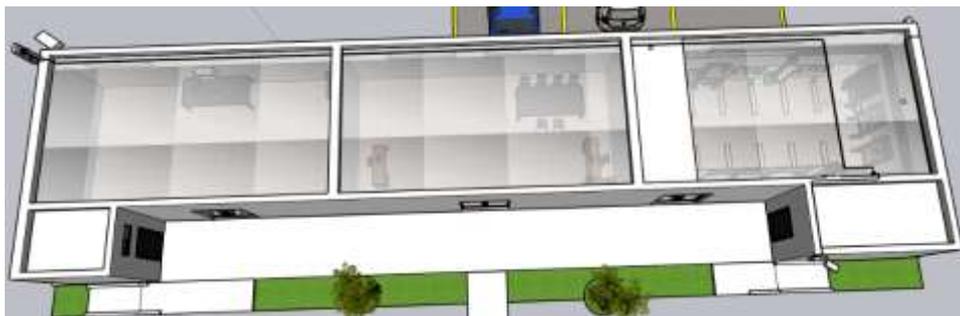


Ilustración 124. Visión panorámica de las ubicaciones de las cámaras y sus conexiones.

Fuente: Elaboración propia.

3.2.2 Escenarios planteados 2

Para el diseño del segundo escenario, empleamos la estructura base del primer escenario, complementándola con la incorporación de nuevos equipos destinados a la implementación de un enlace PTM (Punto a Multipunto) dentro del sistema CCTV propuesto. Los componentes añadidos para este escenario incluyen:

- ✚ Cámara RLC-510AW
- ✚ NanoStation Loco 5AC
- ✚ LiteBeam M5 Gen 2 AC
- ✚ Router TP-Link AC1200
- ✚ Router Tenda 779CB0
- ✚ NVR Reolink
- ✚ Monitor

Estos elementos han sido seleccionados específicamente para optimizar la funcionalidad y eficiencia del sistema en un contexto más amplio y complejo.

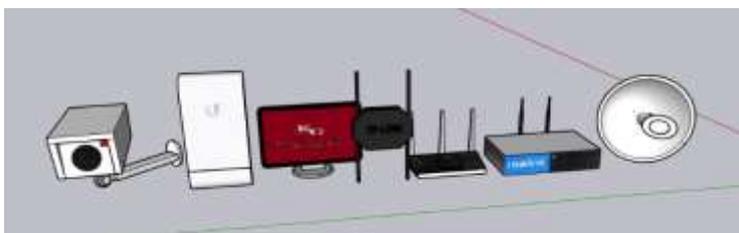


Ilustración 127. Modelado de equipo a utilizar.

Fuente: Elaboración propia.

Cuando se establece una conexión de punto a multipunto, es necesario designar una antena que actúe como emisora de la señal y que funciona en calidad de antena principal, y que desde allí se logre enviar la señal hacia las antenas receptoras. Para

esto, la antena LBE-5AC-GEN2 fue elegida como principal , y se conecta mediante un adaptador PoE, que a su vez proporciona tanto energía como conectividad.

Por otro lado, el PoE en la ranura LAN se conecta directamente al router Tenda, asegurando que la antena principal tenga acceso a Internet. El router Tenda por su parte es la que se encarga de conectar el acceso a internet a la antena, para así mediante el enlace brinda a las antenas receptoras, como la NanoStation Loco 5AC, para luego ser captarán la señal emitida por la antena principal y posteriormente ser retransmitidas, extendiendo así la cobertura de la red.

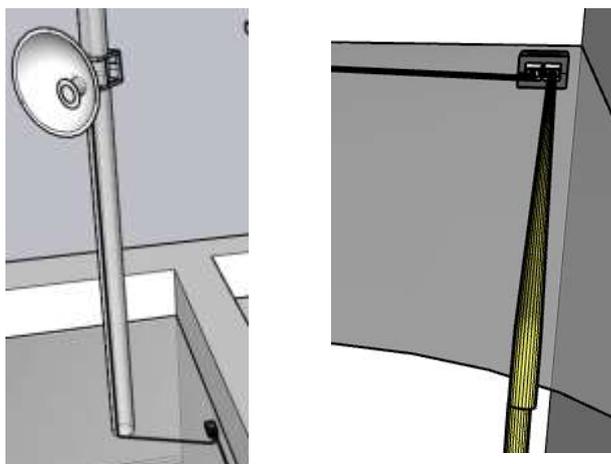


Ilustración 130. Ubicación de la antena emisora y conexión de la antena mediante PoE.

Fuente: Elaboración propia.

Para la primera cámara, se ha decidido mantener la misma localización que se encuentra en el primer escenario, tenían establecida la ubicación se incorporó una antena NanoStation Loco 5AC, dicha antena funcionará como receptora de la señal emitida de la antena principal.

Para que el funcionamiento sea de manera óptima se incorporó un router TP-Link en la configuración el cual se conectará mediante el de la antena conectado del puerto LAN del PoE hacia el puerto WAN de dicho router. Esta conexión es esencial para facilitar la comunicación y distribución de la señal entre la cámara y el sistema de seguridad general.

La señal emitida por el router es esencial para la operatividad de la cámara y cumplir con lo propuesto en el tema, dicha señal permitirá la conexión a la cámara y a su vez pueda capturar y transmitir imagen de vídeo en tiempo real hacia el dispositivo NVR.

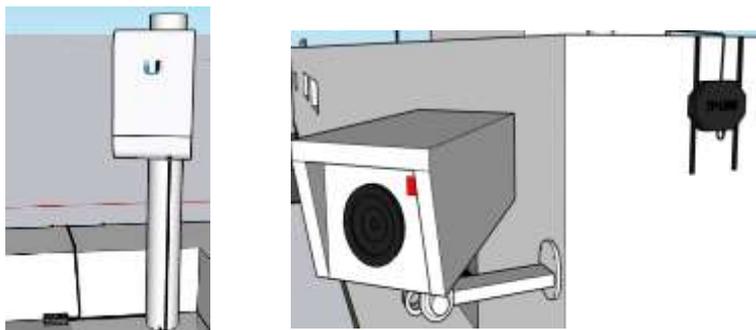


Ilustración 133. Ubicación de la primera antena receptora conjuntos a la primera cámara.

Fuente: Elaboración propia.

Se terminó la segunda posición de la cámara siguiendo el mismo esquema del primer escenario, Tomando en sí la segunda ubicación del anterior escenario, siguiendo de la misma manera en esta segunda antena receptora se replicó el mismo procedimiento que de la antena anterior ya que al trabajar de la misma manera tendrán las mismas especificaciones y configuraciones tanto en antena como en la incorporación del router.

Al replicar e instalar el equipamiento en ambas ubicaciones garantiza una uniformidad en el sistema punto a multipunto, obteniendo una gran calidad y eficiencia en el sistema de transmisión y recepción de señales.

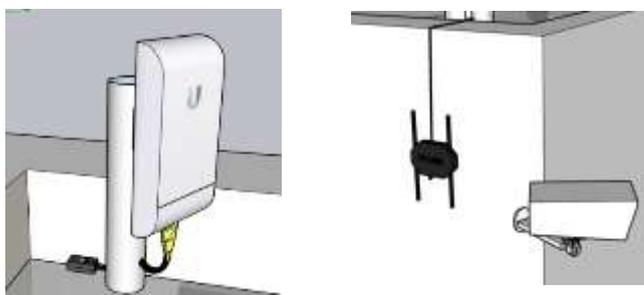


Ilustración 136. Ubicación de la segunda antena receptora conjunto a su cámara.

Fuente: Elaboración propia.

En este escenario particular, la configuración del cableado que se dirige hacia el router está limitada a tres posiciones de cableado disponibles. La primera de estas posiciones, etiquetada como WAN, está dedicada al acceso a Internet del router, proporcionando la conexión esencial para todas las operaciones en línea. La entrada subsiguiente ya está ocupada por un cable UTP que conecta directamente al NVR Reolink, un componente crucial para la grabación y gestión de las imágenes captadas por las cámaras.

Mediante la ilustración 47, apreciamos los puertos utilizados en el roster principal, lo cual se utiliza un puerto LAN conectado directo del puerto LAN del PoE de la antena LBE-5AC-GEN2, con el fin de brindar acceso a la antena emisora de la red.

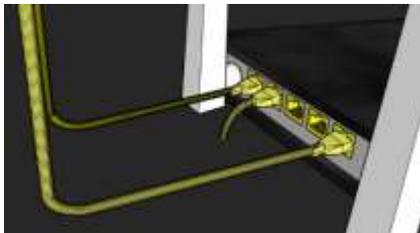


Ilustración 139. Conexión del router hacia la antena receptora y NVR.

Fuente: Elaboración propia.

En la ilustración 48, se presenta una vista panorámica detallada que facilita la observación de la disposición de las antenas emisoras y receptoras. Estas antenas son fundamentales para la configuración de un enlace punto a multipunto dentro del sistema de comunicación. En comparación con el primer escenario, esta ilustración destaca una modificación significativa: la sustitución del cableado estructurado por conexiones inalámbricas, lo cual representa un avance en términos de eficiencia y estética.

Al simplificar el cableado estructurado mejora la flexibilidad y la estabilidad en el sistema al no contar con puntos de fallos facilitando posibles expansiones o modificaciones del sistema sin grandes interrupciones. Al visualizar la ilustración 48, se aprecia la efectiva conexión inalámbrica punto a multipunto.



Ilustración 142. Vista panorámica de las ubicaciones de antenas en los alrededores del edificio de los laboratorios de Facistel.

Fuente: Elaboración propia.

3.2.3 Escenarios planteados 3

En el tercer escenario estará propuesto y elaborado dentro del bloque de los laboratorios de la Facultad de Telecomunicaciones, se servirá del diseño donde están empleados diversas maneras de enlazarse en la red tales como, el cableado

UTP, redes inalámbricas y fibra óptica, con el Wi-Fi se trabajarán con dos frecuencias que son la de 2.4 y 5 GHz, con el fin de realizar una comparativa de cada tecnología utilizada y en diferentes entornos.

Al igual que en los escenarios anteriores, se presentan los equipos que se utilizarán para el modelado en el software SketchUp. Este modelado proporciona una mejor perspectiva y planificación visual, facilitando el proceso de instalación y asegurando que todos los componentes se ubiquen correctamente. Los equipos por usar son los siguientes:

- ✚ Cámara RLC-510AW
- ✚ Router Tenda 779CB0
- ✚ NVR Reolink
- ✚ Transceiver TP-Link
- ✚ Monitor



Ilustración 145. Modelado de equipos utilizado en el 3 escenario.

Fuente: Elaboración propia.

Para la ubicación de la primera cámara, se decidió optar por la misma posición que en el primer escenario, introduciendo un cambio importante en el método de conexión: esta cámara se conectará utilizando fibra óptica. Esta elección se justifica por la implementación de un equipo transceptor, que es capaz de convertir la señal de fibra óptica en una señal compatible para transmisión a través de cable UTP.

Para esta ubicación se utilizará la tecnología Fibra óptica donde va a existir una mejoría en la calidad y en la velocidad de la transmisión del contenido audiovisual, en este punto es esencial para los diferentes estudios especialmente en seguridad donde los requisitos son esenciales que son, alta definición y una transmisión eficaz en tiempo real, sin tener delay, al utilizar Fibra óptica nos asegura una conexión consolidada obteniendo así un desempeño excelente.

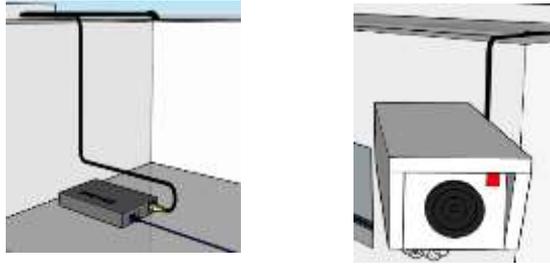


Ilustración 148. Ubicación de la primera cámara y conexión mediante Transceiver.

Fuente: Elaboración propia.

Para la ubicación de la segunda cámara, se optó por una nueva posición en la cual esta será en la parte frontal del laboratorio. En esta segunda ubicación, la elección ha recaído en la utilización de tecnología inalámbrica, empleando tanto las bandas de 2.4 GHz y la banda de 5GHz , con estos métodos nos posibilitará realizar un análisis a profundidad del desempeño de la transmisión de contenido audiovisual, tomando en cuenta bajo las diversas condiciones de frecuencias utilizadas, esto nos da un resultado muy esencial para poder así establecer cuan efectivo es el uso de esta tecnología inalámbrica en ambientes donde exista una supervisión exhausta.

A continuación, en la ilustración 51 se muestra la ubicación de la cámara sin la presencia de cualquier dispositivo extra o accesorio que necesite el equipo a utilizar, brindando la información de a dónde va a enfocar el dispositivo y obviamente en la tecnología en la que se está realizando la práctica, facilitando su habilidad para funcionar de manera autónoma sin ayuda equipos adicionales.

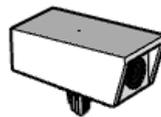


Ilustración 151. Segunda ubicación en base a medio inalámbrico.

Fuente: Elaboración propia.

Para esta práctica se decidió usar la misma posición y ubicación de la cámara como en el primer escenario, teniendo en cuenta que utilizamos una red híbrida seleccionamos un medio de transmisión diferente, dónde en este escenario se va a utilizar la red cableada también llamada cable UTP, que va a estar conectado directamente al dispositivo NVR, con el fin de realizar una comparación entre la red inalámbrica a la red cableada y poder evaluar la efectividad y cuán confiable es cada método de transmisión, uno de los enfoques que nos va a permitir observar la comparación antes mencionada para poder determinar qué tan positivo es el nivel

de seguridad del sistema de vigilancia integrado y ver cuál es el óptimo rendimiento que nos pueda dar..

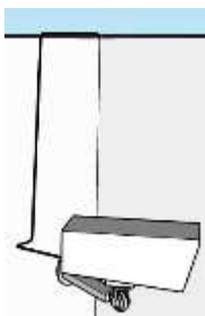


Ilustración 154. Ultima ubicación median cableado UTP.

Fuente: Elaboración propia.

El equipo NVR va a estar conectado a las cámaras según el medio de transmisión que si ha decidido, ya que existen diversas maneras en realizar la conexión a las cámaras, en este caso como se muestra en la ilustración 53 donde del el equipo NVR parte de un cableado UTP donde se dónde se logra una conexión a un dispositivo Transceiver, ya que este equipo tiene la capacidad de convertir la señal eléctrica a una señal óptica logrando así de que nuestros equipos trabajen directamente con fibra óptica, en este sentido se logra ver cómo se logra una convergencia de los tipos de tecnología como pueden ser la conversión de señales, dando un punto positivo de adaptabilidad en diferentes medio de transmisión, así se logra ineficaz ancho de banda para poder así mejorar la calidad y la velocidad de transmisión del contenido audiovisual.



Ilustración 157. Conexión del NVR hacia las diferentes cámaras.

Fuente: Elaboración propia.

A continuación, para el siguiente escenario no ofrece una vista panorámica todo el sistema de conexión que se implementa en cada cámara además, el trayecto donde

se ha utilizado el medio de transmisión de fibra óptica va conectado hacia la primera cámara, donde se puede resaltar la eficacia y la nitidez por donde se transmite hasta llegar al equipo NVR y se observará las imágenes en pantalla, también se utiliza la segunda cámara que va conectada inalámbricamente, donde se muestra la flexibilidad y una correcta instalación, en otro punto para la otra cámara se utilizará el sistema convencional de instalación de una cámara por medio de cableado UTP para tener la comparativa de los 3 casos de las instalaciones de las cámaras y sus medios de transmisión, tal como se muestra es la ilustración 54



Ilustración 160. Vista panorámica del desarrollo del tercer escenario.

Fuente: Elaboración propia.

3.3 IMPLEMENTACIÓN DEL DISEÑO DE LA PROPUESTA

La implementación se inicia con la configuración meticulosa de cada equipo necesario y adaptándose acá escenario planteado anteriormente, la calibración de los dispositivos garantiza que operen de manera óptima. Este procedimiento abarca modificaciones técnicas como la asignación de direccionamiento IP, las actualizaciones de firmware y la incorporación de protocolos de comunicación, además de la comprobación de la conexión entre los equipos utilizados en los diferentes escenarios.

3.3.1 Configuración e instalación de NVR Reolink

Para la configuración del NVR, se debe de conectar un monitor para facilitar su configuro o caso contrario no se podrá configurar, teniendo conectado a alimentación y el momento procedemos a encender el NVR el cual nos presentan la interfaz de inicio juntos con paso a seguir para su configuración.

Iniciando con los parámetros generales como establecer el idioma, la resolución de pantalla, la fecha y por último la hora, estos datos se visualizan en ilustración 55.

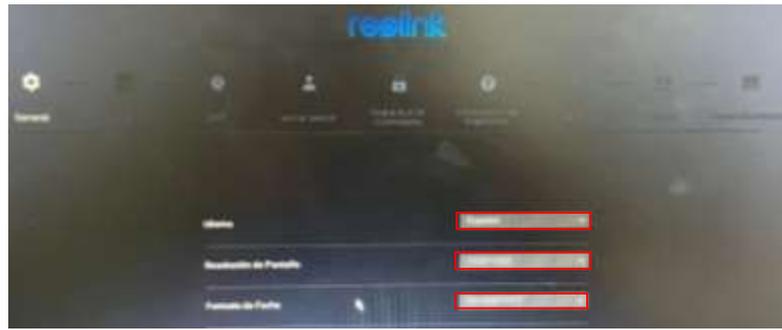


Ilustración 163. Configuración de parámetros generales del NVR.

Fuente: Elaboración propia.

Continuando se estableció parámetros de inicio de sesión los cuales permitirán el no acceso a cualquier persona así se evitar el manipuleo de personas no autorizadas, dicha contraseña se estableció la siguiente:

✚ Contraseña: tesisupse

Así mismo, si se llega a perder la contraseña o se olvide se determinó preguntas de recuperación de contraseña así mismo para evitar de no ser fácil el recuperar la contraseña establecida o cambiar la mismo, dicha pregunta se determinó la siguiente:

✚ Pregunta: ¿Tutor de tesis?, la respuesta establecida es el apellido del tutor en este caso en Amaya.

Previamente se incorporó un disco de 2Terabytes para guardar las grabaciones de las cámaras dentro de la configuración se debe formatear para así evitar cualquier archivo o daño del disco.

El NVR posee de la cualidad de crear redes wireless tanto en bandas de 2.4 GHz y 5 GHz, las cuales de dejaron habilitada ya que posteriormente en otros puntos serán utilizadas para análisis, dichas redes se estableció los siguientes parámetros

Para 2.4 GHZ.

✚ SIID: NVR TESIS 2.4G

✚ Password: T123456789

Para 5 GHz.

✚ SIID: NVR TESIS 5G

✚ Password: T123456789

Para que el NVR se conecte a las cámaras, y dependientemente el medio de conexiones debemos de habilitar el acceso al internet para ellos se designó desde el

router principal un puerto ethernet directo al NVR, dentro del mismo se debe de configurar tanto un IP estática, mascara de subred y sobre todo la puerta de enlace esto datos se visualizaran en ilustración 56, además en el apartado se debe configurar el domino de red que dará el NVR cuando se conecte una cámara ya sea por red inalámbrica o cableada dicho domino se estableció 192.168.1.2 hasta 192.168.1.254.

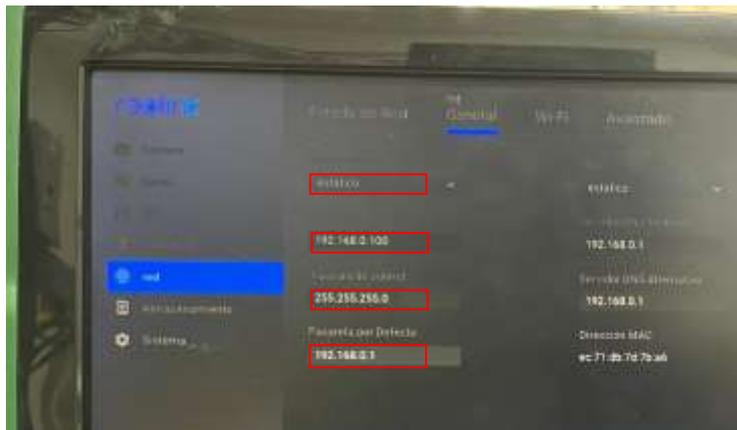


Ilustración 166. Parámetros de red del NVR

Fuente: Elaboración propia.

Como último paso en la configuración del NVR se estableció los parámetros de los puertos de igual manera que se realizó en las cámaras de los cuales se habilitaron todos así permite la conexiones con otros dispositivos, de los servidores a descargar el onvif ya es se determinó con el puerto 8080 esto los permite conectar con otros equipos de cámaras de diferentes marcas, los datos de puertos y los servidores habilitados se presenta en la siguiente ilustración 57.

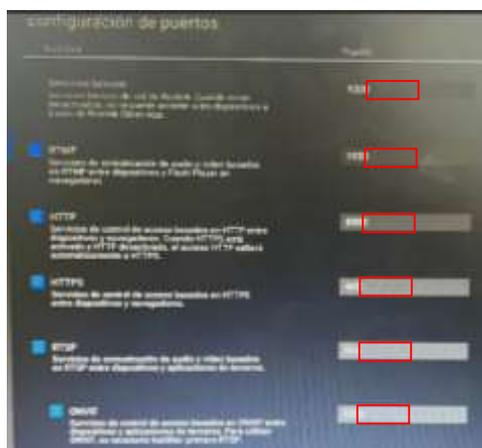


Ilustración 169. Habilitar y asignación de puertos del NVR

Fuente: Elaboración propia.

3.3.5 Rendimiento de medios de transmisión

Con el propósito de evaluar el rendimiento de los diferentes medios de transmisión, conectados directamente al NVR en base a los estándares de compresión de video H.264 y H.265, se definió la siguientes metodología y parámetros a analizar, de los cuales tenemos lo siguientes: Latencia y Retardo.

- ✚ Ancho de banda.
- ✚ Evaluación de eficiencia de almacenamiento
- ✚ Calidad de video.
- ✚ Estabilidad de transmisión.

En la elaboración de cada punto se optó en la realización de una guía detallada, lo cual permitió una ejecución organizada y estructura.

Guía de paso a paso para medir latencia y retardo.

1. Conectar previamente el equipo ya sea computadora o laptop a la misma red del NVR logrando capturar el tráfico entre el NVR y la cámara, previamente se debe asegurar que el NVR este configurado al estándar a utilizar ya sea H.264 o H2.265
2. Descargar e instalar wireshark para la captura del tráfico de la red, para poder descargar el programa dirigirse al siguiente link <https://www.wireshark.org/#downloadLink>, y proceder con la descarga del software, una vez descargado el software inicie el proceso de instalación siguiendo las indicaciones que brida al momento de instalar.
3. Iniciar el proceso de captura de paquetes en wireshark, abriendo wireshark y seleccionando la interfaz de red correspondiente a la conexión del NVR puede ser tanto a red Ethernet o Wi-Fi una vez seleccionado la interfaz presionar “Start”.
4. Filtrar el tráfico del NVR mediante filtro aplico dentro de wireshark, para solo capturar el tráfico entre el NVR y las cámaras, para ellos se deben utilizar las IP tanto del NVR y de las cámaras, introducir el siguiente comando `ip.src == [IP del NVR] || ip.dst == [IP de la cámara]`, esto nos ayuda con el análisis.
5. Activar la transmisión de video en tiempo real en el NVR, además verificar que ambos equipos este con el estándar H.264 o H.265 para que refleje el tráfico con el estándar seleccionado.

6. Identificar el primer paquete que indique el inicio de la transmisión de video desde el NVR hacia la cámara. Dichos paquetes pueden ser de varios protocolos como RTSP o en paquetes HTTP/HTTPS, marcar el tiempo de inicio de este paquete en wireshark.
7. Medir el tiempo de respuesta, se realiza al momento que la transmisión llegué al cliente de visualización, encontrar el primer paquete de respuesta que el NVR envié de regreso, esto paquetes suelen ser ACK si en el caso de protocolo o un paquete de video en RTSP.
8. Realizar lo mismo paso para los diferentes medios de transmisión Fibra, UTP y Wi-Fi y comparar el rendimiento en cada uno, para obtener un promedio más preciso realizar el mismo procedimiento varias veces.

Guía de paso a paso para medir el ancho de banda.

1. Configurar la cámara para que transmita en H.264 o H.265 y asegurar de que el NVR este recibiendo esta transmisión para cada medio de transmisión ya sea en Fibra, UTP y WI-Fi, lo cual permitirá realizar la medición.
2. De igual manera que en la guía anterior se debe de filtrar el tráfico solo en los dispositivos a analizar comando `ip.addr == [IP de la Cámara] || ip.addr == [IP del NVR]`.
3. Analizar el ancho de banda mediante wireshark, se dirige a Statistics > IO Graphs, cambiar la unidad a bits por segundo (bps) para facilitar el análisis del consumo de ancho de banda.

El mismo procedimiento se debe realizar para analizar el ancho de banda de los diferentes medios de transmisión, compara los datos obtenidos tanto en H.264 y H.265.

Guía de paso a paso para medir la calidad de video en PSNR y SSIM

1. Realizar grabaciones en segmentos de vídeo desde la cámara en el NVR configurando en H.264 o H.265. La duración del vídeo debe tener una duración mínima de 1 minuto y asegurando de que el contenido de la escena sea similar para facilitar la comparación

De la misma manera grabar un vídeo de referencia, Dicha grabación debe ser de un segmento de vídeo idéntico de la grabación con el estándar de compresión. Esto servirá como puente de comparación para.

2. Descargar los vídeos grabados desde el NVR tanto los vídeos comprimidos como el vídeo original los cuales una vez descargados deben ser identificados con nombres propios para evitar confusiones en el análisis ejemplos: “video_h265.mp4”, “video_h264.mp4” o “video_referencia.mp4”.
3. Instalación de herramienta para la medición de calidad para la elaboración de este punto ya hablamos de instalar FFmpeg el cual es una herramienta de línea de comandos gratuita que permite utilizar para calcular tanto el PSNR y SSIM, la instalación de dicha herramienta se explicará a continuación:
 - a. Descargar desde el sitio oficial de FFmpeg <https://ffmpeg.org/download.html>
 - b. Una vez dirigida en la página oficial descarga selecciona el sistema operativo utilizada para este caso se seleccionó el sistema operativo de Windows, dentro de este apartado nos presentarán 2 opciones: **Windows builds form gyan.dev** y **Windows builds by BtbN**, ambas opciones son válidas para la instalación la opción escogida para el proceso de instalación fue la primera de Windows builds form gyan.dev
 - c. Llegado a este punto debemos de dirigirnos hasta el apartado de reléase builds y descarga la opción de ffmpeg-release-essentials.zip como lo muestra la ilustración 139 para descarga el archivo en formato zip y ser más fácil el proceso de configuración de la herramienta.



Ilustración 172. Descargar el archivo ffmpeg en formato ZI.

Fuente: Elaboración propia.

- d. Ante de extraer el archivo debemos de dirigirnos dentro de nuestro computador o laptop al disco local C y crear una carpeta con el nombre de ffmpeg para una rápida ubicación al momento de solicitar la herramienta.
- e. Mover el archivo descargado a la carpeta previamente creada, una vez teniendo el archivos en la carpeta procedemos a extraer el archivos el cual no debe quedar con el siguiente nombre después de extraer “ffmpeg-7.1-essentials_build” teniendo el archivos procedemos a abrir y copiar todo lo archivos dentro de la carpeta, lo siguiente en realizar es pegar todo los archivos copiando en dirección “C:\ffmpeg” y eliminarla carpeta ffmpeg-7.1-essentials_build y el archivo .Zip, una realizado nos debe quedar la carpeta de la siguiente manera.



Ilustración 175. Carpeta ffmpeg lista para configurar el punto Path

Fuente: Elaboración propia.

- f. El siguiente paso el agregar FFmpeg a la variable PATH, para ellos tenemos lo siguientes paso:

Dirigirse al menú de inicio y escribir “editar las variables de entorno de sistemas” y proceder a abrir.

Se nos abrirá una ventana donde debemos dirigirnos a la opción de opciones avanzadas y seleccionar el botón de variable del entorno, cómo se muestra la ilustración 141.



Ilustración 178. Selecciones de Variables de entorno para entrar al apartado de PATH.

Fuente: Elaboración propia.

En la sección “variable del sistema”, encuentre la variable PATH y selecciónala, luego, haz Clic en editar.

Haz Clic en “nuevo” y escribe la ruta completa dónde se encuentra el archivo “C:\ffmpeg\bin”, para verificar que colocamos bien la ruta nos debe de quedar como en la siguiente ilustración 136, dentro de entorno de editor de variables.

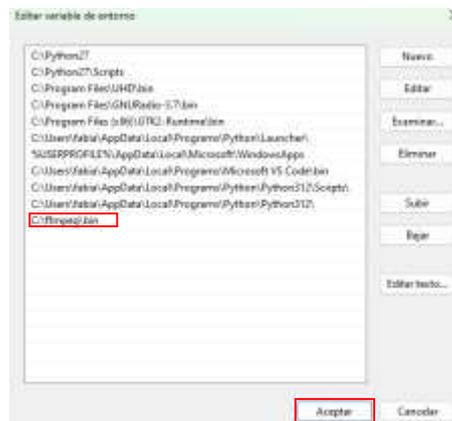


Ilustración 181. Agregar la ruta de FFmpeg dentro de PATH.

Fuente: Elaboración propia.

Para verificar que la instalación fue correcta mediante el símbolo del sistema escribir “ffmpeg -version” y presionamos enter, si la instalación fue correcta nos debe de brindar la información de la versión de FFmpeg instalada, como lo muestra la ilustración 143.

especialmente para los vídeos comprimidos en base al estándar H.265, donde el objetivo es reducir el tamaño sin perder demasiada calidad, en cambio para SSIM un valor cercano a 1 indica que la comprensión en H.265 está manteniendo una calidad visual muy parecida el vídeo de referencia.

Realizar los mismos pasos para poder analizar y comparar los medios de transmisión tanto en fibra, UTP y Wi-Fi así mismo registrar los resultados mediante tablas comparativas para un mayor análisis.

Guía de paso a paso para medir la estabilidad de transmisión.

1. Verificar la conexión de la cámara al NVR este de forma independiente para cada medio de transmisión.
2. Asegura de que el NVR la cámara está en configurada para la transmisión en H.264 o H.265.
3. Activar la vista en tiempo real en el NVR sin grabar, ya que esto permite observar la transmisión en condiciones reales.
4. Monitorear los siguientes factores en cada medio de transmisión:
 - a. Pausa o congelaciones de la imagen: estar pendiente en cualquier pausa o congelación de la imagen en la transmisión y proceder a anotar cuánta pausa realizó en un periodo de tiempo determinado.
 - b. Buffering: algunos NVR muestra un icono que registra la frecuencia y duración del Buffering en cada medio de transmisión.
 - c. pérdida de calidad temporal: verificar si hay una reducción en la estoy bien resolución o aparición de pixelamiento en la imagen.
5. Mediciones de paquete perdido mediante wireshark, mediante el tráfico previamente capturado realizar el mismo paso del filtrado para sólo obtener datos entre el NVR y la cámara una vez obtenida dirigirse desde wireshark a Statistcs > Conversations selecciona la pestaña de protocolo UDP o TCP, observar si se pierde algún paquete o si hay retransmisiones lo que puede indicar problemas de estabilidad.
6. Realizar pruebas en condiciones de redes variables para los diferentes medios de transmisión ya sea proximidades al router interferencia entre otras.

Guía de paso a paso para evaluar la eficiencia de almacenamiento.

1. Conectar la cámara al NVR mediante el medio de transmisión (fibra, utp y Wi-fi) de manera individual para evaluar cualquier diferencia en los tipos de conexión.
2. Dentro de las configuraciones del NVR, seleccionar el estándar de compresión de vídeo H.265 y verificar que en la cámara este es aplicar las mismas configuraciones, lo mismo se puede realizar para el estándar H.264 y se procede a grabar mi amor estándar.
3. Se realiza grabaciones en períodos de segmento de uno a 5 minutos como mínimo en cada estándar, asegurándose las mismas escenas en ambas sin muchas interrupciones.
4. Importar los archivos del NVR aún computador tanto las grabaciones hechas con el estándar H.264 y H.265, comparar el tamaño de MB de los archivos para luego analizar y comparar ambos.
5. Realizar cálculos de eficiencia de almacenamiento, para dichos cálculos se realizó la siguiente fórmula para obtener un valor en porcentaje y ser más fácil el momento de analizar, la fórmula utilizada es la siguiente:

$$\text{Ahorro de espacio (\%)} = \frac{\text{Tamaño H.264} - \text{Tamaño H.265}}{\text{Tamaño H.264}} \times 100$$

Realizar el mismo procedimiento para los diferentes medios de transmisión y registrar los resultados obtenidos de cada transmisión para luego ser comparados y determinar cuál método de transmisión es más eficiente.

3.3.2 Implementación escenario 1

Partiendo del diseño realizado en SketchUp, se procede a configurar minuciosamente los equipos que se utiliza antes de su instalación en lugares previamente seleccionados, dentro de esto se aplicará el direccionamiento de IP e integrar los protocolos de comunicaciones necesario para garantizar la correcta conectividad y operatividad de los equipos, esto nos asegura que cada equipo esté completamente preparado para su implementación efectiva en su ubicación designada

3.3.2.1 Configuración de Router Tenda

Utilizando los datos proporcionados por el fabricante, se determina que la dirección IP predeterminada para acceder a la interfaz de configuración del dispositivo es

192.168.0.1. Con esta información en mano, el siguiente paso es conectar físicamente el dispositivo a una computadora mediante un cable LAN, asegurando una conexión estable y directa.

Una vez establecida la conexión, se abre cualquier navegador web en la computadora y se ingresa la dirección IP 192.168.0.1 en la barra de direcciones. Esto permitirá acceder a la página de configuración del dispositivo. Al intentar acceder a esta página, se solicita crear una contraseña de inicio de sesión para garantizar la seguridad de la configuración, la contraseña establecida fue "T123456789@" como medida de seguridad para inicio de sesión.

Previamente establecida la contraseña de inicio de sesión, se auto dirige a la pantalla de inicio de sesión de un router Tenda. Para acceder a las configuraciones del router principal nos pedirá que ingresemos la contraseña previamente establecida "T123456789@" para luego poder autenticar nuestro acceso y permitir configurar el equipo a su conveniencia.



Ilustración 187. Inicio de sesión en Router Tenda.

Fuente: Elaboración propia.

Configuración de un router Tenda, como primer paso se verifica que el enrutador este correctamente conectado, luego en la sección configuración de red se procede a realizar las configuraciones correspondientes; donde en método IP, se debe seleccionar IP dinámica, indicando que el router obtendrá automáticamente una dirección IP del proveedor de servicio de internet (ISP).

Antes de configurar los parámetros de red debemos de saber internet especificados lo siguientes puntos: dirección IP asignadas al router, mascara de subred, IP de puerta de enlace del enrutador principal de laboratorio y opcional los parámetros DNSS.

A continuación, se detallan los pasos a seguir en esta etapa de la configuración:

- ✚ En el parámetro de dirección IP se coloca la dirección IP 192.168.23.1, facilitando la comunicación con otros dispositivos dentro de la red local a través de la dirección IP asignada.
- ✚ Para el parámetro máscara de subred se establece 255.255.255.0, permite al router identificar a los dispositivos que pertenecen a la misma subred
- ✚ En el parámetro puerta de enlace predeterminada se configura con la dirección IP 192.168.23.1, esta es utilizada para que otros dispositivos en la red puedan acceder a internet.
- ✚ Dentro de los parámetros DNS se configuran dos, el DNS primario o predefinido se establece con la dirección IP 8.8.8.8, que es correspondiente al servidor DNS principal proporcionado por Google, permite que los dispositivos conectados a la red puedan acceder a sitios web y servicios en línea, y para el DNS secundario o alternativo se establece la dirección IP 8.8.4.4, este también es un servidor de Google, pero este servidor se utiliza como respaldo asegurando que exista una alternativa para la resolución de nombre de dominio.



Ilustración 190. Direccionamiento de Gateway y su máscara.

Fuente: Elaboración propia.

El paso por seguir dentro de las configuraciones del Router TENDA, en esta parte se va a definir los parámetros más importantes de una red inalámbrica:

- SSID
- Clave de Seguridad

La red puede ser identificada con los nombres de “**Tesis_FM**”, además incluyendo la seguridad o más conocida como la contraseña, que es “**T123456789@**” ya que

desde este punto es el que asegura el acceso, también se habilito la opción, de usar la misma contraseña del WI-FI, como credencial de la administración del enrutador, la interfaz posee una simplicidad y mensajes claros para así poder mejorar la experiencia.

La red de 5GHz se activa automáticamente utilizando la misma configuración del SSID de la red de 2,4GHz, Agregando al final la palabra “5G” para diferenciarla claramente, además, se mantiene la misma contraseña que la que utiliza la red de 2,4GHz, Evitando así las confusiones y facilitando la conexión a ambas bandas lo que es crucial para asegurar una transición suave y acceso eficiente a la red de alta velocidad que ofrece la banda de 5GHz.

The screenshot shows the Tenda router's web interface. At the top, the Tenda logo is on the left and 'Chino simplificado' is on the right. Below the logo, it says '¡Disfruta de Internet en tan solo unos sencillos pasos!'. A progress bar at the top indicates four steps: 1. Comprobar conexión de red (checked), 2. Configuración de la red (checked), 3. Configuración de wifi (active), and 4. Finalizar. The main form area contains:

- 'nombre wifi' field with the value 'Tesis_FM'.
- 'secreto wifi' field with the value '123456789@!'. Below this field is a password strength indicator showing 'seguridad de la contraseña' with a red bar and the label 'medio'.
- A checked checkbox labeled 'Establecer la contraseña de WI-FI como contraseña de administración del enrutador'.
- 'Próximo paso' button.
- 'Anterior' button.

Ilustración 193. Cambio de configuración de adaptadores de red del equipo portátil.

Fuente: Elaboración propia.

3.3.2.2 Configuración de antena Ubiquiti NanoStation Loco M2

Como en el caso del router también se debe ingresar mediante un cable LAN conectado al computador, pero antes se debe cambiar la configuración del adaptador para así poder obtener una conexión con el equipo.

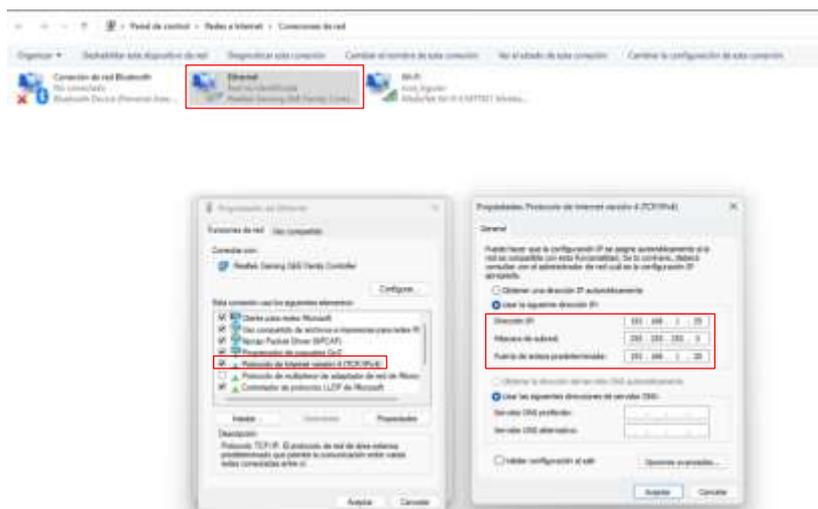


Ilustración 196. Parámetros de la red inalámbrica.

Fuente: Elaboración propia.

Se digita en cual navegador del computador la IP de default que viene dentro de los equipos ubiquiti 192.168.1.20, ante de ingresar al interfaz de la antena se muestra una ventana de seguridad donde se debe dar clic en configuraciones avanzadas.

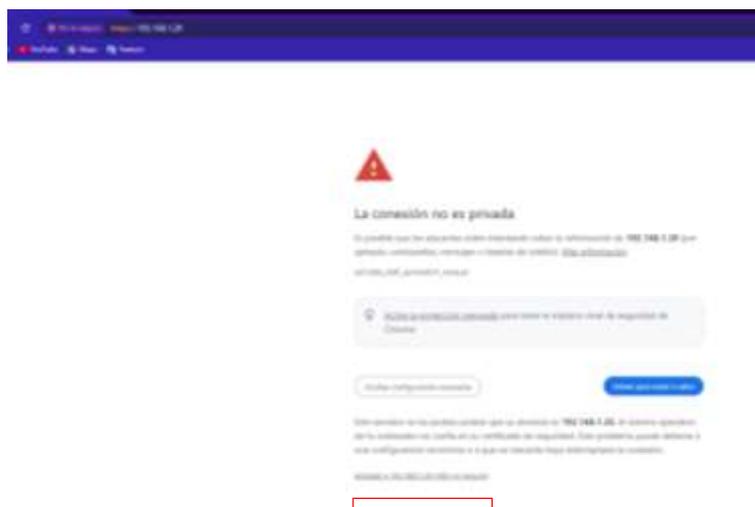


Ilustración 199. Ingreso del navegador por IP de default.

Fuente: Elaboración propia.

En la siguiente pantalla se muestra el inicio de sesión del sistema operativo AirOS de Ubiquiti Networks, utilizado para la configuración y administración de dispositivos de red. Para las configuraciones necesarias, existe un campo para introducir el nombre de usuario, en este caso "**ubnt**", y un campo protegido para ingresar la contraseña en este campo se coloca la contraseña predeterminada "**ubnt**".

Dentro del menú nos brinda la opción de cambiar el país de operación del dispositivo, el cual se selecciona el país “México” también se elige el idioma de la interfaz el equipo para trabajar entonces seleccione no el idioma “English”. Para finalizar con este apartado e ingresar a las configuraciones del equipo se selecciona el botón “Login” y se procede a dar Clic.



Ilustración 202. Interfaz de inicio de equipo Ubiquiti Loco M2.

Fuente: Elaboración propia.

El siguiente paso es dirigido a la sección de Wireless, se deben realizar la configuración correspondiente, en el parámetro Wireless Mode se selecciona

- ✚ "Access Points", indicando que el dispositivo funcionara como un cliente conectándose a un punto de acceso.
- ✚ En el parámetro SSID, se coloca el nombre con el que se identificara la red; en este caso está configurado como "TESIS_FM_C1".
- ✚ El parámetro Channel Width se estableció en ancho de banda 40 MHz, permitiendo al dispositivo aprovechar al máximo el ancho de canal según la disponibilidad y las condiciones de la red.
- ✚ Además, se debe tener en cuenta que la antena está configurada como "Built in (2x2) - 8 dBi", indicando que se utiliza la antena interna con una ganancia de 8 dBi, y la potencia de salida se le asigna en 8 dBm.
- ✚ En la sección Wireless Security, el protocolo de seguridad está configurado en "WPA2-AES", utilizando una clave precompartida (PSK) para la autenticación, con la clave "T123456789",

Para finalizar en ese apartado, se selecciona "Change" para aplicar y guardar los cambios realizados en la configuración.

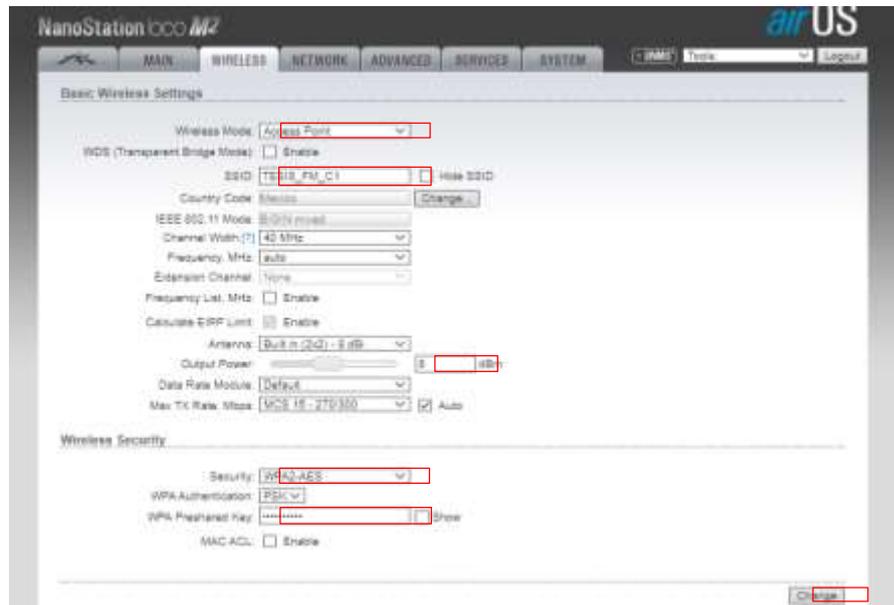


Ilustración 205. Asignación de parámetros.

Fuente: Elaboración propia.

Para continuar con las configuraciones nos ubicamos en la sección de Network y realizamos la siguiente asignación de IP estática.

- ✚ En la sección en Network se establece dentro del parámetro Network Mode como "Bridge", para que el dispositivo actuará como un puente en la transferencia de datos entre las diferentes redes.
- ✚ Se configura como dirección IP estática, específicamente con la dirección IP 192.168.0.25 esta dirección nos permitirá ingresar al equipo estando conectado de la red principal o de su red propia, la máscara de red 255.255.255.0 y con la puerta de enlace 192.168.0.1.
- ✚ Para los DNS se configura con los servidores de Google mencionados anteriormente, el servidor DNS primario o predefinido es 8.8.8.8 y el secundario o alternativo 8.8.4.4. También, se debe habilitar de IPv6, y configurar como "SLAAC" (Stateless Address Autoconfiguración).

Finalmente, se selecciona "Change" (Cambiar) para aplicar y guardar los cambios realizados en la configuración.

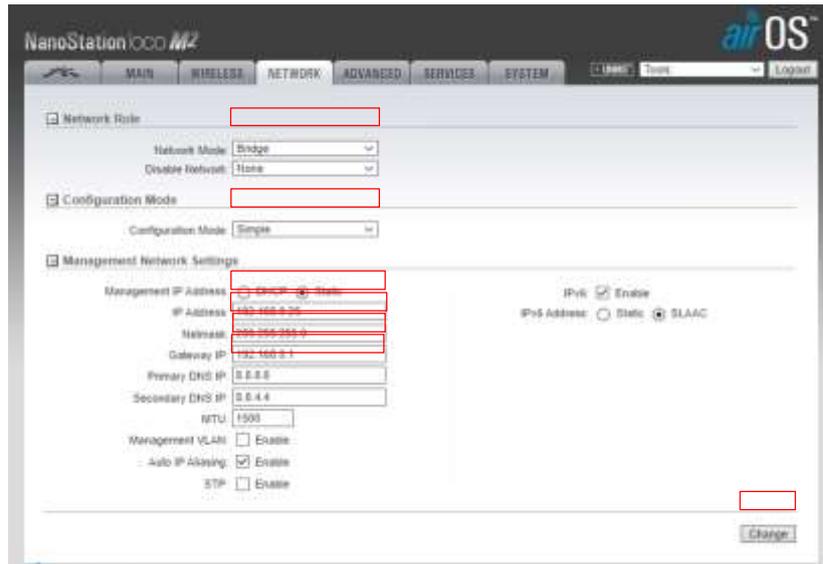


Ilustración 208. Asignación de IP estática conjunto con puerta de enlace.

Fuente: Elaboración propia.

3.3.2.3 Configuración de antena Ubiquiti NanoStation M2

Para esta antena al ser de la misma marca de las anteriores se realiza lo mismo paso que se realizando en la configuración anterior, los cambios que se realizaran se detallaran a continuación:

Nos ubicamos en el apartado Wireless, primero debemos seleccionar el modo de operación como “Access Point”, asegurando que el dispositivo funcione correctamente dentro de la red.

Luego procedemos a configurar un nuevo SSID, “TESIS_FM_C3”, eligiendo un nombre único y fácil de identificar para todos los usuarios de la red.

A continuación, asignamos una contraseña segura la cual será “T123456789”, que cumplen con los requisitos de seguridad recomendados que incluye una combinación de letras y números y caracteres especiales, la cual es crucial para proteger el acceso a nuestra red de dispositivos no autorizados.

Para finalizar configuramos el rango de operación de frecuencia, dejándolo en un modo automático para que el dispositivo seleccione la mejor frecuencia disponible para garantizar una conexión estable y minimizando las interferencias con otros dispositivos, optimizando así el rendimiento y la cobertura de la red.

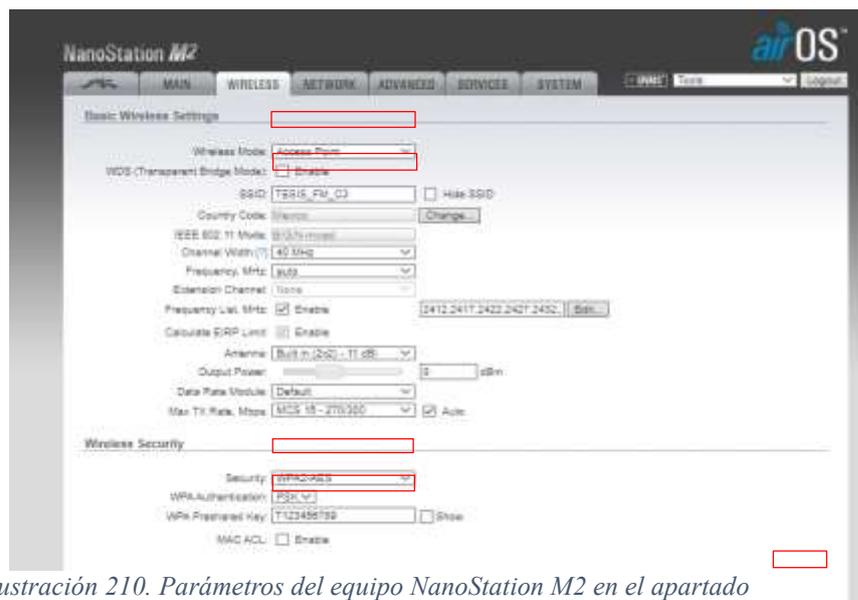


Ilustración 210. Parámetros del equipo NanoStation M2 en el apartado Wireless.

En la sección de network se realiza una configuración similar a la ya realizada en el dispositivo Ubiquiti NanoStation Loco M2 Como de operación, máscara de subred, puerta de enlace y DNS primaria y secundaria, la única diferencia es la asignación de IP fija al dispositivo que facilita el acceso de cualquier dispositivo conectado a la red. Esta IP fija es esencial para identificar y gestionar el dispositivo de manera eficiente dentro de la red asegurando una conectividad estable y un fácil acceso para la administración y monitoreo del dispositivo.

- ✚ Primero se configura el modo de red como “bridge” con el fin de que el dispositivo actuará como un puente para pasar tráfico entre diferentes encuentros de la red.
- ✚ Segundo se asigna una IP estática 192.168.0.35, permitiendo el acceso al dispositivo desde la red principal o su propia red.
- ✚ Tercero la configuración de la máscara de red 255.255.255.0 y la puerta de enlace 192.168.0.1, estos datos son importantes ya que permitirá el acceso al internet de este equipo.
- ✚ Cuarto se asigna los DNS en este en este caso se utilizó los de servicio Google 8.8.8.8 cómo DNS primario y 8.8.4.4 como de DNS secundario.

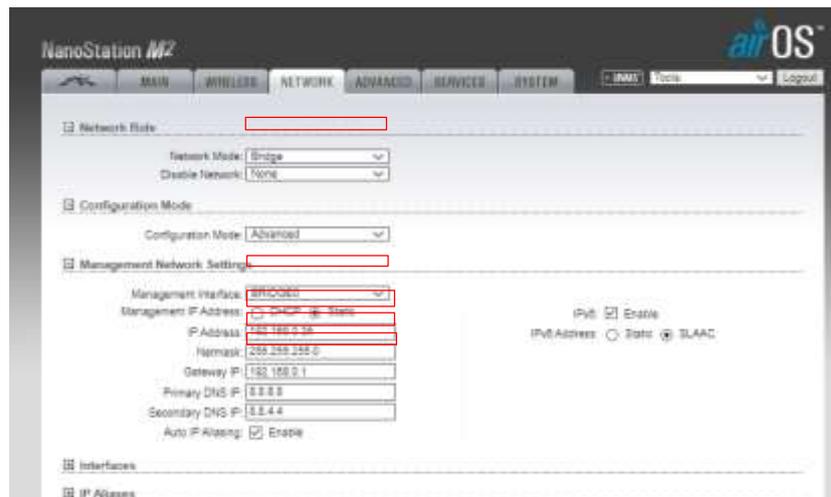


Ilustración 214. Asignación de IP para el acceso al equipo y el acceso al internet.

Fuente: Elaboración propia.

3.3.2.4 Configuración Cámaras Reolink Color

Este ejemplar de cámara brinda 2 maneras de configurarse lo que se detalla a continuación, la primera manera es designar una dirección IP a la cámara cuando se lo interconecta al enrutador principal ya que este proceso no permite a que la cámara se incorpore de manera rápida a la red local ya que esto favorece al acceso y monitoreo desde dispositivos móviles conectados a la misma red por lo que simplifica procesos siendo ideal en entornos en el cual se busca una conexión estable y constante.

La segunda manera se forma una estructura lo que permite el acceso a internet al dispositivo para posteriormente utilizar una aplicación móvil para configurar la cámara, la gran ventaja de este método es que permite configurar y monitorear la cámara de manera remota sin las necesidades encontrarse en la misma ubicación ya que la aplicación nos ofrece una interfaz didáctica y fácil de usar en la cual cabe destacar que brinda funciones como alertas en tiempo real almacenamiento en la nube y permitiendo compartir el acceso a tercera persona, estos 2 métodos detallados proporcionan grandes ventajas y se adaptan a distintas necesidades en cualquier caso este modelo de cámara está diseñado para adaptarse a diversos entornos y brindar soluciones versátiles para obtener un correcto monitoreo y vigilancia.

Cámara 1

Para utilizar el primer método antes mencionado y ser utilizado en la primera cámara es necesario asignarle una dirección y espera por lo cual es indispensable tener acceso al enrutador del lugar en el cual se encuentra ubicada la cámara, como ingresó ahora enrutador comúnmente se realiza accediendo al navegador y colocar la dirección IP del enrutador en la barra de elecciones las IP comunes son 192.168.0.1 o 192.168.1.1 para posteriormente ingresar a las credenciales de acceso que habitualmente se localizan en una etiqueta del enrutador en el manual de la cámara



Ilustración 217. Asignación automática de IP dentro del router.

Fuente: Elaboración propia.

Dentro de la configuración del enrutador, busca la sección de dispositivos conectados. Aquí verás una lista de todos los dispositivos actualmente conectados a la red. Encuentra tu cámara en esta lista. Es probable que aparezca con un nombre genérico o con su dirección MAC, que puedes encontrar en el manual de la cámara o en una etiqueta en el dispositivo.

Teniendo identificada la cámara dentro del router procedemos fijar la dirección IP la cual fue 192.168.0.111, nos dirigimos hacia el navegador y escribo la dirección IP en la barra de navegación. Al hacer lo mencionado aparecerá una ventana de advertencia de seguridad dónde nos brindas la información de la conexión no es segura o privada, esta información debemos hacer caso omiso para entrar a las configuraciones de la cámara, para continuar con el proceso seleccionamos las configuraciones avanzadas nos dirigimos a "Ir a 192.168.0.111 (no seguro)" y procedemos a dar Clic.

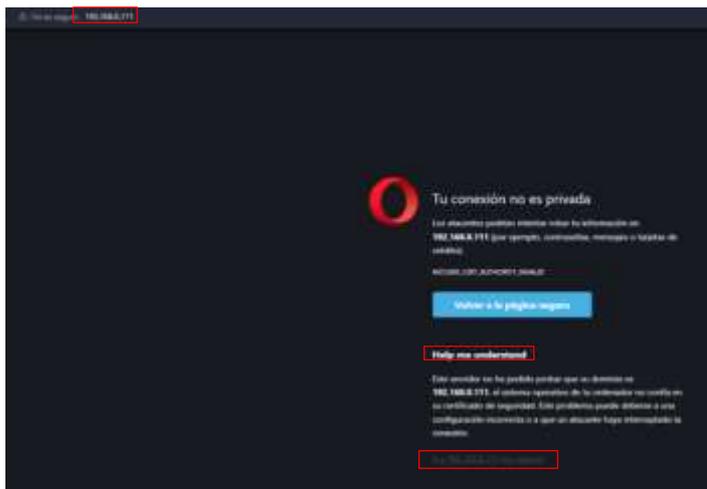


Ilustración 220. Ingreso mediante el navegador con la dirección IP.

Este proceso nos redirigirá a la ventana de inicio de sesión de la cámara RLC-510WA. Introduce las credenciales de acceso predeterminadas, que suelen ser "admin" tanto para el nombre de usuario como para la contraseña, a menos que las hayas cambiado anteriormente.

En este caso cómo se cambió previamente las credenciales de inicio de sesión, pon mi nombre de usuario se mantuvo como "admin", mientras que la nueva contraseña se estableció como "admin12345".

Una vez dentro, podrás acceder a las configuraciones de la cámara, donde puedes ajustar la resolución de video, las alertas de movimiento y la configuración de red.



Ilustración 223. Inicio de sección e ingreso de credenciales de la cámara RLC-510WA.

Fuente: Elaboración propia.

Una vez en las configuraciones de la cámara nos trasladamos a la sección de red dentro de la misma procedemos a configurar la red wireless, verificamos que la red Wi-Fi esté configurado adecuadamente, si el SSID aparece en el apartado de escaneo de red simplemente la seleccionamos y procedemos a ingresar la contraseña correspondiente.

Caso contrario al no aparecer en la lista de escaneo el SSID de la red, se debe de agregar manualmente tanto el nombre SSID de la red el tipo de seguridad “WPA2” y por último la contraseña de la red wireless. Se debe de verificar que los datos ingresados sean los correctos para evitar contratiempos al momento de conectar la red a la cámara. Al integrar la red seleccionada a la cámara permite es fácil acceso y monitoreo remoto a través de los dispositivos que esté conectado a la misma red Wi-Fi de la cámara.

- 🚦 SSID: TESIS_FM_C2
- 🚦 Contraseña: T12345678



Ilustración 226. Selección de la red Wi-Fi donde se conectará la cámara e ingreso de SSID y contraseña.

Fuente: Elaboración propia.

Una vez establecida la conexión a la red cómo es importante recordar que inicialmente la cámara recibirá una dirección IP a través de DHCP. Para futuras configuraciones, es recomendable cambiar estos datos a una IP estática. Para hacerlo, dentro del importado de red, nos dirigimos a la opción de configuración en la pestaña avanzadas. Dentro de esta nueva sección procedemos a configurar cada ítem con una IP estática. Los pasos que seguir son los siguiente

- 🚦 **Conexión IP Estática:** Esto significa que la cámara utiliza una dirección IP fija que no cambie con el tiempo. Es útil en entornos donde se requiere una conexión constante y confiable, ya que facilita el acceso a la cámara sin tener que buscar una nueva dirección IP para vez que intentemos acceder a la cámara.

- ✚ Dirección IP: Para evitar conflicto con direcciones de se establece una IP fija la cual nos permitirá acceder de manera local o remota a las configuraciones de la cámara y poder monitorearla desde cualquier dispositivo que se encuentre conectada a la red, la IP asignada fue 192.168.0.111.
- ✚ Mascara de subred: Como mascara de subred tenemos 255.255.255.0, determina qué parte de la dirección IP corresponde a la red y qué parte a los dispositivos (hosts) en esa red.
- ✚ Puerta de enlace: Es una de las direcciones esenciales, nos permite acceder a la red, la IP asignada 192.168.0.1, esta es la dirección IP que le enrutador o dispositivo de red que conecta la red local a otra red, como internet. La cámara enviará datos fuera de la red local a través de esta puerta de enlaces.
- ✚ DNS primario y secundario: Para el DNS referido se escogió los del servidor de Google 8.8.8.8 y el aleatorio es otro que pertenece a los mismo servidores Google 8.8.4.4. con funcionalidad de respaldar en caso de que el DNS preferido no esté disponible.

Ante de salir de esta sección debemos guardar los datos que hemos configurado, para ellos debemos de dirigirnos hacia el botón de guardar y damos clic, la cámara actualizada su configuración de red según parámetros introducidos

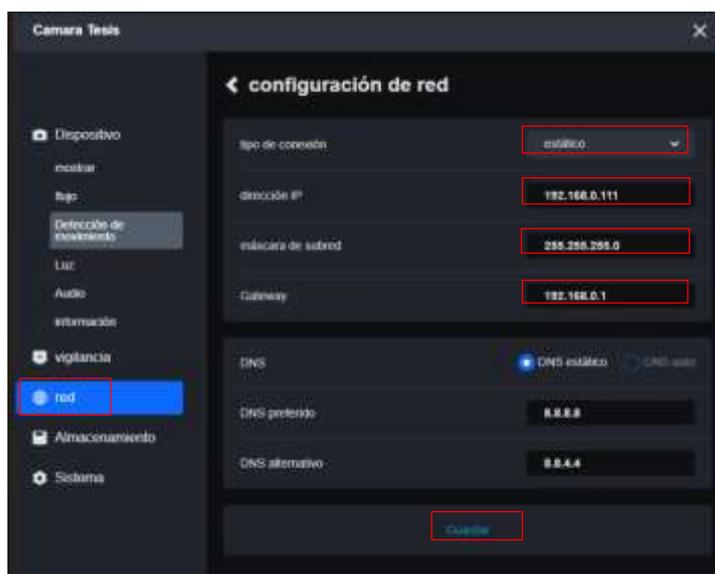


Ilustración 229. Cambio de configuración de red a estática.

Fuente: Elaboración propia.

Otro apartado que verifico y configuro con nuevos parámetros es la configuración del servidor. Esto es esencial para poder acceder a la cámara desde otros dispositivos o desde un NVR que se encuentre en otra red.

Para llegar a esta sección, debemos seguir estos pasos:

1. Acceder al equipo de red: Acceder a la configuración de la cámara y se dirige hasta la sección de red.
2. Seleccionar configuración avanzada: Desde la sección de red, seleccionar la opción de configuración avanzada. Este apartado nos brindará opciones adicionales de protocolos propios de la cámara.
3. Dirigirse a la configuración del servidor: En la sección avanzada, dirigirse a la opción de configuración del servidor.

Una vez en la configuración del servidor, realizamos los siguientes cambios de puerto para asegurarnos de que la cámara puede ser accesible desde otros dispositivos o un NVR en una red diferente:

 Servicio básico:

- Puerto: 5000
- Configuración de los servicios básicos de red de Reolink. Mantener este puerto permite la comunicación básica con la aplicación cliente de Reolink.

 RTMP:

- Puerto: 1935
- Activar si se necesita la transmisión en tiempo real de audio y video entre dispositivos y aplicaciones que usan RTMP.

 HTTP:

- Puerto: 8080
- Mantener activado para permitir el acceso a través del protocolo HTTP. Es importante para acceder a la cámara desde navegadores web.

 RTSP:

- Puerto: 554
- Activar si se necesita transmitir audio y video en tiempo real a través de aplicaciones de terceros que usan RTSP.

ONVIF:

- Puerto: 8000
- Activar para permitir la interoperabilidad con dispositivos y aplicaciones de terceros compatibles con ONVIF.

Estas modificaciones hacen posible que el acceso y la gestión mediante diferentes dispositivos o redes hacia la cámara, resulta en una flexibilidad para diversas necesidades de monitoreo y vigilancia.

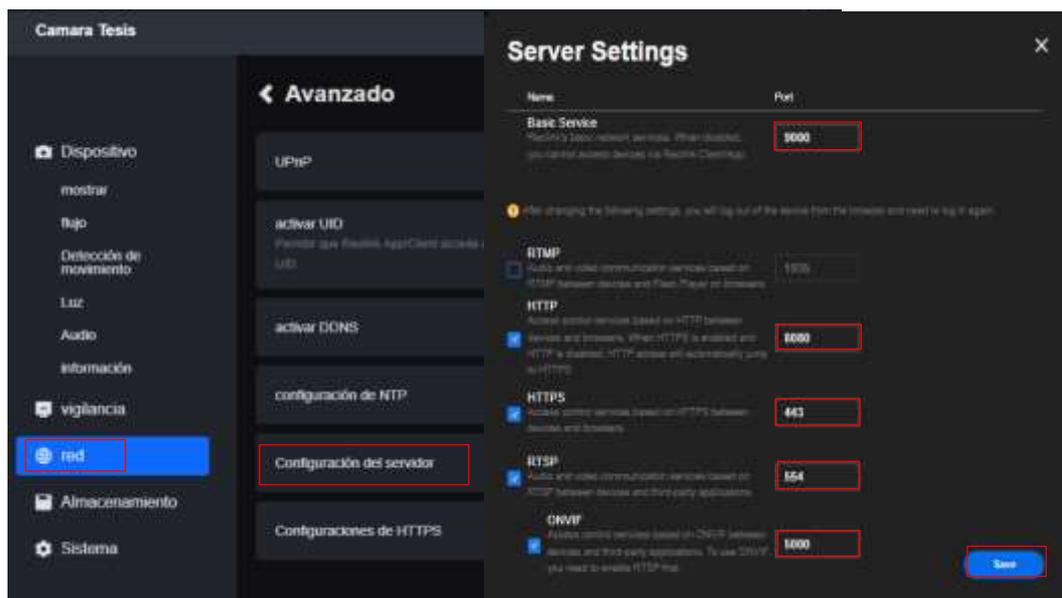


Ilustración 232. Configuración de servidor y puerto de conexión.

Fuente: Elaboración propia.

Para concluir el montaje de la primera cámara empleando el primer procedimiento mediante la ilustración 74 observamos que la cámara se encuentra capturando imágenes de forma continua y la cual se presenta como "Cámara Tesis". Se ha establecido la conexión mediante Wi-Fi lo cual verifica que las conexiones realizadas previamente fueron exitosas.

Mediante la captura de fotogramas se evidencia que la cámara se encuentra funcionando de manera efectiva transmitiendo vídeo en tiempo real, lo que resulta esencial para un seguimiento eficaz. La conexión de la cámara bajo el nombre de "Cámara Tesis" simplifica sobre el conocimiento de la red especialmente cuando existen varios dispositivos conectados al mismo sistema de vídeo vigilancia.

Una vez realizada con éxito las configuraciones se lograron poder acceder de manera remota la cámara "Cámara tesis" mediante los medios conectados a la misma

red Wireless, dónde se logró observar las transmisiones en tiempo real de dicha cámara.



Ilustración 235. Conexión establecida de la cámara y visualización de imagen.

Fuente: Elaboración propia.

Cámara 2

Para iniciar con la respectiva conexión segunda cámara RLC-510WA, para esto es necesario disponer del uso de la app llamado Reolink, esta aplicación se halla disponible en la App Store y Play Store para su respectiva descarga, luego de las aplicaciones ha sido localizada se lleva cabo el proceso la descarga y posteriormente su instalación en los diferentes dispositivos móviles, todo esto ya culminado el proceso de instalación el siguiente paso consiste en abrir la aplicación donde podrá verificar la correcta funcionalidad de la misma. A continuación se procede a ingresar a la aplicación dónde debemos registrarnos creando un usuario para poder acceder a todas las funciones que se encuentran en la app, esto es un método que brinda seguridad y un control de acceso a los mismos usuarios, con el fin de poder mejorar, controlar según las necesidades que se requiera para el entorno final en donde esté ubicada la cámara, para una correcta visualización y supervisión del área destinada.

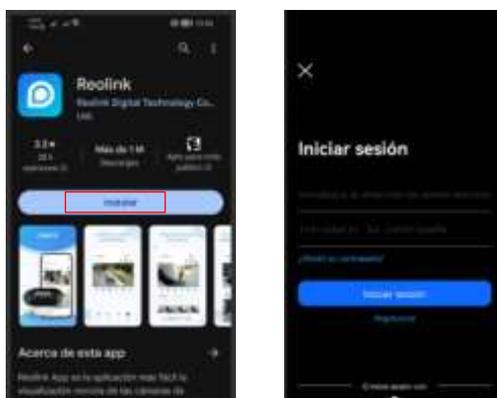


Ilustración 238. Proceso de instalación de la aplicación Reolink mediante la Play Store.

Fuente: Elaboración propia.

Una vez dentro de la aplicación "Reolink", debemos agregar la cámara siguiendo las instrucciones detalladas en el manual de instalación. El primer paso es escanear el código QR de la cámara para establecer el enlace inicial. Este proceso permite que la aplicación reconozca y conecte la cámara a la red.

También debemos tener en cuenta que para poder visualizar la imagen que nos brinda las cámaras es necesario tener las credenciales de acceso, que para este caso se va a configurar el usuario de "admin" y su respectiva clave de seguridad que sería "admin12345", tomando en cuenta de que la seguridad es primordial para restringir el acceso a terceros, para evitar algún daño, pérdida o mala manipulación de los dispositivos.

Con todo el proceso concluido y completado las con figuraciones iniciales y una correcta familiarización con la aplicación, además, las cámaras tienen una configuración avanzada dónde se puede controlar o ajustar varios puntos de la cámara como lo pueden ser las alertas de movimiento y la resolución del contenido audiovisual, así se logra optimizar lo máximo posible del rendimiento del sistema de CCTV según las necesidades del cliente final.

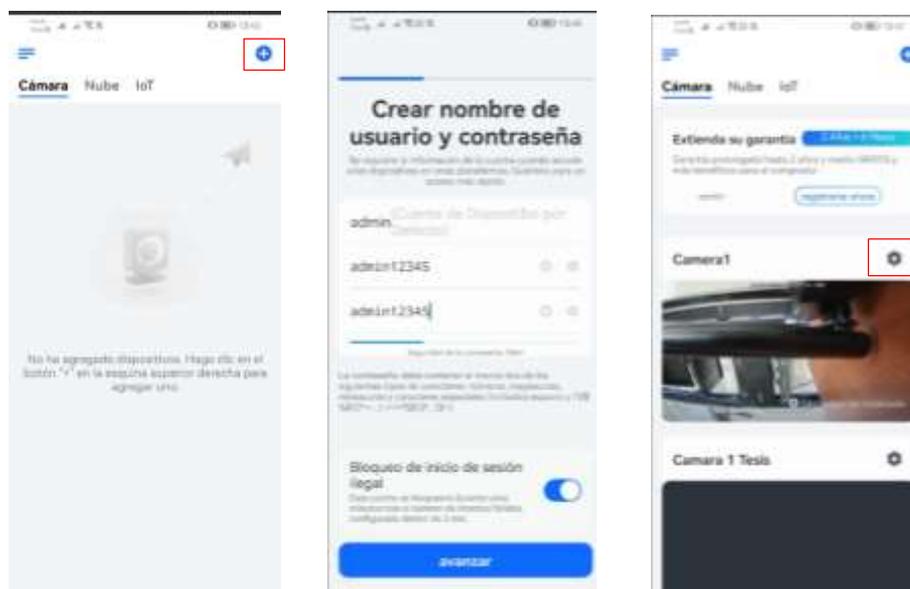


Ilustración 241. Inicio de sesión de la aplicación Reolink y primeras configuraciones dentro.

Es necesario configurar la red Wi-Fi a la cual se conectará la cámara, ubicada conforme a los escenarios previamente definidos. Para establecer una conexión

segura y eficiente, debemos especificar los detalles de la red. Los datos necesarios para la configuración son los siguientes:

- ✚ SSID (nombre de la red): TESIS_FM_C1

- ✚ Contraseña: T123456789

Estos detalles son esenciales para asegurar que la cámara se conecte a la red correcta y opere de manera óptima dentro del entorno establecido. Al proporcionar un SSID único y una contraseña segura, garantizamos no solo la conectividad, sino también la seguridad de la red, evitando accesos no autorizados y posibles vulnerabilidades.

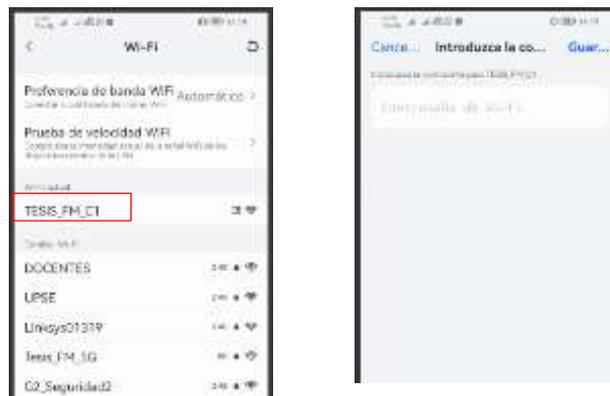


Ilustración 244. Configuración de red Wi-Fi mediante la aplicación Reolink.

Fuente: Elaboración propia.

Para las configuraciones adicionales necesarias para la implementación de nuestra propuesta, es crucial considerar la dirección IP que ha sido asignada automáticamente a la cámara por el protocolo DHCP. Esta dirección IP, "192.168.0.120", se utilizará para acceder a la cámara a través de un portátil, facilitando la gestión y el monitoreo remotos. Dicha dirección se encuentra detallada dentro de la sección de información de red en las configuraciones del dispositivo, bajo el apartado correspondiente a la asignación de IP.

En este paso es muy importante verificar la dirección IP en las configuraciones de la red dónde se podrá observar y confirmar si la conectividad se ha hecho de la manera correcta, también la dirección IP permite a los dispositivos que estén dentro de la misma red y que tengan el permiso y acceso a las cámaras les permita la autorización de manipular o realizar ajustes de las cámaras. Además, se pueden realizar soluciones de problemas que se llegasen a presentar dentro del sistema de seguridad.

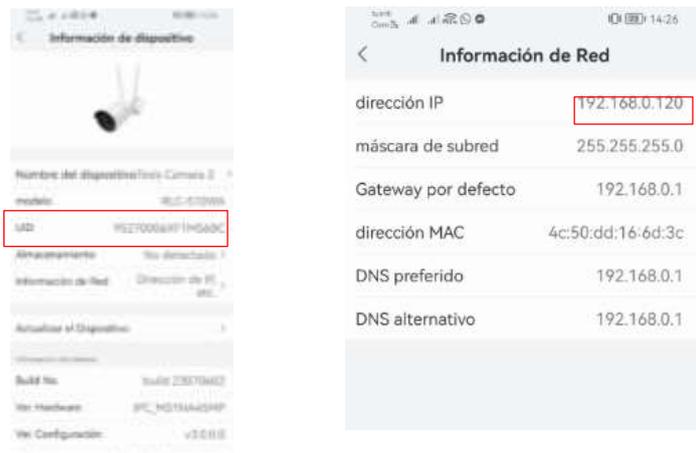


Ilustración 247. Verificación de información de la red y IP para posterior configuración.

Fuente: Elaboración propia.

Tan pronto como se obtiene la dirección IP “192.168. 0.120”, se la coloca en la barra de direcciones del navegador que una vez cargado la dirección no va a presentar una ventana de seguridad que permite avanzar hacia la interfaz de la cámara para así lograr este objetivo es indispensable es seleccionar la alternativa de “opciones avanzadas” en el cual se desplegarán varias opciones sobre la conexión de la IP en la que se está trabajando por lo consiguiente se elige la opción “deseo continuar” en el cual da como resultado la redirección a la interfaz de la cámara en el cual se gestionan las funciones.

Para poder disponer del acceso completo de las herramientas de la interfaz como paso principal se deben ingresar las credenciales usadas con anterioridad en el inicio de sesión para facilitar el ingreso a través de la aplicación móvil esto es necesario para respaldar la seguridad y el manejo adecuado en la manifestación del dispositivo, después de haber ingresado los datos requeridos correctamente se autoriza automáticamente el acceso a la justicia avanzadas de configuración donde se podrá personalizar y visualizar más a detalle la cámara RLC 510-WA como también la supervisión del área que se desea vigilar en tiempo real.

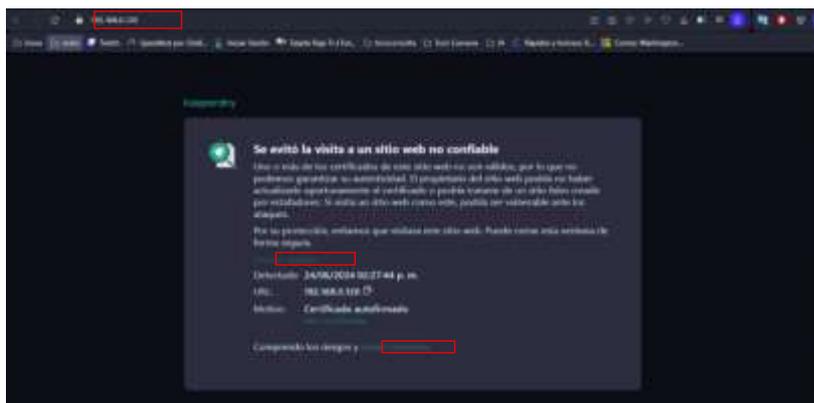


Ilustración 250. Inicio de sesión mediante el navegador con la IP obtenida de la ilustración 78

Una vez que accedemos a la interfaz del equipo, procedemos a navegar hasta el apartado denominado "Red" o "Network". En esta sección, es crucial seleccionar la opción "Server Settings", donde llevaremos a cabo la configuración de los parámetros de red. Aquí, debemos introducir y configurar los mismos datos utilizados previamente en la configuración de la cámara anterior para asegurar la consistencia y funcionalidad del sistema.

Este procedimiento implica modificar elementos como la dirección IP, hoy el puerto del servidor y las configuraciones de seguridad, replicando las mismas configuraciones realizada en la cámara anterior ya que han demostrado ser efectivas para mantener una con estable y segura. Al implementar las mismas modificaciones, simplificamos la administración de varios dispositivos red mejorando la interoperabilidad y el rendimiento general del sistema de vigilancia.

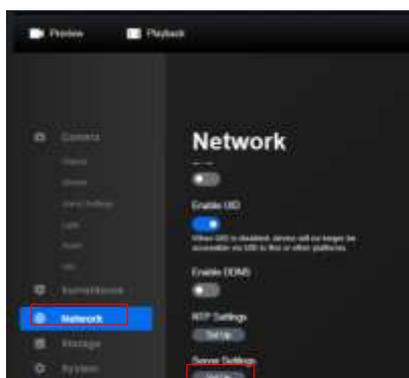


Ilustración 253. Configuración de los servidores.

Fuente: Elaboración propia.

Mediante la ilustración 81, observamos las configuraciones realizadas en el apartado "Server Settings" donde se activó y designó los puertos de acceso remoto, la misma ilustración analizada demuestras un desglose detallado de la funcionalidad otorgada a cada protocolo y los puertos pertinentes.

El procedimiento realizado asegura que la disposición de los puertos sea correctamente adecuada con los protocolos requeridos para un desempeño óptimo del sistema. Al realizar las mismas configuraciones en ambas cámaras garantizamos que cada puerto esté adecuadamente configurado para manejar las comunicaciones de la red conforme a los requisitos técnicos establecidos.

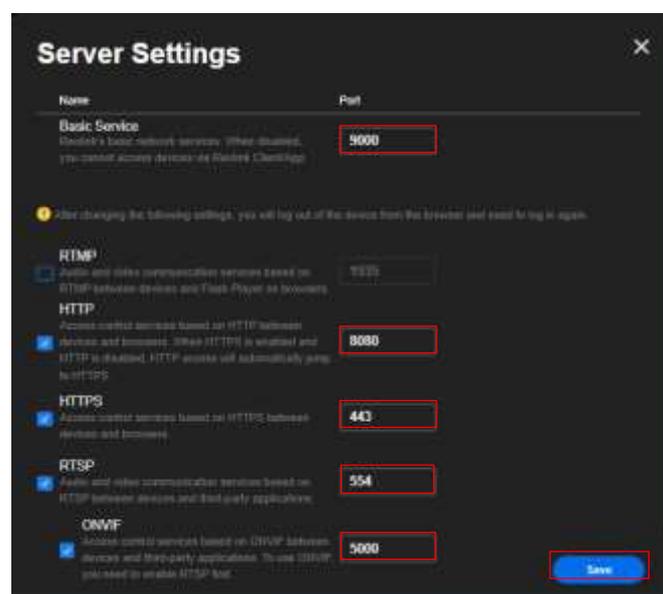


Ilustración 256. Configuración de puerto de conexión.

Fuente: Elaboración propia.

3.3.2.5 Implementación física de los equipos de red CCTV

Una vez teniendo los equipos debidamente configurados y siguiendo con el diseño propuesto en puntos anteriores se continuo con la instalación de equipos en los lugares previamente establecido en los exteriores del laboratorio de facsistel.

Para garantizar una identificación de los equipos y del cableado en el exterior se emplea etiquetas de extremo a extremo, dichas etiquetas son esenciales para un mantenimiento posterior o una fácil localización en problemas dados, para la primera instalación, se definió y aginaron las siguientes etiquetas.

- ROUTER (192.168.0.1)
 - ❖ WAN-R1-ETH16-SWHP
 - ❖ ETH1-R1-LAN-LC-M2

- ❖ ETH2-R1-LAN-NS-M2
- LOCO M2 (192.168.0.25)
 - ❖ LAN1-LC-M2-ETH1-R1
 - ❖ POE1-LC-M2
 - ❖ POE-LC-M2(SOURCE)
- NANOSTATION M2 (192.168.0.30)
 - ❖ LAN1-NS-M2-ETH2-R1
 - ❖ POE2-NS-M2
 - ❖ POE-NS-M2(SOURCE)

Tras tener el modelo de las etiquetas, se emplearon en relación del recorrido del cableado y en los diferentes equipos, lo cual permitió su fácil identificación durante el proceso de instalación. Posteriormente, se siguió con lo establecido en el diseño presentación anteriormente, la instalación se inició con la primera cámara, colocada en la ubicación exacta especificada en la ilustración 81.

Así con el tendido del cableado se efectuó con un cable UTP que se conectar desde el puerto ethernet 2 del router identificado con la etiqueta “ETH2-R1-LAN-NS-M2”, hasta el puerto LAN del PoE de la antena Loco M2 dicho extremo del cable se identificó como “LAN1-NS-M2-ETH2-R1”, continuando desde el puerto de alimentación del POE, se tendió un cable UTP identificado como POE1-NS-M2 hasta llegar a la antena dicho extremo se identificó como POE-NS-M2(SOURCE), proporcionando a la par tanto energía como la capacidad para la transmisión de la señal.



Ilustración 259. Etiquetado de cableado desde el PoE.

Una vez concluido el trayecto hasta la antena, la misma se fijó mediante abrazaderas metálicas a un tubo de acero asegurado en la pared que de igual manera se aseguró con grapas metálicas. Finalmente, la cámara que había sido previamente configurada, en un soporte asegurado a la pared de tal forma que estuviera perfectamente sujeta y ubicada para su adecuado funcionamiento.

En la ilustración 83, se puede visualizar el resultado de la instalación correspondiente a la primera localización de la cámara dentro del escenario 1, a su vez se logra apreciar a las etiquetas debidamente en cableado como en el equipo.

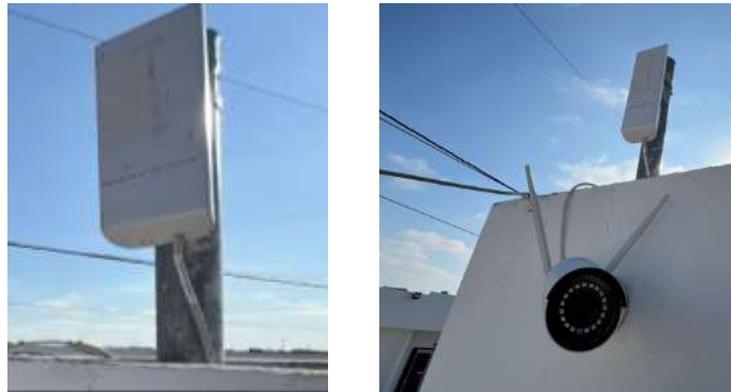


Ilustración 262. Resultado final de instalación de la primera cámara.

Para la instalación de segunda cámara se llevó a cabo en base la segunda ubicación del diseño esta corresponde a la parte de trasera del laboratorio, como en la primera instalación se inició con el tendido del cable UTP del equipo a del puerto ethernet 1 identificado como ETH1-R1-LAN-LC-M2, posterior se ayudó con la infraestructura del laboratorio para no quedar en evidencia el cableado hasta llegar al PoE específicamente en el puerto LAN al llegar el cable hasta el puerto se identificó como LAN1-LC-M2-ETH1-R1, se volvió de tender otro cable UTP esta vez lleva el identificador de POE1-LC-M2 como el cable anterior se apoyó de la infraestructura para hacer llegar a la bandeja donde reposan el resto de cableado de laboratorio, hasta que pueda salir del laboratorio el cual se apoyó con grapa en el exterior para un mayor agarre hasta llegar a la antena NanoStation Loco M2, dicho extremo de cable a llegar a la equipo se identificó de la siguiente manera POE-LC-M2(SOURCE)



Ilustración 265. Etiquetado de PoE correspondiente a la segunda ubicación.

Fuente: Elaboración propia.

La antena se aseguró de la misma forma que en la primera instalación con los mismos materiales, con el objetivo de mantenerla estable para su funcionamiento posterior. La cámara también se instaló de la misma manera y se aseguró con el mismo material, unido a esto, fue instalada en el árbol correspondiente. En la ilustración 85 se muestra el resultado final instalación donde se incluyen también las etiquetas colocadas en el cableado y en cada uno de los dispositivos finales, facilitando la organización visual y ubicación de éstos.



Ilustración 268. Instalación final de la segunda cámara.

Fuente: Elaboración propia.

Al finalizar las instalaciones se detallan la IP de los equipos así se mantiene un control de inventario y evitar cualquier conflicto de IP, para ellos se elaboró una tabla donde se visualizarán la IP utilizadas junto al usuario y contraseña de cada equipo utilizado.

Tabla 16. Inventario de equipos utilizado con respectivos usuario y contraseña.

Fuente: Elaboración propia.

Nombre del equipo	IP	Usuario	Contraseña
Tenda (Principal)	192.168.0.1		T123456789@
Ubiquiti Loco M2	192.168.0.25	ubnt	ubnt123456
Ubiquiti NanoStation	192.168.0.30	ubnt	ubnt12345
Cámara 1	192.168.0.111	admin	admin12345
Cámara 2	192.168.0.120	admin	admin12345

3.3.3 Implementación escenario 2

Dentro de este escenario, se implementará varios dispositivos de frecuencia 5GHz para la creación de una red punto a multipunto destinada a un sistema CCTV, el enrutador Tenda utilizado en el primer escenario es compatible con la doble banda, una característica muy significativa ya que permite utilizar todas las configuraciones mencionadas anteriormente.

Las configuraciones realizadas en las bandas de 5 GHz ofrecen una cobertura adecuada una mayor estabilidad en la transmisión, estos elementos son esenciales para mantener un sistema de videovigilancia sin interrupción.

Esta adaptabilidad posibilita preservar la integridad y la seguridad de un sistema cctv, ajustándose a las demandas variables y garantizándonos empeño óptico constante.

3.3.3.1 Configuración Ubiquiti LiteBeam 5Ac 2 Generación

Este equipo, al ser de una generación superior ofrece dos métodos distintos para acceder a su interfaz de usuario. La primera opción implica que el sistema puede ser conectado mediante un PoE para energizar tanto al equipo como en la conexión a la computadora por medio de un cable LAN para una mejor comunicación estable y rápida. En segundo lugar, es accesible a través de la red inalámbrica del equipo “**LBE-5AC-Gen2:FCECDAC0F1E7**”, lo que le da la portabilidad para acceder al dispositivo a través de cualquier otro dispositivo compatible, por ejemplo, un teléfono inteligente, Tablet o computador portátil. Esta doble capacidad de acceso lo hacen muy conveniente para monitorear y modificar el dispositivo según las preferencias y necesidades de cada uno.

En la configuración de este dispositivo, se ha seleccionado la primera opción, que es la de ingresar a través de un cable LAN. Cómo configurar el equipo paso a paso utilizando esta opción se explicará más adelante.

Antes de intentar ingresar a esta configuración, simplemente se debe asegurar que todo esté conectado adecuadamente: se conecta el cable pues directamente a la antena para proporcionar la energía; el puerto LAN va conectado a la computadora portátil.

Para poder ingresar ante debemos realizar un cambio de configuración en el equipo portátil que se centra en la configuración adaptadores de red, en la opción de ethernet en cual debemos ubicarnos en la opción “**Habilitar el protocolo de internet versión 4**” y realizamos el cambio de parámetros.

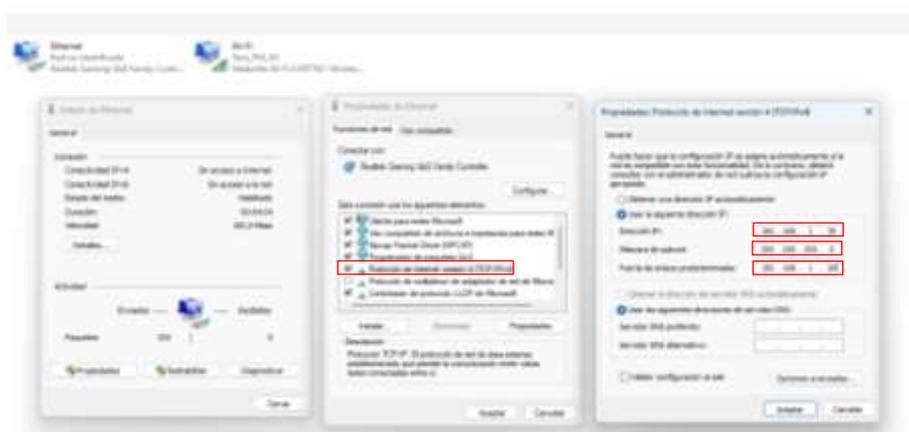


Ilustración 271. Cambio de protocolo IPv4 dentro del equipo portátil

Fuente: Elaboración propia.

De la configuración en la computadora portátil, se inicia el navegador web y se escribe la dirección IP predeterminada de los dispositivos ubiquiti, “192.168.1.20”. Debido a que es un dispositivo nuevo, no se abrirá inmediatamente la ventana de inicio, más bien, se abrirá una ventana que mostrará que no es una conexión segura. En tal caso, deberías ir configuración avanzadas y allí encontrarás la opción para ir al sitio no seguro “192.168.1.20”. Al hacer Clic en él toma te redirigirá automáticamente al menú de inicio de sesión.

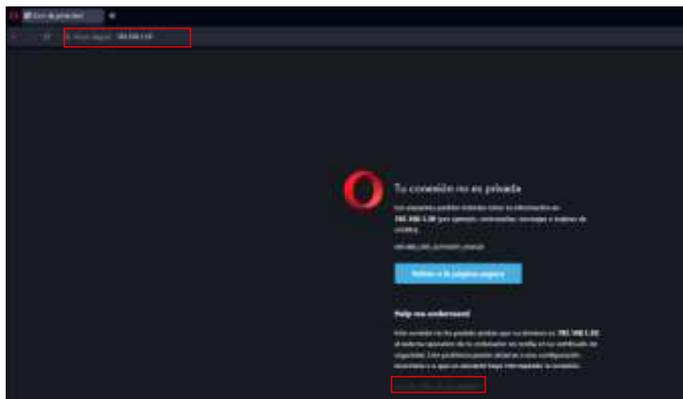


Ilustración 274. Ingreso por medio del navegador por IP de default.

Fuente: Elaboración propia.

En la sección de inicio de sesión pide que se ingrese el nombre de usuario y la contraseña, en este caso de prueba se ha cambiado las credenciales predeterminadas para un uso propio y son las siguientes:

🚦 Nombre de usuario: ubnt

🚦 Contraseña: tesis12345.

En el caso de que el equipo no ha sido alterado y todavía tienen experiencia de originales de fábrica, utilice:

🚦 Nombre de usuario: ubnt

🚦 Contraseña: ubnt

Estas son las credenciales por defecto que vienen todos los equipos ubiquiti



Ilustración 277. Inicio de sesión dentro del equipo.

Fuente: Elaboración propia.

Para continuar con la configuración, una vez ingresado al equipo nos ubicamos en el apartado de Wireless. En esta sección, debemos realizar varias configuraciones relevantes para asegurar la conexión con las demás antenas. Como este es un dispositivo emisor, vamos a configurar este dispositivo específico con eso.

- ✚ Modo punto de acceso debe estar en modo activado para que el que el dispositivo está ahora en el modo AP y, por lo tanto, otros dispositivos pueden unirse a la red Wi-Fi.
- ✚ Modo PTP de encontrarse desactivado al realizar eso nos permite la conexión para múltiples conexiones de clientes.
- ✚ Ancho de banda se estable en 20 MHz proporciona un buen equilibrio entre interferencia y rendimiento.
- ✚ Frecuencia central para trabajar se estableció con 5745MHz dentro de esta frecuencia establecida dentro del canal 155 dentro de toda la banda de 5 GHz.
- ✚ Control Frecuencia debe ser idéntica con la frecuencia de trabajo que se estableció en 5745 MHz y así determinar la frecuencia idéntica para el control de frecuencia también garantiza que la transmisión se realice a través de un solo canal sin el cambio de frecuencias que puedan amenazar la estabilidad de la red.
- ✚ Asignación de SSID como AP_TESIS_WN es el nombre único que se asignará a la red y que se podrá ver en la lista de redes inalámbricas disponibles en los dispositivos.
- ✚ El tipo de seguridad de la red inalámbrica es WPA2 es la forma más común en que se configura una red doméstica o de oficina pequeña.
- ✚ Clave designada Tesis12345 es uno de los elementos críticos en relación con la seguridad en red

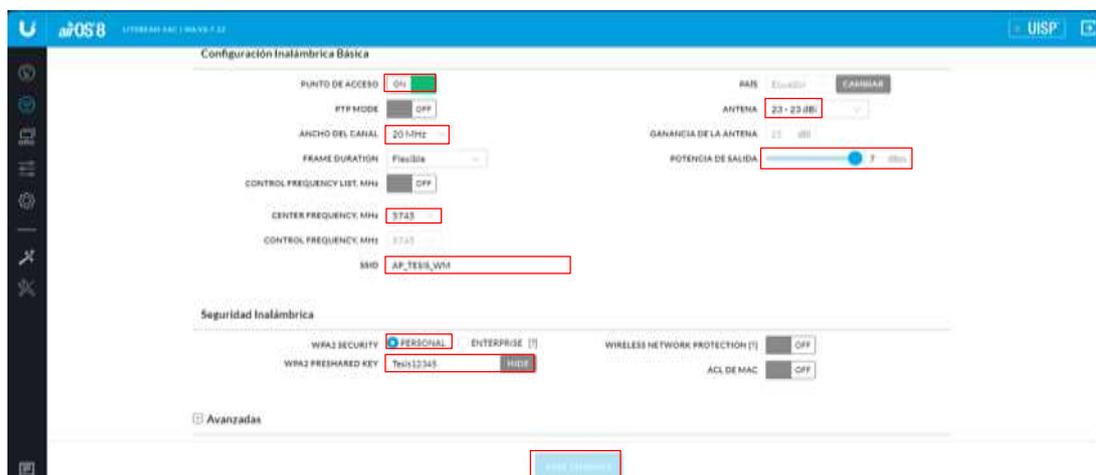


Ilustración 280. Configuración en el apartado Wireless.

Fuente: Elaboración propia.

Finalmente, también se debe recordar que todas las configuraciones hechas deben guardarse correctamente antes de cerrar la sesión de configuración. Solo entonces los cambios se harán efectivos y el dispositivo operará según los parámetros necesarios. Para esto, abra el botón "Save Changes" en la interfaz de usuario. Al hacer clic en el botón "Save Changes", el sistema tomará y guardará todas las configuraciones hechas durante la sesión. Es prudente no salir del proceso de salvado antes de la finalización para no perder datos o salvaguardar ajustes inválidos. El siguiente paso en la configuración es ir a la pestaña "Network". La sección, se detallarán los parámetros esenciales para acceder a la red desde la computadora principal, es muy importante que los parámetros se describan correctamente para que la red sea estable y funcione adecuadamente. A continuación, se presenta una descripción más detallada de los siguientes parámetros importantes:

- ✚ Modo de Red: Configura en modo "Bridge" facilitando la comunicación entre diferentes segmentos de red sin realizar enrutamiento, en este modo el equipo conecta nombres locales y permite su interconexión entre ambas redes principales.
- ✚ IP Estática: Se estableció "192.168.0.22", este IP debe ser única para el equipo dentro de la red local, esta IP no ayudará para acceder y administrar el dispositivo.
- ✚ Mascará de red: La máscara de red correspondiente al host será "255.255.255.0".
- ✚ IP puerta de Acceso: La puerta de enlace sería el enrutador que vincula la red local con internet "192.168.0.1", esta es una dirección crucial que se debe ingresar correctamente para que la máquina principal sepa cómo dirigirse a otras redes y llegar a internet.
- ✚ Servidor DNS principal y secundario: para el DNS principal se escogió los del servidor Google "8.8.8.8" y el DNS secundario es "8.8.4.4" que también pertenece a un servidor público de Google.

Al igual que en los casos anteriores, es crucial guardar las configuraciones con el fin de evitar cualquier inconveniente al navegar libremente dentro de la interfaz del equipo. Para ello, diríjase a la opción “Save Changes” y haga Clic en ella. Se debe de esperar hasta que las configuraciones se guarden automáticamente para así garantizar que los cambios se apliquen correctamente.

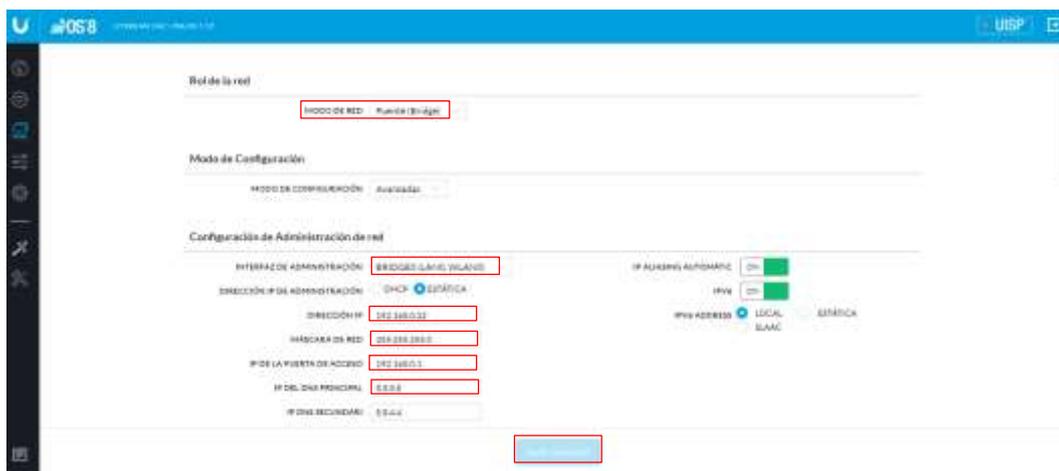


Ilustración 283. Asignación de IP dentro de la sección network.

Fuente: Elaboración propia.

3.3.3.2 Configuración Ubiquiti NanoStation 5Ac Loco

Este equipo comparte las mismas cualidades que el ubiquiti LiteBeam 5AC en términos de métodos de inicio de sesión, al configurar este dispositivo tenemos la opción de iniciar sesión de manera: a través de una conexión la cableada o mediante su red Wi-Fi.

La configuración empleada se enfoca en la segunda opción la cual se enfoca en utilizar la red Wi-Fi de la antena e iniciar sesión por medio de ella. Dicha red Wi-Fi se encuentra identificada como “**Loco5AC:F4E2C690A458**”, este método se emplea particularmente en circunstancias donde no se cuente con conexiones cableadas inicia dispositivos adaptables a este medio, lo que brinda una mayor flexibilidad y facilidad de acceso mediante su incorporada.

Cómo se explicó anteriormente, es fundamental conectarse a la red Wi-Fi del equipo mencionado para proceder con las configuraciones, una vez que el portátil esté conectado a esta red Wi-Fi se nos proporcionara la opción acceder automáticamente a la interfaz del dispositivo.

- ✚ En el portátil, navegue hasta las opciones de red y localice la red Wi-Fi identificada como **Loco5AC:F4E2C690A458** y conectar.
- ✚ Se abrirá el navegador con una IP automática designada 192.168.172.1

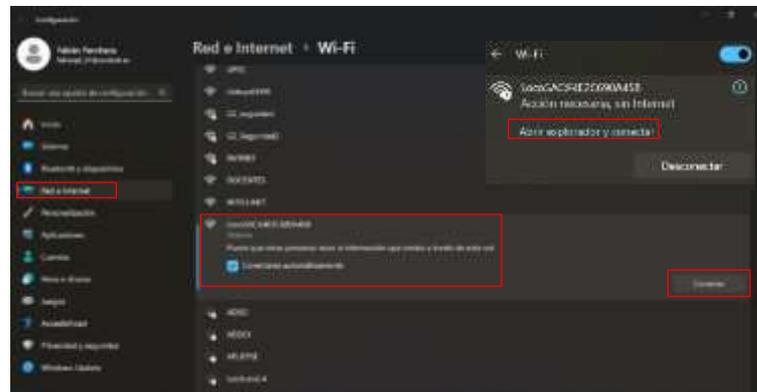


Ilustración 286. Conexión con el Wi-Fi del equipo para acceder a sus configuraciones.

Fuente: Elaboración propia.

El siguiente paso consiste en acceder a las configuraciones del equipo para ello, es necesario conocer las credenciales proporcionadas por el fabricante. En algunos casos, el usuario puede establecer su propia contraseña de inicio de sesión desde el principio, a continuación, se detallarán ambos casos:

- ✚ Cuando el equipo solicite ingresar el nombre de usuario y la contraseña, se deben utilizar las credenciales predeterminadas de la marca Ubiquiti, que son las siguiente:
 - Usuario: ubnt
 - Contraseña: ubnt
- ✚ En el caso de que el equipo permite establecer un nuevo nombre de usuario y contraseña desde el inicio, las credenciales escogidas para este equipo serán las siguientes:
 - Usuario: ubnt

- Contraseña: tesis123456.



Ilustración 289. Inicio de sesión en el equipo Loco 5AC.

Fuente: Elaboración propia.

Dentro de las configuraciones del equipo, nos ubicamos en la sección wireless, luego nos dirigimos al parámetro SSID, al seleccionar esta opción se desplegará una nueva ventana que nos facilita el escaneo de todas las redes existentes en la zona adyacente.

Se presenta una nueva pestaña donde tendremos están de las redes detectadas en dentro del área escaneada, dentro de la lista debemos de seleccionar la red previamente configurada en antena principal dicha red se denomina “AP_TESIS_WM”, una vez seleccionada la red procedemos a conectar y establecer las conexiones entre ambas antenas, el proceso de enlazar ambas antenas es crucial ya que garantiza su sincronización y su capacidad de comunicación de manera eficiente.

Una vez teniendo seleccionado la red procedemos a escribir su contraseña para enlazar ambos puntos, además, se explicará por qué ciertos apartados de la configuración están desactivado ese caso.

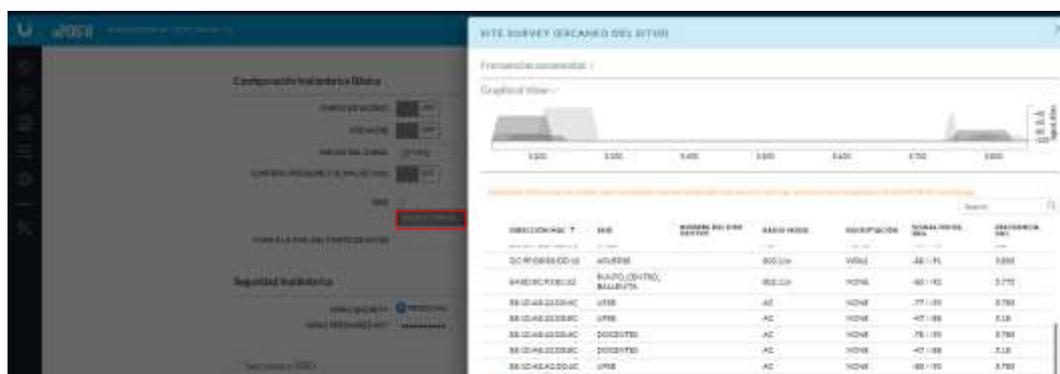


Ilustración 292. Escaneo de señal emisora.

Fuente: Elaboración propia.

- ✚ Punto de acceso debe estar desactivado para que no transmita señal WI-FI, y que los dispositivos no puedan conectarse a través de este punto de acceso, debido a que este funcionara como modo cliente.
- ✚ Modo PTP debe estar deshabilitado debido a que si se habilita establecerá una conexión directa y dedicada entre dos dispositivos y se necesita que este en modo multi usuario.
- ✚ Ancho del canal se establece en 20 MHz para tener un equilibrio entre la capacidad de datos y la resistencia a las interferencias.
- ✚ Control frecuencia scan lista se desactiva para que no realice escaneo automáticamente si no que el usuario seleccione manualmente.
- ✚ Auto Ajuste Distancia se activa para permitir que el dispositivo se ajuste automáticamente sus parámetros de transmisión en función de la distancia entre el punto de acceso y los dispositivos conectados.
- ✚ Ganancia de la antena se configura en 13dBi indicándome que la antena puede amplificar significativamente la señal permitiendo mayor alcance y mejor cobertura.
- ✚ Potencia de salida se configura en 17 dBm para emitir la señal suficiente para aplicaciones necesarias en la red inalámbrica.
- ✚ Distancia se establece con 0.6 km para mantener una conexión efectiva con otros dispositivos dentro de la red.
- ✚ SSID se asigna el siguiente nombre “AP_TESIS_VW” permitiendo a los usuarios identificar y conectarse a la red proporcionada por este dispositivo.
- ✚ WPA2 Security debe establecerse en modo personal debido a que proporciona una clave precompartida para todos los dispositivos.
- ✚ WPA2 Preshared Key se asigna la clave “Tesis12345” asegurando que solo los dispositivos autorizados puedan acceder a la red.

Finalmente debe guardar las configuraciones en el botón Save Changes, para asegurar que los cambios realizados se guarden correctamente.

Dentro de la sección de network también se procede a realizar configuración para

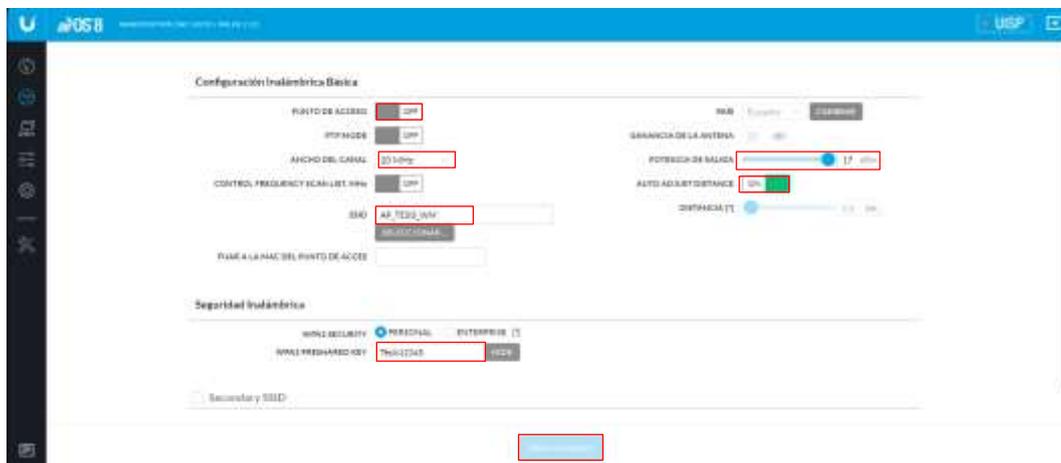


Ilustración 295. Configuración restante dentro de Wireless.

Fuente: Elaboración propia.

el funcionamiento del enlace dentro de ella tenemos la siguiente:

- ✚ Modo de red se establece como puente (Bridge), permitiendo que el dispositivo actúe como intermediario entre dos o más redes, logrando que el tráfico fluya entre ellas sin realizar cambios en las direcciones IP de los paquetes.
- ✚ Dirección IP de Administración se configura como estática para que la administración del dispositivo asegure que la dirección IP del dispositivo no cambie con el tiempo.
- ✚ Dirección IP se asigna “192.168.0.160” siendo esta la dirección asignada al dispositivo dentro de la red local, permitiendo que los administradores de red accedan al dispositivo para configuración y monitoreo.
- ✚ Máscara de red se asigna “255.255.255.0” indicando que la red tiene un prefijo de 24 bits, lo que significa que hay 256 direcciones posibles en la subred.
- ✚ IP de la Puerta de Acceso se asigna la dirección IP “192.168.0.1” es el dispositivo que conecta la red local a otras redes.
- ✚ IP del DNS Principal y secundarios lo cual se establece el 8.8.8.8 como primario, permitiendo conexión con un servidor DNS publico

proporcionado por Google.IP , para el secundario se determinó el siguiente DNS 8.8.4.4, actúa como DNS de respaldo en caso de que el principal no esté disponible.

Para que los cambio en la configuración se guarden debemos de presionar el botón Save Chandes



Ilustración 298. Configuración del equipo en su apartado network.

Fuente: Elaboración propia.

Para finalizar se muestra la siguiente imagen donde muestra la interfaz de la conexión punto a punto (PTP) entre el dispositivo NanoStation 5AC loco como dispositivo local, con la potencia de transmisión (TX Power) en 17 dBm y LiteBeam 5AC con el nombre AP_Tesis como dispositivo remoto con la potencia de transmisión (TX Power) en 7 dBm. El potencial del enlace es de 91.52 Mbps, el rendimiento del enlace es de 141.96 Mbps a una distancia de 450.00 m.

El dispositivo local tiene la señal de -18 dBm en escala de -21 a -41 dBm, ruido de base de -98 dBm y el ancho de canal de 20 MHz (5745 MHz - 5755 MHz), la tasa de datos RX es de 6X. Mientras el dispositivo remoto tiene la señal de -12 dBm en escala de -12 a 43 dBm, la tasa de datos RX es de 8X, el ruido base y ancho de canal son iguales al dispositivo local.



Ilustración 301. Enlace establecido entre los equipos.

Fuente: Elaboración propia.

3.3.3.3 Configuración Ubiquiti NanoStation 5Ac Loco

Para la configuración de este equipo como se replicarán los pasos utilizados para el equipo anterior, el proceso se centra e identificar el nombre de la red Wi-Fi la específica de este equipo que es “**Loco5AC:F4E2C6824537**”.

Una vez que se haya reconocido esta red, continuaremos con los procedimientos detallados previamente, que incluye el ingreso de la contraseña de la red, ajustar las configuraciones necesarias y verificar la conexión.

A partir de este punto, los pasos a seguir son los mencionados con anterioridad el único cambio a realizar es en el apartado de network que son los siguientes:

- ✚ El direccionamiento IP se asigna “192.168.0.141” con la asignación de esta IP dentro de la red local, nos permite el acceso al dispositivo desde cualquier equipo que se encuentre dentro de la red para así poder realizar cualquier configuración extra o monitorear la misma.
- ✚ Los datos de la máscara se mantienen igual que el anterior que se asignó como “255.255.255.0”.
- ✚ Otro dato que se mantiene es la IP para la puerta de enlace en la cual sigue siendo “192.168.0.1”.
- ✚ Los DNS primario y secundario también se mantiene al ser de dominio de Google estos DNS asignado “8.8.88” como primario y el secundario “8.8.4.4”.

Para finalizar debemos guardar las configuraciones esto se logra al seleccionar el botón “Save Changes” se debe esperar unos segundos hasta que se guarde por completo la configuración realizada



Ilustración 304. Asignación de IP dentro de la sección network.

Fuente: Elaboración propia.

Luego de realizar la configuración correspondiente se verifica el estado de conexión entre el emisor y el receptor del respectivo radio enlace, lo mencionado se puede corroborar en la ilustración 93, donde podemos observar un enlace óptimo a una distancia de 300m, los parámetros a destacar en el equipo local, con la potencia de transmisión (TX Power) en 17 dBm mientras que el equipo remoto con la potencia de transmisión (TX Power) en 7 dBm. El potencial del enlace es de 149.73 Mbps, el rendimiento del enlace es de 143.52 Mbps.



Ilustración 307. Verificación de estado de conexión entre la emisora y el punto b.

Fuente: Elaboración propia.

3.3.3.4 Configuración de cámara RLC-510WA

Para este escenario se utiliza las configuraciones realizadas previamente en el punto 3.3.1.4 del primer escenario, eso se debe al que utilizar las mismas cámaras y sus direcciones IP al estar en el mismo segmento de la red, la diferencia él se da del tipo de frecuencia a utilizar mientras que en primer escenario se utilizó la frecuencia de 2,4 GHz, para este escenario se emplea la frecuencia de 5Ghz.

Para lograr esto mediante el radio enlace se habilito redes de 5 GHz para cada cámara en este mediante la ilustración 94, se aprecia como se cambia la red inalámbrica de cámara que previamente tenia de 2,4 GHz, se agregó manualmente la siguiente red de 5 GHz.

- ✚ SSID: Tesis_esc2_5G
- ✚ Password: Tesis123456789

De igual manera en la segunda cámara se cambió la red inalámbrica de 2,4Ghz que tenía a la nueva red de 5Ghz, los datos de la nueva red son las siguiente:

- ✚ SSID: Tesis_esc2_2_5G
- ✚ Password: T123456789



Ilustración 310. Cambio de red dentro a 5Ghz de la cámara RC-510WA

Fuente: Elaboración propia.

3.3.3.5 Implementación física de los equipos de red CCTV

Una vez culminado la configuración de los equipos, el siguiente paso es llevar a cabo su implementación en los exteriores del laboratorio de telecomunicaciones, para ellos, nos guiaremos en todo momento de lo previamente propuesto en el diseño del escenario 2.

Ante de la implementación, se realizado nuevas etiquetas propios para el escenario 2, esto nos garantiza una identificación eficaz durante el tendido el cableado estructurado. Este proceso de etiquetado es fundamental, ya que facilita mucho al momento de identificar distintas conexiones y agiliza la detección de problema

presentado, para la siguiente implementación se definieron y asignaron las siguientes etiquetas:

- ROUTER (192.168.0.1)
 - ❖ ETH1-R1-LAN-LBT-5AC
- LITE BEAM 5AC (192.168.0.22)
 - ❖ LAN1-LBE-5AC-ETH1-R1
 - ❖ POE1-LBE-5AC
 - ❖ POE-LBE-5AC-1(SOURCE)
- LOCO 5AC (192.168.0.141)
 - ❖ LAN1-NSM-5AC-WAN-R2
 - ❖ POE2-NSM-5AC
 - ❖ POE-NSM-5AC(SOURCE)
- LOCO 5AC (192.168.0.160)
 - ❖ LAN1-NSM-5AC-WAN-R3
 - ❖ POE3-NSM-5A
 - ❖ POE-NSM-5AC(SOURCE)

Finalizando el proceso de etiquetado, se inicia el proceso de tendido del cableado, donde se tomó en cuenta las ubicaciones designadas en segundo diseño propuesto para ello se siguió en cada paso tanto en las ubicaciones de las cámaras como de antenas emisoras y receptoras.

Una de la parte principal para el funcionamiento optimo del sistema es la instalación de la antena emisora, ya que de ella depende el funcionamiento de las antenas receptoras conjuntos a las cámaras, la ubicación previamente fue designada en el diseño en la ilustración 44.

Ante de realizar el tendido del cableado se debe situar la antena emisora en su lugar designado, para ellos se empleó un tubo de acero de apoyo para evitar que el equipo se esté moviendo por factores del clima así evitemos perdida de transmisión, una vez ya asegurado la antena al tubo se colocó en la base ya instalada sobre la losa del laboratorio para garantizar una estabiliza y alineación adecuada, para mayor sujeción se agregó tensores de acero al tubo, proporcionando un refuerzo extra y reducir las vibraciones y movimientos mientras se use, una vez terminado de ajustar los tensores la ubicación de antena quedaría como se ve en la ilustración 99

El recorrido inicio desde el router principal donde se designó el puerto ethernet 1 para luego conectar un cable UTP que posee la etiqueta ETH1-R1-LAN-LBT-5AC, se utilizó la estructura del rack hasta llegas al PoE 1 donde se conectó el otro extremo del cable UTP donde se colocó la siguiente etiqueta LAN1-LBE-5AC-ETH1-R1, para energizar y transmitir datos se lanzó otro cable utp directamente desde el PoE 1, el extremo que se conectó al PoE se etiqueto como POE1-LBE-5A, se siguió con el recorrido mediante la infraestructura del laboratorio hasta poder llegar de la parte del tejado donde se encuentra situada la antena LiteBeam 5AC el extremo que llego a la ubicación del equipo lo identificaron como POE-LBE-5AC-1(SOURCE).



Ilustración 316. Instalación de antena emisora.

Fuente: Elaboración propia.



Ilustración 313. Etiquetado del Poe de antena emisora.

Fuente: Elaboración propia.

Prosiguiendo con el proceso, se instala la primera cámara conjunto a la antena receptora y un router conforme a los lineamientos establecido en el diseño, para esta instalación, se siguieron las indicaciones empleadas del diseño que llevo hacia la ilustración 45.

Nos situamos al costado derecho del edificio como lo estipula el diseño, al ser sobre la losa del laboratorio no se contaba con puntos eléctricos para energizar los equipos para solucionar se habilito un punto eléctrico desde el laboratorio de automatización hasta lo más cercado de equipos, ya teniendo solucionado el problema de la alimentación eléctrica, se instalado la antena 1 identificado como LOCO 5AC (192.168.0.141) dicha se pasó se ajustó con abrazaderas metálicas a un costado de la pared junto a su soporte un tubo de acero para mayor estabilidad y optimizar el

radio enlace. Llegado a esto realizaron las conexiones mediante cable utp donde lo primero el realizar es energizar la antena para ellos se tendió un pequeño cable conectado al PoE dicho extremo conectado se etiqueto como POE2-NSM-5AC y el extremo que llego al equipo con POE2-NSM-5AC(SOURCE), el siguiente cable utp se tendió desde el puerto LAN del PoE 2 hacia el router R2 con el fin de brindar acceso al internet y a su vez proporcionar una red wireless de 5Ghz para la conexión de la cámara para identificar dicho tendido se determinó con la etiqueta LAN1-NSM-5AC-WAN-R2.

Como paso final en el proceso de instalación, se procedió a montar equipo la primera cámara RLC-510w, la cual se encontraba previamente configurada, solo fue necesario fijar el soporte utilizando tornillos para una mayor fijación a la pared, a continuación, se calibro el ángulo de la cámara así optimizando un mayor campo de visión, la implementación completa se aprecia en la ilustración 96.



Ilustración 322. Etiquetado de conexiones del PoE 2.

Fuente: Elaboración propia.



Ilustración 319. Instalación completada correspondiente a la primera ubicación del escenario 2.

Fuente: Elaboración propia.

Acorde al estipulado en el diseño, nos situamos en la parte trasera del edificio debido a nuestra posición sobre la losa de laboratorio no se contaba de puntos eléctricos para energizar los equipos cómo por lo que se habilitó un punto eléctrico desde el laboratorio de telecomunicaciones hasta la ubicación más cercana de los equipos. Una vez resuelto el problema de la alimentación eléctrica, se inició con la instalación de la segunda antena, la cual fue etiquetada como LOCO 5AC (192.168.0.160). Dicha antena se fijó a un costado de la pared mediante abrazaderas metálicas En un soporte adicional con tubos de acero ya que aumenta la estabilidad en el sistema y optimiza el radioenlace.

Posteriormente, se efectuaron las conexiones mediante cable utp, el primer proceso fue energizar la antena a través de un cable tendido al PoE 3, etiquetado el extremo

conectado como POE3-NSM-5A y el extremo que llega al equipo fue etiquetado como POE3-NSM-5A (SOURCE). El último cable UP fue tendido desde el puerto LAN del Poe3 hasta el router R3, primero para aprovechar el acceso al internet y segundo para configurar una red inalámbrica de 5 GHz para la conexión de la cámara. Este tendido se identificó con la etiqueta LAN1-NSM-5AC-WAN-R3.

La implementación incluyó el montaje de la segunda cámara RLC-510w configurada en un paso previo, sólo fue necesario fijar el soporte utilizando tornillos para una mayor sujeción, así mismo se calibró el ángulo de la cámara para tener una mayor optimización del campo de visión, pensión completa se documenta en la licitación

99



Ilustración 325. Etiquetado de conexiones del PoE 3.

Fuente: Elaboración propia.



Ilustración 328. Instalación completada correspondiente a la última ubicación del escenario 2.

Una vez finalizadas las instalaciones, se registran las direcciones IP que se asignan a cada equipo para tener un cuidadoso registro de inventario y así mantener lejos al máximo los peligros de poseer la dirección IP. Esto se hizo a través de una tabla en la que se mantiene las IP asignadas, el nombre de cada usuario y su correspondiente contraseña, logrando una adecuada y eficiente administración de los recursos destinados a red. (véase tabla 16)

Tabla 17. Inventario de equipos utilizado con respectivos usuario y contraseña del segundo escenario.

Fuente: Elaboración propia.

Nombre del equipo	IP	Usuario	Contraseña
Tenda (Principal)	192.168.0.1		T123456789@
Ubiquiti LiteBeam 5AC	192.168.0.22	ubnt	tesis12345.
Ubiquiti Loco 5AC	192.168.0.141	ubnt	tesis123456.
Ubiquiti Loco 5AC	192.168.0.160	ubnt	tesis123456.
Cámara 1	192.168.0.111	admin	admin12345
Cámara 2	192.168.0.120	admin	admin12345

3.3.4 Implementación escenario 3

Siguiendo los escenarios propuestos en sketchup, el ultimo escenario se enfoca en probar los diferentes medios de transmisión y determinar el medio más óptimo y que presenta menos pérdida de datos.

Como resultado, la integración de las cámaras en la red ya existente también resultó más sencilla al mantener la configuración establecida en los escenarios anterior de las cámaras, también se logra la coherencia con las especificaciones de red y la forma en que se manejan los datos de video. El NVR estaba conectado a la cámara en la dirección IP a través de DHCP.

En el proceso de pruebas iniciales, el NVR Asignar de manera automática las direcciones IP de las cámaras, esto garantiza que la cámara sea rápidamente identifica y reconocida por la red del NVR.

Una vez establecida la conexión inicial mediante DHCP, se cambió la configuración de IP de la cámara a una dirección IP estática, el cambio de IP es algo necesario para el desarrollo del escenario, ya que una dirección IP estática asegura una identificación fija de la cámara, se configuró esta IP estática de manera que, en el caso de una implementación con cableado y otra sin cable de transmisión, se implementó para que ambos métodos no se interrumpieran. Por lo tanto, las cámaras no se desconectan o se pierden su conectividad y estabilidad, logrando optimizar, así, una mejor cobertura y fiabilidad del sistema CCTV en la última instalación escenario.

Antes de continuar con la implementación del último escenario se verificar la configuración de red de cada cámara.

Cámara 1

En el caso de la cámara 1, se mantuvieron las configuraciones previamente establecidas, al conectarse al NVR se estableció inicialmente en modo DHCP para facilitar su detección automática en la red. Sin embargo, para uso más práctico se cambió por IP estática con un nuevo direccionamiento, dicho datos actualizados de la configuración de red se puede visualizar en ilustración 106.

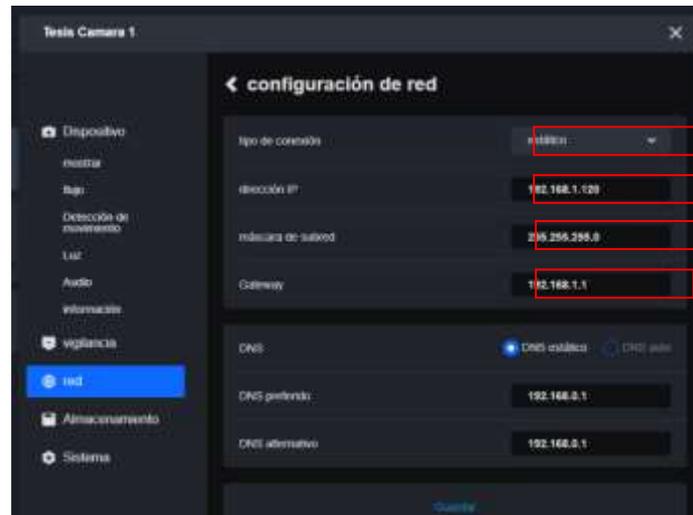


Ilustración 331. Configuración de red actualizado para 3° escenario.

Fuente: Elaboración propia.

Cámara 2

Para la cámara 2, se aplicaron los mismos parámetros de configuración ya utilizado en los escenarios anteriores, al conectar la cámara directamente al NVR se configuró en modo de HP para una detección automática y rápida de la red. Sin embargo, con el fin de proporcionar la máxima estabilidad y control del sistema finalmente integrado, se asignó un IP estática para la segunda cámara como en el caso anterior con un direccionamiento específico para una integración definida en la red.

Los detalles completos de la configuración se pueden encontrar en ilustración 107.

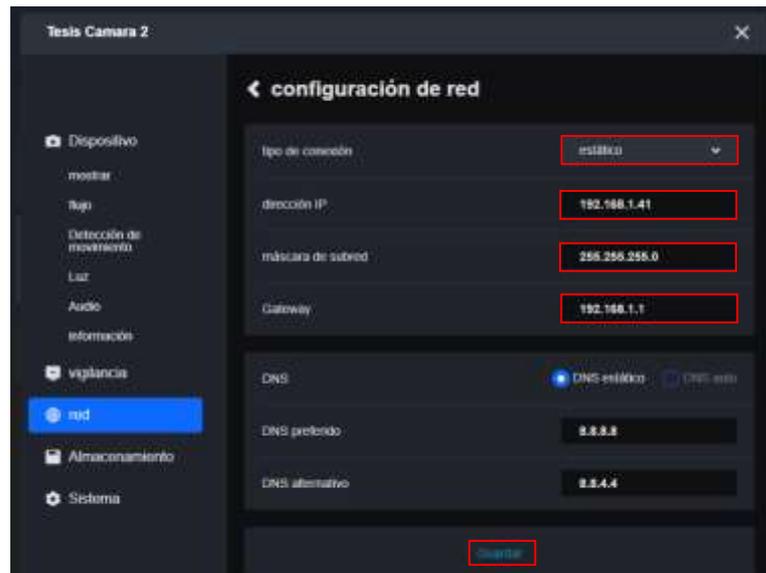


Ilustración 333. Actualización de IP para la segunda cámara.

Fuente: Elaboración propia.

3.3.4.1 Implementación por medio wireless

La implementación de la conexión inalámbrica se llevó a cabo en dos etapas diferenciadas por la frecuencia de transmisión empleada, cada cámara se configuró para conectarse tanto a las redes Wi-Fi emitidas desde el NVR las cuales establecieron en la configuración de red previamente asignada.

Dado que el NVR asigna automáticamente una dirección IP acá dispositivos conectados, lo siguientes a configurar es únicamente dentro de la cámara donde consiste en acceder al menú de configuración de red de la cámara, seleccionar la opción de conexión Wi-Fi y actualizar la red previamente configurada con la nueva red emitida por el NVR.

En el caso de la cámara uno, los nuevos parámetros configurados fueron los siguientes:

- 📶 SSID: NVR TESIS 2.4G
- 📶 Password: T123456789



Ilustración 337. Actualización de conexión inalámbrica cámara 1.

Fuente: Elaboración propia.

Para la segunda cámara se siguió el mismo proceso del anterior cámara diferenciado que a esta nueva cámara se conectara a una Wi-Fi de frecuencia de 5Ghz. para la cámara dos se definieron los nuevos parámetros de la red Wi-Fi a conectar, son los siguientes:



Ilustración 340. Actualización de conexión inalámbrica cámara 2.

Fuente: Elaboración propia.

Una vez teniendo configurada ambas cámaras se continuo con el proceso de implementación, donde se siguió con el diseño empleado en sketchup para las ubicaciones de las cámaras para ellos se ubicaron en la parte frontal del laboratorio la cámara configura con la red de 2.4 GHz ya que debido a alcance que tiene esta

frecuencia fue adecuada para esta ubicación, dicha ubicación se visualiza en la ilustración 111.

Para la segunda cámara se optó por la tercera ubicación del diseño empleado en sketchup, mediante el diseño se instaló en la parte posterior del laboratorio en esta ubicación se instaló la cámara configurada a red de Wi-Fi de 5 GHz, esta ubicación se optó por el poco alcance que tiene esta frecuencia y a la pérdida de señal que tiene al atravesar las paredes del laboratorio, por ellos la ubicación a no tener muchos obstáculos fue la adecuada para la instalación de la segunda cámara.



Ilustración 343. Ubicación de la primera cámara del último escenario.

Fuente: Elaboración propia.



Ilustración 346. Ubicación de la segunda cámara del último escenario.

Fuente: Elaboración propia.

3.3.4.2 Implementación por medio

cableado UTP cat5

Dentro de la implementación utilizando cableado estructurado específicamente UTP cat5, las ubicaciones de las cámaras fueron basadas estratégicamente en base al diseño del escenario 3 en sketchup.

Dadas que ambas cámaras ya se encuentran configuradas con las direcciones IP asignadas por el NVR, el proceso se centró únicamente en la instalación física de cada cámara y el correspondiente tendido del cableado estructurado.

Antes de empezar con el tendido de cableado se eligió la ubicación de cada cámara, empezando con la cámara 1 ubicada en la misma posición que el diseño previamente mencionado, continuando con el tendido del cableado para dicha cámara se conectó un extremo al puerto ethernet 1 del NVR, posteriormente se continuó con el recorrido mediante la estructura que posee el laboratorio facilitando el tendido hasta llegar a que el cableado salga del laboratorio para continuar con el recorrido, hasta llegar a la parte trasera del laboratorio de automatización donde previamente está instalada la cámara RLC-510WA, para conectar el extremo

faltante a el puerto ethernet de la cámara, dicho recorrido fue de 70 metros tomando desde la conexión del NVR hasta la cámara 1.

La cámara 2, se ubicó en la parte posterior del laboratorio como lo sugirió el diseño a seguir de este escenario, una vez defino la ubicación se realizó el debido tendido del cableado, comenzando con conectar un extremo al puerto ethernet 2 del NVR para iniciar el recorrido de igual manera como el tendido anterior se ayudó de las bandeja de cableado ya existente del laboratorio facilitando su recorrido hasta llegar a la parte posterior de laboratorio donde se encuentra la cámara 2 previamente instalada, llegando a este punto se conectar el otro extremo del cable UTP al puerto ethernet de la cámara 2, cabe recalcar que dicho recorrido fue de 10 metros.



Ilustración 349. Conexiones UTP de las cámaras en el NVR

Fuente: Elaboración propia.



Ilustración 352. Instalación de cámara con medio de transmisión de cable UTP.

Fuente: Elaboración propia.

3.3.4.3 Implementación por medio de fibra óptica

Como último medio de transmisión, se implementó la conexión median la fibra óptica, debido a que las cámaras no disponen de puertos de conexión ópticamente es compatible coma se requiere el uso de convertidores de medios para ajustar la señal. En este caso, se utilizaron transceptores TP-link realizar la conversión de la señal eléctrica a óptica permitiendo así la conexión entre la cámara y la red mediante fibra óptica.

De igual manera, que en las instalaciones anteriores se basaron en el diseño previamente propuesto, manteniendo las ubicaciones definidas en el escenario del cableado UTP.

La primera ubicación del tendido de fibra corresponde a la cámara 1, la cual se encuentra instala en la parte trasera del laboratorio de automatización, el tendido inicio:

- ✚ Conectado cable UTP al puerto ethernet 1 del NVR el extremo faltante se conectó al puerto ethernet del transceiver TP-Link, así logrando convertir la señal eléctrica del cable UTP a un medio óptico.
- ✚ La fibra óptica fue conectada mediante conector mecánico SC al cuarto óptico del transceiver, el conector fue realizado de manera específica para evitar pérdida el momento de la inserción al puerto del transceiver. Es importante recalcar la realización del conector mecánico es funcional, pero no es la mejor opción para evitar pérdidas por inserción, por lo general el procedimiento de empalme por fusión es el más adecuado para reducir dichas pérdidas de inserción, dado que contribuirá a reducir la menor pérdida y permitirá una mayor estabilidad en la conexión. No obstante, en la ejecución de la propuesta se optó por el conector mecánico de vino a las conexiones de la infraestructura en la que se realizó la instalación.
- ✚ Como en los escenarios anteriores, el tendido de la fibra se llevó a cabo utilizando las bandejas del cableado para asegurar un recorrido ordenado y protegida. En cuanto al transceiver en esta parte del proceso corresponde al transceiver A o emisor, encargado de la transmisión óptica desde el hasta la ubicación de la cámara
- ✚ Al llegar a la ubicación de cámara debemos de realizar el mismo procedimiento previamente descrito, iniciando con la elaboración del conector mecánico en la fibra óptica, para su posterior conexión con el transceiver B (receptor) el cual en es el encargado de reconvertir la señal óptica a eléctrica.
- ✚ Siguiendo con la conexión, se conectó un cable UTP des el puerto ethernet del transceiver al puerto ethernet de la cámara, de esta manera, se completó la conversión de la señal óptica a un medio de transmisión UTP, lo que permitió una transmisión de datos eficiente y estable entre NVR y la cámara integrando ambos medios de transmisión.

- ✚ El tendido de fibra óptica cubrió una distancia de 70 metros, y dejando una reserva de 3 metros.



Ilustración 358. Conexión entre el NVR y el Transceiver para la primera cámara.

Fuente: Elaboración propia.



Ilustración 355. Conexión del transceiver B para conectar a la cámara.

Fuente: Elaboración propia.

En cuando a la segunda cámara se volvió a realizar el mismo procedimiento mencionado a diferencia que esta vez se comenzó el puerto ethernet 2 del NVR, conectando hacia el transceiver emisora siguiendo con el recorrido al largo del laboratorio hasta donde se encuentra el transceiver B o receptor que de igual manera se realizó el conector mecánico con pulido SC, una vez realizado el tendido de fibra se empleó el cableado utp desde el puerto ethernet del transceiver receptor hasta el puerto ethernet de la cámara, dicha cámara se encuentra ubicada en la parte posterior del laboratorio de telecomunicaciones. El recorrido de fibra óptica cubrió una distancia de 7 metros dejando una reserva de 5 metros, se deja dicha reserva de manera preventiva para cualquier daño que se tenga con el tiempo.



Ilustración 364. Segunda conexión por medio de transceiver para la cámara 2.

Fuente: Elaboración propia.



Ilustración 361. Conexión de la cámara 2 mediante UTP después de haber Utilizado el transceiver B.

Fuente: Elaboración propia.

3.3.5 Implementación de código en Python

Para la elaboración del código, se implementó un lenguaje de programación basada en Python, debido a su versatilidad y eficiencia en la gestión de código. No obstante, considerando que la interfaz nativa de Python puede resultar menos intuitiva para la programación se optó por incorporar el software Visual Studio Code. Esta herramienta complementaria ofrece una interfaz más amigable y una serie de funcionalidad avanzada que facilita la escritura, depuración y gestión del código.

Para la instalación de Python se debe seguir los siguientes pasos:

- ✚ Se deber de descargar el archivo desde la página oficial de Python o del siguiente link <https://www.python.org/downloads/>.
- ✚ Una vez descargado debemos de tener el siguiente archivo con nombre “python-3.12.4-amd64.exe”.
- ✚ Teniendo el archivo debemos de dar clic derecho y ejecutar como administrador una ventana se abre automáticamente donde debemos presionar la opción sí.
- ✚ Llegado a este punto se abrirá una ventana para iniciar con el proceso de instalación, donde debemos de seleccionar la opción de Install Now.

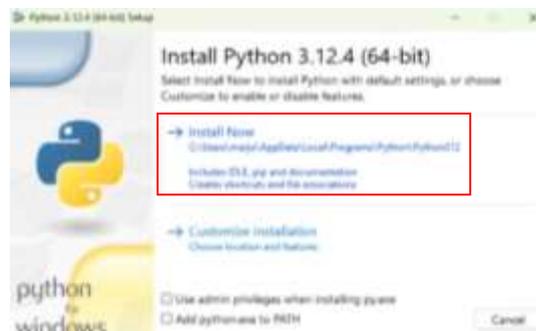


Ilustración 367. Proceso de instalación de Python.

Fuente: Elaboración propia.

- ✚ Después de selecciona solo debemos de esperar hasta que se complete el proceso de instalación de software, para verificar que el programa se instaló correctamente se procede en ubicarnos en la opción de buscar de la PC y buscar “Python 3.12.3(64-bit).

Teniendo ya instalado Python procedemos a realizar la instalación de Visual Studio Code para ellos debemos de seguir el siguiente paso:

- ✚ Para iniciar con la instalación del software primero debemos de descargar el instalador para ellos debemos de dirigirnos al siguiente link <https://code.visualstudio.com/download>, donde se visualizar el diferente archivo de instalación correspondiente a la característica de la PC que se instalara.
- ✚ Una vez descargado debemos de buscar el archivo con nombre “VSCodeUserSetup-x64-1.88.0.exe” ya teniendo el archivo procedemos a ejecutar, se despliega una ventana donde inicia el proceso de instalación para ellos debemos de seleccionar que aceptados lo termino de instalación y procedemos a dar en “Siguiente”.



Ilustración 370. Aceptación de termino en el proceso de instalación de Visual Studio Code.

Fuente: Elaboración propia.

- ✚ En la siguiente ventana que muestra en la ilustración 120, nos muestra el siguiente paso de la instalación donde procedemos a seleccionar la ubicación donde estará el archivo teniendo establecido la ruta del archivo procedemos a dar en “Siguiente”.

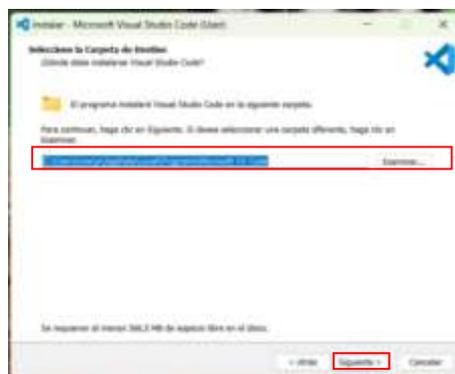


Ilustración 373. Ubicación del Archivo Visual Studio Code.

Fuente: Elaboración propia.

- En esta etapa de la instalación, se ofrece la opción de crear acceso directo en el escritorio entre otras posibilidades. Antes de llegar a esta ventana, se nos muestra otra en la cual simplemente debemos seleccionar “siguiente”, como vemos en la ilustración 121.



Ilustración 376. Creación de acceso directo.

Fuente: Elaboración propia.

- Para finalizar debemos esperar mientras se instale el software de Visual Studio Code, una vez se instale debe de mostrar una ventana igual a la ilustración 96, donde se muestra que la instalación fue exitosa y el software está listo para ser utilizado.



Ilustración 379. Finalización del proceso de instalación.

Fuente: Elaboración propia.

Ante de explicar la codificación debemos de tener en cuenta que el programa de Visual Studio Code no se encuentra conectado directamente con Python, para ellos debemos de instalar las extensiones correspondientes dentro de la interfaz de visual studio code.

Para realizar eso debemos que abrir el programa de visual studio code y ubicarnos en el apartado de extensión lo mencionado se visualiza en la ilustración 98. Una vez estando en apartado de extensión debemos de buscar las extensiones de Python y

proceder a instalar, para verificar que se encuentra instalada las extensiones deben esta igual como en la ilustración 123.



Ilustración 381. Instalación de extensiones de Python dentro de visual studio code.

Fuente: Elaboración propia.

Dentro de la propuesta se elaboraron dos códigos enfocados en diferentes análisis, el primer código emplea un modelo de aprendizaje automático Yolov5 el cual se enfoca en detectar varios objetos y a la vez calcular la distancia en tiempo real de cada uno, lo que permite una medición precisa y exacta de cada objeto detectado en entorno que requiera un seguimiento preciso de objetos.

El segundo código fue diseñado en la elaboración de círculos de referencia, creados mediante una cámara IP específica para el estudio del cálculo de distancia entre ambas cámaras y comparado con valores obtenidos físicamente, los círculos de referencia son creados a partir de la vista panorámica de cada cámara enfocando distancia en metros.

3.3.5.1 Código de cálculo de distancia de objetos en tiempo real

Para la implementación del código, se utilizó varias librerías dentro del entorno de visual studio code, entre las librerías incluyen:

- 📦 Open CV
- 📦 Pandas
- 📦 Numpy
- 📦 Yolov5
- 📦 Torch

3.3.5.1.1 Instalación librería OpenCV

La librería OpenCV (Open Source Computer Vision Library) es una biblioteca de software de código abierto dedicada a la visión por computadora y el aprendizaje automático. Fue desarrollada inicialmente por Intel y está disponible para múltiples plataformas, incluyendo Windows, Linux, macOS y Android. Su propósito

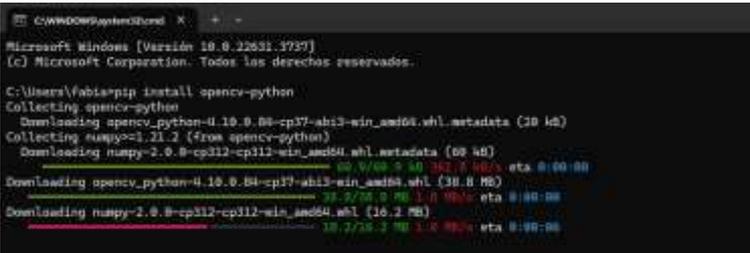
principal es proporcionar una infraestructura común para aplicaciones de visión por computadora y facilitar el uso de estos algoritmos en aplicaciones comerciales y de investigación.

Aplicaciones de librería OpenCV

- ✚ Procesamiento de imágenes.
 - ✚ Reconocimiento de patrones.
 - ✚ Análisis de video.
- ✚ Fotografía computacional.
 - ✚ Realidad aumentada.
 - ✚ Robótica.

Para la instalación de la librería se debe de seguir los siguientes pasos:

1. Abrir el command terminal del computador realizando la combinación de tecla “Windows” + “R”, a ejecutar esta combinación se despliega una pestaña donde debemos de ingresar “cmd” para así abrir el command terminal.
2. Una vez dentro del command terminal debemos de escribir el siguiente comando “pip install opencv-python” y presionamos enter.
3. En la ilustración 124, nos muestra el proceso de instalación de la librería donde se encuentra descargando todos los paquetes de la librería opencv, solo se debe esperar hasta que finalice el proceso y cerrar el command terminal para este punto ya puede utilizar la librería dentro de visual studio code.



```

C:\WINDOWS\system32\cmd X + +
Microsoft Windows [Versión 10.0.22631.3937]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\fabia>pip install opencv-python
Collecting opencv-python
  Downloading opencv_python-4.10.0.84-cp37-abi3-win_amd64.whl.metadata (30 kB)
Collecting numpy<=1.21.2 (from opencv-python)
  Downloading numpy-2.0.0-cp312-cp312-win_amd64.whl.metadata (88 kB)
  Downloading numpy-2.0.0-cp312-cp312-win_amd64.whl (30.9 MB)
  Downloading opencv_python-4.10.0.84-cp37-abi3-win_amd64.whl (38.8 MB)
  Downloading numpy-2.0.0-cp312-cp312-win_amd64.whl (16.2 MB)

```

Ilustración 385. Instalación de librería OpenCV.

Fuente: Elaboración propia.

3.3.5.1.2 Instalación librería numpy

La librería numpy (numerical Python) es una biblioteca fundamental para la computación científica en Python, tiene la capacidad de manejar grandes volúmenes de datos y realizar operaciones matemáticas. Una de las cualidades es que puede utilizar array y matrices multidimensionales, junto con una colección de funciones matemáticas, lógicas.

Características de la Librería numpy

- ✚ Arrays multidimensional.
- ✚ Broadcasting.
- ✚ Funciones matemáticas y lógicas.
- ✚ Manipulación de arrays.
- ✚ Integración de otras librerías.

En la instalación de la librería dentro del software visual studio code debemos de seguir las siguientes indicaciones:

1. Para instalar de la librería numpy, debemos de seguir el primer paso de la instalación de opencv.
2. Llegado a este punto estando en el command terminal debemos digitar el siguiente comando para proceder con la instalación de la librería “pip install numpy””.
3. Al ejecutar este comando se inicia el proceso de descarga e instalación de la última versión de numpy, cómo se muestra lustración 125.



```

C:\Users\chadlan> pip install numpy
Collecting numpy
  Downloading numpy-1.24.3-cp310-cp310-macosx11.0.pkg (11.2 MB)
Installing collected packages: numpy
Successfully installed numpy-1.24.3

```

Ilustración 388. Instalación de librería Numpy.

Fuente: Elaboración propia.

3.3.5.1.3 Instalación librería PyTorch

Anteriormente se conocía como torch, pero en la actualidad lleva por nombre PyTorch es una biblioteca de aprendizaje automático mediante código abierto basado en Python y lúá, fue desarrollada en el año 2016 por la empresa Facebook AI Research ahora conocido como Facebook Meta.

Se ha convertido en una herramienta muy popular para el desarrollo de redes neuronales profundas y modelos de aprendizaje automático, tiene una facilidad de uso y se integra perfectamente con Python.

Dentro de esta librería tenemos las siguientes características:

- ✚ Facilidad de uso.
- ✚ Rendimiento.
- ✚ Flexibilidad.
- ✚ Comunidad.

Componentes de la librería PyTorch

- ✚ Tensores dinámicos.
- ✚ Autograd (diferencias automáticas).
- ✚ Modelos de redes neuronales.

- 🚦 Interoperabilidad con Numpy.
- 🚦 Entrenamiento en GPU

Como en el caso de las librerías anteriores se explicará a continuación la instalación de esta librería dentro del software utilizado visual studio code.

1. Debemos a repetir el paso 1 para llegar al command terminal
2. Estando dentro del command terminal procedemos a escribir el siguiente comando para instalar la librería PyTorch “pip install torch torchvision torchaudio”
3. Al escribir el comando mencionado se procede a instalar todos los componentes necesarios para utilizar la librería PyTorch cómo se muestra en la ilustración 126, qué nos enseña el proceso de instalación de los componentes dentro del programa.

```

C:\Users\user> pip install torch torchvision torchaudio
Collecting torch
  Downloading torch-2.0.1-cp39-cp39-macosx_11_0_arm64.whl (440.6 MB)
Collecting torchvision
  Downloading torchvision-0.17.1-cp39-cp39-macosx_11_0_arm64.whl (1.1 MB)
Collecting torchaudio
  Downloading torchaudio-0.12.1-cp39-cp39-macosx_11_0_arm64.whl (1.1 MB)
Collecting numpy
  Downloading numpy-1.24.3-cp39-cp39-macosx_11_0_arm64.whl (14.7 MB)
Collecting setuptools
  Downloading setuptools-68.0.0-py3-none-any.whl (609 kB)
Collecting typing_extensions
  Downloading typing_extensions-4.6.2-py3-none-any.whl (35 kB)
Collecting filelock
  Downloading filelock-3.11.1-py3-none-any.whl (9.8 kB)
Collecting jinja2
  Downloading jinja2-3.1.2-py3-none-any.whl (133 kB)
Collecting MarkupSafe
  Downloading MarkupSafe-2.1.2-cp39-cp39-macosx_11_0_arm64.whl (11 kB)
Collecting sympy
  Downloading sympy-1.11.1-py3-none-any.whl (5.4 MB)
Collecting mpmath
  Downloading mpmath-1.3.0-py3-none-any.whl (506 kB)
Collecting fsspec
  Downloading fsspec-2023.10.0-py3-none-any.whl (168 kB)
Collecting aiohttp
  Downloading aiohttp-3.8.6-cp39-cp39-macosx_11_0_arm64.whl (380 kB)
Collecting aiohttp-retry
  Downloading aiohttp_retry-2.8.3-py3-none-any.whl (10.1 kB)
Collecting tqdm
  Downloading tqdm-4.66.1-py3-none-any.whl (78 kB)
Collecting safetensors
  Downloading safetensors-0.4.0-cp39-cp39-macosx_11_0_arm64.whl (1.1 MB)
Collecting huggingface_hub
  Downloading huggingface_hub-0.19.4-py3-none-any.whl (485 kB)
Collecting pyyaml
  Downloading pyyaml-6.0.1-py3-none-any.whl (138 kB)
Collecting requests
  Downloading requests-2.31.0-py3-none-any.whl (48 kB)
Collecting urllib3
  Downloading urllib3-2.0.7-py3-none-any.whl (124 kB)
Collecting certifi
  Downloading certifi-2023.11.17-py3-none-any.whl (159 kB)
Collecting idna
  Downloading idna-3.6-py3-none-any.whl (61 kB)
Collecting charset-normalizer
  Downloading charset-normalizer-3.3.2-py3-none-any.whl (66 kB)
Installing collected packages: typing_extensions, urllib3, tqdm, safetensors, requests, pyyaml, numpy, MarkupSafe, jinja2, filelock, aiohttp-retry, aiohttp, sympy, mpmath, huggingface_hub, fsspec, certifi, charset-normalizer, idna, torch, torchvision, torchaudio
Successfully installed aiohttp-3.8.6 aiohttp-retry-2.8.3 certifi-2023.11.17 charset-normalizer-3.3.2 filelock-3.11.1 fsspec-2023.10.0 huggingface_hub-0.19.4 idna-3.6 jinja2-3.1.2 MarkupSafe-2.1.2 mpmath-1.3.0 numpy-1.24.3 pyyaml-6.0.1 requests-2.31.0 safetensors-0.4.0 sympy-1.11.1 torch-2.0.1 torchvision-0.17.1 torchaudio-0.12.1 tqdm-4.66.1 typing_extensions-4.6.2 urllib3-2.0.7
  
```

Ilustración 391. Proceso de instalación de librería PyTorch.

Fuente: Elaboración propia.

3.3.5.1.4 Instalación librería pandas

El nombre de pandas es una contracción del término “Panel Data”, es una biblioteca de análisis de datos dentro del software libre Python, esta librería está diseñada para flexibilizar las prácticas y eficiencia en la hora de trabajar con datos etiquetados y relacionados especialmente en dos estructuras de datos importantes:

- 🚦 Series de datos unidimensionales
- 🚦 DataFrame

Pandas es una librería ampliamente utilizada dentro de las ciencias de datos, análisis de datos y aprendizaje automático gracias a su gran amplia capacidad para manejar grandes volúmenes de datos y realizar operaciones complejas de una manera eficiente.

Características de la librería pandas

- 🚦 Estructura de datos flexible.
- 🚦 Manipulación de datos.

- ✚ Indexación y selección de datos.
- ✚ Entrada y salida de datos.
- ✚ Manipulación de fechas y tiempo.
- ✚ Visualización de datos.

Aplicación de pandas

- ✚ Análisis de datos
- ✚ Ciencia de datos y aprendizaje automático
- ✚ Manipulación de datos
- ✚ Finanzas y economía

De igual manera que en los casos anteriores se empleará una pequeña guía de instalación de dicha librería para usar dentro del software visual estudio code ya que hay otra manera de instalación como por el medio de GitHub.

1. Se repite el mismo paso que con las instalaciones de las librerías anteriores con la diferencia que se utilizó otro comando “pip install pandas”.
2. Una vez digitado el comando se procede instalar diferentes componentes de la librería cómo se muestra en la ilustración 127, dicha ilustración no muestra los diferentes componentes instalados hasta la finalización de esta al salir de esta ventana se verifica que la instalación fue realizada correctamente.

```

C:\Users\user> pip install pandas
Collecting pandas
  Downloading pandas-2.0.0-py3-none-any.whl (10.4 MB)
    100% |#####| 10.4 MB 1.8 MB/s
Collecting numpy
  Downloading numpy-1.26.0-cp311-cp311-win32.whl (10.4 MB)
    100% |#####| 10.4 MB 1.8 MB/s
Collecting scipy
  Downloading scipy-1.11.0-cp311-cp311-win32.whl (10.4 MB)
    100% |#####| 10.4 MB 1.8 MB/s
Collecting matplotlib
  Downloading matplotlib-3.7.1-cp311-cp311-win32.whl (10.4 MB)
    100% |#####| 10.4 MB 1.8 MB/s
Collecting python-dateutil
  Downloading python_dateutil-2.8.2-py2.py3-none-any.whl (247 kB)
    100% |#####| 247 kB 1.8 MB/s
Collecting pytz
  Downloading pytz-2023.3-py2.py3-none-any.whl (502 kB)
    100% |#####| 502 kB 1.8 MB/s
Collecting tzdata
  Downloading tzdata-2023.3-py2.py3-none-any.whl (309 kB)
    100% |#####| 309 kB 1.8 MB/s
Installing collected packages: pandas, numpy, scipy, matplotlib, python-dateutil, pytz, tzdata
Successfully installed pandas-2.0.0 numpy-1.26.0 scipy-1.11.0 matplotlib-3.7.1 python-dateutil-2.8.2 pytz-2023.3 tzdata-2023.3

```

Ilustración 394. Proceso de instalación de librería Pandas.

Fuente: Elaboración propia.

3.3.5.1.5 Instalación librería Yolov5

Yolov5 es un modelo de aprendizaje que es utilizado para la detección de objeto, el nombre de Yolo es acrónimo de (You Only look Once) y el v5 de la versión utilizada, desarrollada por la empresa Ultralytics.

Posee la cualidad de detectar objetos ya sea uno o varios dentro de una imagen o video, además de poder clasificar el objeto detectado dependiendo de su clase ya

sea una persona, animal o cosa, dicho objeto se proporciona un cuadro delimitando dicho objeto para indicar su ubicación exacta. [47]

Características del modelo de aprendizaje YOLOv5:

- ✚ Eficiencia y velocidad.
- ✚ Facilidad de uso.
- ✚ Compatibilidad y despliegue.

Dentro de los usos del modelo tenemos:

- ✚ Robótica.
- ✚ Control de calidad industrial.
- ✚ Vehículos autónomos.
- ✚ Vigilancia.
- ✚ Análisis de imágenes médicas.

El modelo de aprendizaje se encuentra en el siguiente link <https://github.com/ultralytics/yolov5>, donde se puede utilizar desde el mismo repositorio GitHub o también descargando el archivo en los formatos que ofrece.

Para ejecutar el modelo desde la plataforma GitHub se utiliza la librería Torch dentro del código se añade la siguiente línea de código:

```
model = torch.hub.load('ultralytics/yolov5', 'yolov5s', trust_repo=True)
```

de la línea mencionada cabe recalcar lo siguiente: se usó **torch.hub.load** para cargar el modelo preentrenados directamente del repositorio GitHub, **'ultralytics/yolov5'** se establece el lugar dentro del repositorio donde se encuentra alojado el modelo YOLOv5, **'yolov5s'** indica qué versión del modelo se está cargando en este caso se carga la versión pequeña se identifica por la letra “s” al final de la palabra yolov5 y por ultimo **trust_repo=True** al ser un modelo cargado desde un repositorio publico este argumento nos ayudara a eludir algunas característica de seguridad.

3.3.5.1.6 Desarrollo del código

Para la realización del código de un sistema de detección y medición de distancia en tiempo real utilizando cámaras IP y un modelo de detección de objetivo basado en el modelo YOLOv5. Para el desarrollo del código se estructuro en varios pasos fundamentales, los cuales se describirán a continuación:

1. Importación de librerías: se importan las librerías necesarias para la detección de objetos y procesamiento de imágenes, en este caso se una “cv2” para operar una imagen usando OpenCV, “numpy” para objetivos de arrays y matrices numéricas, “torch” para operaciones con PyTorch, y

por último “pandas” para operaciones de manipulación de datos tabulares que podamos necesitar si queremos analices adicionales.

2. Verificación de dispositivos: se utiliza para verificar con PyTorch si el sistema posee un GPU en caso de ser cierto, se configura el dispositivo en “Cuda”, ya que el rendimiento para el procesamiento será mucho más rápido, pero si es falso, usaremos la CPU.
3. Cargar el modelo YOLOv5: usaremos el modelo YOLOv5 preentrenados para la operación de detectar objetos. La carga del modelo se realizará usando el comando “torch.hub.load” en el código que cargará un modelo de torchvision, además especificar la versión del modelo a utilizar.
4. Definición de clases: de objetos que pueden detectar en el modelo son extraídas del modelo YOLOv5 y almacenadas en las variables “classes”, gracias al cual es posible identificar el nombre de cada objeto identificado en tiempo real.
5. Configuración de parámetros de la cámara y objetos: se define la longitud focal estimada y la altura real del objeto, típicamente la altura promedio de una persona en metros. Estos parámetros son necesarios para el cálculo de la distancia entre la cámara y el objetivo identificado por medio de la fórmula, qué relación a la altura real del objetivo con sus tamaños en píxeles.
6. Configuración de la conexión a la cámara IP: se establece la conexión a la cámara IP utilizando el protocolo RTSP con la URL de la conexión de la cámara Reolink, se inicia la captura de vídeo en tiempo real mediante el comando “cv2.VideoCapture”.
7. Captura de video y detección de objetos: se estableció un bucle para la captura de vídeo, donde en cada iteración, se lee un frame y se controla que la lectura sea exitosa. Luego, se convierte el frame de BGR a RGB, un formato requerido por el modelo YOLO v5
8. Proceso de detección con YOLOv5: para cada frame, se aplica el modelo YOLOv5 de detección de objetos, estas detecciones incluyen coordenadas del objeto de las imágenes, el índice de la clase del objetivo y el nivel de confianza

9. Filtrado y extracción de información: luego, para cada objeto detectado, se define un filtro de confianza y sólo se muestra las detecciones en la pantalla sin la confianza supera el 50%. Luego, se extraen las coordenadas del objetivo en píxeles y se define la clase del objeto aceptado con el índice recibido por el modelo.
10. Estimación de distancia: Mediante la altura de los objetivos en píxeles y la fórmula de distancia $“(altura_real * longitud_focal) / altura_píxeles”$, usando los parámetros mencionados son necesarios para realizar el calcula la distancia aproximada en metro entre la cámara y el objetivo.
11. Visualización de resultado: sobre cada objeto detectado, se dibuja un rectángulo verde que lo rodea, también se muestra el nombre de la clase del objeto y la distancia estimada en metros. Se ha ajustado el tamaño y el grosor del texto para mejorar la legibilidad.
12. Redimensionado y visualización del video en tiempo real: finalmente, redimensionamos el frame para que se ajuste a la ventana de visualización y mostramos en una ventana titulada “Video en tiempo real con detección y distancia”. Este proceso permite ver el vídeo en tiempo real junto con la detecciones y distancias calculadas
13. Finalización del proceso: el bucle que captura continúa ejecutándose hasta que se presione la tecla “q”, al presionar dicha tecla la cámara se libera y cierra todas las ventanas de visualización finalizando así el proceso de captura y procesamiento de imágenes y distancias en tiempo real.

Una vez concluido con los pasos descrito anteriormente, se obtuvo un código final funcional que opera sin errores y presenta un desempeño optimo en la detección de objetos y estimación de distancia en tiempo real, para consultar el código completo y detallado, véase el anexo 1.

3.3.5.2 Código de cálculo de distancia entre dos camaras

3.3.5.2.1 Instalación de librería matplotlib

La librería matplotlib, es una librería utilizada dentro de python para crear gráficos y visualización de datos, la palabra matplotlib es la combinación de 2 palabras MAT, qué hace referencia a Matlab, ya que fue desarrollada originalmente para

proporcionar a los usuarios de python una alternativa abierta y gratuita a las capacidades de gráficos de Matlab. Y PLOTLIB abreviaturas de “plotting library”.

Anteriormente se mencionó que fue desarrollada en base a Matlab, lo que permite generar gráficos en 2 DY, líneas, dispersión, histograma, gráfico de barra y otros tipos de visualización.

Características de la librería matplotlib:

- ✚ Interfaz fácil de usar
- ✚ Variedad de gráficos
- ✚ Personalización completa
- ✚ Integración con otras bibliotecas

Aplicaciones

- ✚ Análisis de datos estadística
- ✚ Ciencia de datos y machine learning.
- ✚ Investigación científica.
- ✚ Finanzas y economía.
- ✚ Visualización de redes.
- ✚ Geografías y datos espaciales

Para la instalación de la librería se realizará una pequeña guía, la cual se mostrará a continuación:

1. Abrir el command terminal del computador realizando la combinación de tecla “Windows” + “R”, a ejecutar esta combinación se despliega una pestaña donde debemos de ingresar “cmd” para así abrir el command terminal.
2. Una vez dentro del command terminal debemos de digitar el siguiente comando “pip install matplotlib” y presionamos enter para iniciar con la descarga e instalación de la librería.
3. En la ilustración 128, podemos observar el proceso de descarga y los diferentes componentes que se instalando junto a la librería, una vez que el proceso de descarga termine y en el Command terminal

podamos navegar, procedemos a cerrar la pestaña de Command terminal y dirigirnos a visual studio code.



```

C:\Users\Usuario> pip install matplotlib
Collecting matplotlib
  Using cached matplotlib-3.5.0-py3-none-any.whl (12.9 MB)
Collecting numpy<=1.24.0, >=1.21.0
  Using cached numpy-1.24.0-cp310-cp310-win32.whl (19.8 MB)
Collecting python-dateutil<=2.8.2, >=2.7
  Using cached python_dateutil-2.8.2-py2.py3-none-any.whl (249 kB)
Collecting cycler<=0.11.0, >=0.10
  Using cached cycler-0.11.0-py3-none-any.whl (7.1 kB)
Collecting fonttools<=4.42.0, >=4.22.0
  Using cached fonttools-4.42.0-py3-none-any.whl (1.0 MB)
Collecting kiwisolver<=1.4.5, >=1.3.1
  Using cached kiwisolver-1.4.5-cp310-cp310-win32.whl (130 kB)
Collecting packaging<=23.1, >=20.9
  Using cached packaging-23.1-py3-none-any.whl (47 kB)
Collecting pillow<=9.5.0, >=8.1.2
  Using cached pillow-9.5.0-cp310-cp310-win32.whl (2.2 MB)
Collecting pyparsing<=3.1.0, >=3.0.7
  Using cached pyparsing-3.1.0-py3-none-any.whl (101 kB)
Installing collected packages: pillow, pyparsing, python-dateutil, packaging, fonttools, cycler, numpy, kiwisolver, matplotlib
Successfully installed matplotlib-3.5.0 numpy-1.24.0 python-dateutil-2.8.2 packaging-23.1 fonttools-4.42.0 cycler-0.11.0 kiwisolver-1.4.5 pillow-9.5.0 pyparsing-3.1.0

```

Ilustración 397. Instalación de Liberia matplotlib.

Fuente: Elaboración propia.

3.3.5.2.2 Desarrollo del código

El código que desarrollar nos permitirá la visualización en tiempo real de la escala de distancia sobre la imagen capturada desde una cámara IP, utilizando círculos concéntricos los cuales representaran las distancias relativas en metros. Para el desarrollo del código se estructuró en varios pasos fundamentales, los cuales se describirán a continuación:

1. Importación de librerías: Se importa las librerías necesarias para el procedimiento y visualización de imagen. Se usa “cv2” para la alimentación del vídeo y la manipulación de la imagen, “matplotlib.pyplot” para la visualización en tiempo real con gráficos y “numpy” para cálculos matemáticos requerido para el análisis de distancia.
2. Configuración de las cámaras IP: Se agregaron los URLD streaming en tiempo real con protocolo de transmisión RTS de ambas cámaras IP. A través de cv2.VideoCapture, mediante la función anterior se realiza la apertura de la transmisión de video, además se verificará si ambas cámaras están conectadas caso contrario no se ejecuta el resto de línea de código.
3. Visualización y configuración de la figura: Previamente se verificar que ambas cámaras, matplotlib se encarga de mostrar la imagen adquirida por la cámara IP, además se configura el tamaño de 15x15

pulgada de la imagen resultante al momento de la ejecución del código.

4. Función de dibujo de círculos de distancia: La función “draw_distancia_circles” recibe como parámetro el frame de la cámara, en el centro de los círculos en píxeles y el radio máximo en Pixel para crear varios círculos y un factor de conversión de píxeles a metros.

En la misma función se asigna el color y el grosor, así como el tamaño y el grosor de las etiquetas de texto. En la elaboración de los círculos se realizando calcula un radio diferente y la distancia correspondiente en metro al radio del círculo, una vez realizado el cálculo se presenta lo obtenido en la imagen resultante al ejecutar el código en tiempo real.

5. Función de cálculo de distancia entre punto: La función “calculate_distance” calcula la distancia euclidiana entre dos puntos en pixeles, lo cual se utiliza para determinar la distancia entre el centro de la cámara en el fotograma.
6. Establecimientos de factor de conversión: Se establece una distancia de referencia en metros y la correspondiente en pixeles, se usan para calcular un factor de conversión que permite estimar la distancia real en metros a partir de los píxeles en el fotograma
7. Bucle de captura y procesamiento de imagen: Se define un bucle, que se encarga de capturar imágenes de ambas cámaras IP dentro de cada iteración:
 - ❖ Se verifica la captura de ambos fotogramas, y en caso de error, se finaliza el ciclo.
 - ❖ Para la cámara 2, se calcula el centro y el radio máximo para los círculos de distancia. Luego se llama a la variable “draw_distance_circles” para dibujar círculos concéntricos sobre el fotograma, indicando en la escala de la distancia.

- ❖ Para calcular la distancia en píxeles entre el centro de las ambas cámaras se calcula con “calculate_distance” se convierte a metros utilizando el factor de conversión.
8. Visualización en tiempo real: El fotograma con los círculos se convierte a formato RGB y se muestra mediante matplotlib. La figura mostrada se va actualizando en tiempo real para así lograr mostrar el vídeo capturado con las escalas de distancia.
 9. Liberación de recurso: Finalizando con el código, una vez detenido el bucle de captura, proceden a liberar los recursos de las ambas cámaras y se cierra automáticamente las ventanas de visualizade OpenCV

Una vez completados los pasos descritos anteriormente, se obtuvo un código funcional el cual presenta un óptimo funcionamiento a la hora de visualizar los círculos de distancia en la cámara número 2, los cuales presentan una distancia acertada a la hora de verificar externamente la distancia entre la cámara. Para consultar el código completo y detallado, véase el anexo 2

3.3.5.3 Desarrollo de un generador de ruido en GNU Radio

Ante de empezar con el proceso de desarrollo del diagrama, debemos de tener instalado el software de GNU Radio, el programa debe se instalado correctamente caso contrario presentarás fallas al momento de conectar el HackRF One, donde no reconocerá el puerto conectado.

Para evitar eso se basó el proceso de instalación en base a la tesis titula **aplicación óptica para el desarrollo de procesos lógicos utilizando GNU radio y tecnología SDR** para acceso directo al proceso de instalación seguir el siguiente link <https://repositorio.upse.edu.ec/bitstream/46000/10316/1/UPSE-TTE-2023-0003>, dentro del documento dirigirse a la página 206-213.

Una vez seguido con los pasos mencionados abrimos el software GNU radio donde debemos de tener una pantalla similar a la siguiente:

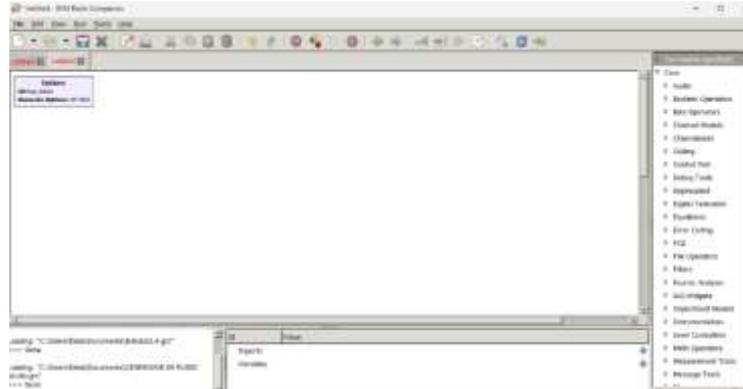


Ilustración 400. Pantalla de inicio de GNU radio.

Fuente: Elaboración propia.

3.3.5.4 Definiciones de diferentes bloques en GNU Radio

Previo a iniciar con el diseño del generador de ruido, fundamental comprender las funciones de los bloques que se utilizaran, esto garantiza que el proceso sea más preciso y eficiente al momento de configurar cada bloque, permitiendo optimizar el desempeño del sistema, a continuación se presentan varios bloques disponibles en GNU radio juntos con su descripción de su funcionamiento:

Options

El bloque “Options” permite configurar variables globales del flujo de datos, entre ellos el nombre y descripción, dentro del bloque se define el tipo de interfaces gráficas se está desarrollando pueden ser QT GUI, WX GUI, No GUI, también facilita la integración con otros sistemas y herramientas, realizando las respectivas configuraciones asegurando el flujo de datos logrando comunicarse correctamente con hardware específico o sistemas externos.

Variable

El bloque “variable”, es utilizado como variable global, resultando esencial en diagramas de flujos donde se necesite dicha variable en diferentes bloques, facilitando la modificación de ellos, es común utilizarlo en valores en frecuencia, `sample_rate` o tasa de muestreo, ganancia, y otros parámetros

Wx gui slider

El bloque “Wx GUI Slider”, permite al usuario modificar valores en los parámetros establecidos en el diagrama de flujo, sin necesidad de detener la simulación mediante un control deslizante, dentro del rango establecido, es ideal utilizar este bloque para el uso de audios y videos.

Wx gui text box

El bloque “Wx GUI Text Box”, permite ingresar texto o números deseados, dentro de la ejecución del diagrama, sin necesidad de detenerla, estos pueden ser parámetros de ganancia, frecuencia y umbrales, facilitando la configuración de bloques dentro del diagrama.

Wx gui notebook

El bloque “Wx GUI Notebook”, permite al usuario organizar los resultados mediante panel de control, en una sola ventana, pero en diferentes secciones, mejorando la presentación de los resultados obtenidos en el diagrama de flujo, estos pueden ser gráficos de tiempo y frecuencia, controles deslizantes o cajas de textos.

Wav file Source

El bloque “Wav file Source”, permite leer datos de un archivo en formato WAV y utilizarlo como fuente de entrada para el diagrama de flujo en procesamiento de señales, sirve para aplicaciones que requieren la reproducción o análisis de datos de un audio pregrabado, la implementación de este bloque ayuda en proyectos de sistemas de comunicación, simulación de entorno acústico y el procesamiento de señales de audio, proporciona muestras de audio en formato de punto flotante (float) o entero (int), según el proyecto.

Audio Source

El bloque “Audio Source”, permite capturar y utilizar datos de audios proveniente de un dispositivo de entrada, estos pueden ser tarjetas de sonido, micrófono que estén dentro del flujo de datos, facilitando el análisis de señales de audio en vivo, mientras proporciona una fuente de entrada directa y continua de datos de un audio. Este bloque resulta útil en sistemas de comunicación, procesamiento de una señal de voz, y experimentación con señales acústicas, permitiendo a los usuarios procesar, analizar y manipular señales de voz, estas pueden ser en formato punto flotante (float) o entero (int), dependiendo el proyecto.

Multiply const

El bloque “Multiply const”, es utilizada para escalar una señal multiplicándole por una constante, siendo importante en el procesamiento de señales, permitiendo ajustar la amplitud de una señal, al realizar esto se puede aumentar o disminuir la señal según la necesidad, este bloque es considerado en aplicaciones que necesitan

normalización de señal, ajuste de ganancia, o calibración de amplitud, entre ellas están sistemas de comunicación, potencia de una señal transmitida o recibida, evitando distorsión o saturación en el proyecto.

Add

El bloque “add”, permite realizar operación de suma entre dos o más señales de entrada, combinando en una única señal de salida, este opera en el dominio de las muestras, significando que pasa cada muestra en los flujos de entradas, realiza una suma aritmética de los valores correspondiente generando una muestra de salida con el resultado, resultando útil en aplicaciones de procesamiento de señales, en sistemas de modulaciones y demodulación, así como en superposición de señales, al permitir que la suma directa de las señales facilita la manipulación y análisis de datos.

Rational resampler

El bloque “Rational resampler”, permite aumentar o disminuir la tasa de muestreo de una señal de manera eficiente, donde la tasa de muestreo se define por una relación de numero enteros (L/M), usando dos operaciones consecutivas, primero expandiendo la señal al interpolarla con ceros, conocida como interpolación (L), para luego reducir la tasa de muestreo al aplicar un filtro pasa bajo y decimar, conocida como decimación (M), minimizando la introducción de aliasing. El uso de este bloque resulta importante convertir señales en diferentes dominios de frecuencia, como en transmisión y recepción de señales de radio donde las tasa de muestro tanto como en el transmisor y receptor pueden diferir.

Throttle

El bloque “Throttle”, se utiliza para controlar la tasa de procesamiento de flujo de datos, introduciendo retardos de manera controlada logrando una velocidad máxima de datos procesados por segundos, esencialmente en escenarios que está limitado por hardware, como en simulaciones o durante en desarrollo de procesamiento de señales, teniendo en cuenta que, sin este bloque, los flujos de datos pueden consumir toda la capacidad del CPU, causando sobrecarga del sistema.

Wbfmt transmit

El bloque “Wbfmt transmit”, se utiliza para implementar señales de radio FM de banda ancha, toma una señal de audio de entrada puede ser analógica o digital, luego

la modula en frecuencia para crear una señal FM de banda ancha para su transmisión, el proceso de modulación de la frecuencia consiste en variar la frecuencia de la portadora en función de amplitud, creando una señal para ser transmitida en un canal de radiofrecuencia. Además, el bloque incluye filtros y limitadores que ayudan a procesar la señal para la transmisión.

Wx gui FFT sink

Parámetros “Wx gui FFT sink”, permite la visualización del espectro de frecuencia de una señal mediante transformada rápida de Fourier, toma una señal de entrada y calcula su FFT, resultando una representación gráfica de distribución de la señal para la frecuencia, permitiendo a los usuarios observar aspectos importantes de una señal, como potencia espectral, frecuencias específicas y el comportamiento en frecuencia de modulaciones o filtrados, la visualización ayuda a identificar problemas de interferencias, ruido, y distorsión de la señal, también se puede ajustar parámetros de escala, rango de frecuencia, y estilo de visualización.

Osmocon sink

El bloque “Osmocon sink”, se utiliza para la transmisión de señales de radiofrecuencias (RF) por medio de dispositivos hardware compatibles con el bloque, como radios definidos por software (SDR) USRP, HackRF, BladeRF, y otros, el bloque actúa como una interfaz en los flujos de procesamiento de señales en GNU y el hardware SDR, permitiendo procesar las señales en el entorno de software para luego emitirla por el hardware.

Este bloque recibe muestra de señal digital o analógica procesada y las envía al dispositivo SDR, configurando elementos como frecuencia de transmisión, tasa de muestreo y ganancia de transmisión, resultando importante para implementación de sistemas de transmisión de radio, donde las señales moduladas se convierten en señales de radio logrando transmitir y recibirlas en otros dispositivos.

Low pass filter

El bloque “Low pass filter”, se utiliza para eliminar frecuencias altas de una señal, permitiendo el paso de frecuencias bajas dentro de un rango específico, este bloque resulta fundamental para el procesamiento de señales digitales, donde la eliminación de ruido y la extracción de información no deseada son importantes, el filtro pasa baja aplica una respuesta de frecuencia atenuando las frecuencias

superiores en el rango establecido permitiendo el paso de frecuencias inferiores sin demasiada atenuación, el filtro contiene parámetros de frecuencia de corte, frecuencia de transición y atenuación que determina el comportamiento del filtro.

Wx gui chooser

El bloque "Wx GUI Chooser ", proporciona menú despegable o botones de radio para seleccionar distintas configuraciones facilitando la modificación de los parámetros de la simulación sin necesidad de detener el proceso, es útil en procesamiento de señales, permitiendo al usuario elegir distintas frecuencias de operación o tipos de modulaciones a realizar, mediante una interfaz dinámica.

Noise Source

El bloque "Noise Source", se utiliza para generar señales de ruido que pueden ser añadidas a los flujos de datos o pruebas independientes, se puede producir diferentes tipos de ruido, tales como, ruido blanco gaussiano, ruido uniforme, entre otros, facilitando el análisis y el procesamiento de señales, permite a los usuarios especificar parámetros de amplitud del ruido y el tipo de distribución estadística, son esenciales en pruebas de algoritmos de cancelación de ruido y simulación de ambientes con señal ruidosa.

Wx gui waterfall sink

El bloque "Wx gui waterfall sink", se utiliza para visualizar el espectro de frecuencia de una señal en función del tiempo, su representación es en forma cascada (waterfall), mostrando como cambian los componentes de la frecuencia de una señal a lo largo del tiempo, este bloque resulta importante para análisis temporal - frecuencial, permitiendo visualizar variaciones y tendencia en la distribución de las frecuencias, genera una gráfica de eje horizontal representando la frecuencia y el eje vertical representando tiempo, los colores representa la magnitud de la frecuencia, si el color es intenso representa mayor potencia, este bloque resulta fundamental en aplicaciones de monitoreo de señales, detección de interferencias, identificación de señal modulada y vigilancia del espectro radioeléctrico.

Wx Fosphork sink

Bloque WX Fosphork Sink en GNU Radio es un instrumento o artificio avanzado de visualizar de manera instantáneo o en tiempo real, con el fin de lograr observar el espectro de señales. Este bloque emplea la biblioteca de procesamiento gráfico

Fosphork, que se basa en OpenGL para renderizar gráficos de alta velocidad, aprovechando el procesamiento paralelo de la GPU para lograr una visualización de espectro en tiempo real y con alta resolución.

3.3.5.5 Desarrollo de generador de ruido para redes WLAN de 2.4GHz

El presente trabajo, se describe el desarrollo de un generador de ruido configurado para que funcione en las bandas de 2.4GHz, ya que dicha banda es la más conocida en temas de redes WLAN. El propósito es implementar un generador de ruido para evaluar el desempeño y la resistencia de las redes inalámbricas antes de la interferencia y condiciones de ruido.

Se realizó el diseño y la configuración del generador de ruido empleando el software GNU Radio, este software tiene la particularidad de poder trabajar con tecnología SDR, además emplea una amplia gama de bloques de procedimientos de señales y componentes de visualización en tiempo real, GNU radio posee la flexibilidad y precisión en el ajuste de parámetros del generador permitiendo adaptar el ruido generado a las condiciones específicas de la banda de 2.4 GHz, por lo cual fue elegido el software para la realización del generador de ruido.

En esta sección, se explica los bloques y configuraciones utilizadas en GNU Radio para el desarrollo del generador de ruido, así cada componente del sistema se selecciona en función de sus capacidades para generar y visualizar señales de ruido en forma controlada, posibilitando la creación de un entorno de prueba representativa de las condiciones de interfaz de usuario en redes WLAN. Además, se describen las opciones de interfaz gráfica que permiten al usuario ajustar en tiempo real los parámetros como la frecuencia y la amplitud del ruido brindando así una optimización en el proceso de experimentación y análisis de resultados.

Una vez teniendo definido la elaboración del generador de ruido enfocado en las redes WLAN de 2.4GHz, donde se definió por medio de bloques de programación los canales a intervenir, en donde basta con elegir el canal a momento de ejecutar el código. El diagrama de bloque general del generador de ruido de WLAN de 2.4 GHz se muestra a continuación en la siguiente ilustración 130.

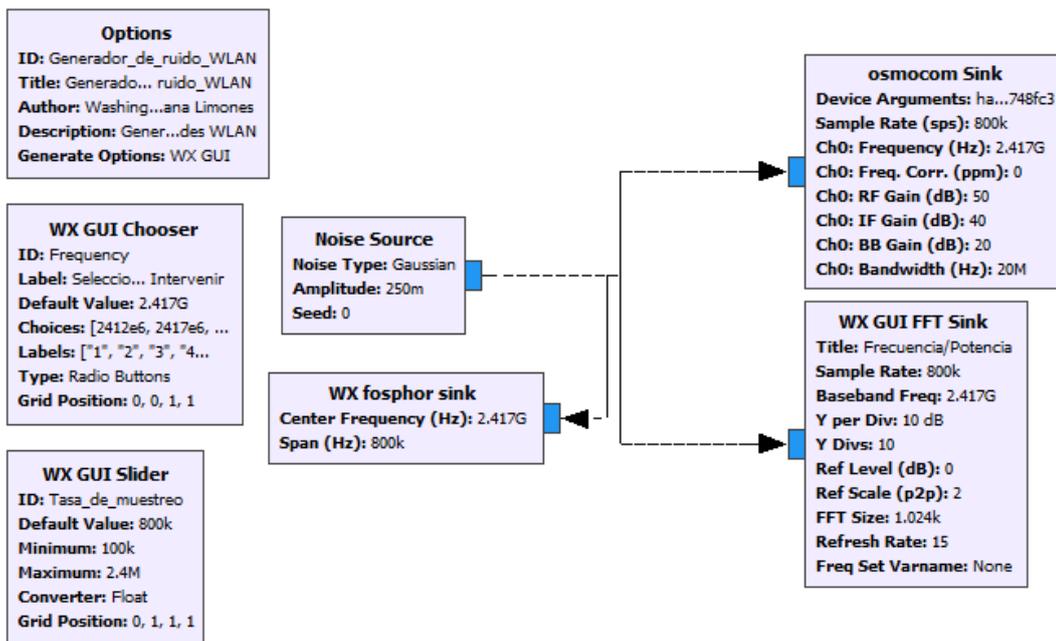


Ilustración 403. Diagrama de bloque del generador de ruido baso en redes WLAN de 2.4GHZ.

Fuente: Elaboración propia.

Para la descripción y configuración de los bloques utilizados se elaboró la siguiente guía, dónde se mencionarán los bloques necesarios y las configuraciones empleadas en cada de los bloques que conforma el diagrama:

1. Options: La utilización de este bloque fue asignar la ID que tendrá nuestros programas, el título que se presentará al momento de iniciar el programa conjunto al autor y la descripción del diagrama a crear y el archivo a crear, dicho dato mencionado se logra apreciar en la imagen que se muestra a continuación:



Ilustración 406. Configuración del bloque Options.

Fuente: Elaboración propia.

2. WX GUI slider: debemos asignarle un ID al bloque para tal caso se asignó el nombre de “Tasa_de_muestreo” cuyo valor de defecto el bloque se estableció en 800k, cuyos valores mínimos estarán definidas del siguiente rango 100k a 900k, el número de pasos para tomar es 100 finalmente, se asigna la posición que tendrá al momento de ejecutarse el programa, los datos mencionados previamente se pueden llegar a visualizar en la ilustración 132.

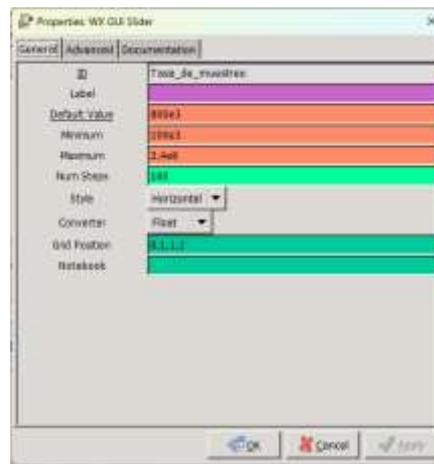


Ilustración 409. Configuración del bloque WX GUI Slider

. Fuente: Elaboración propia.

3. WX GUI Chooser: establecimos el ID del bloque como Frecuencia_objetivo, dentro del aparatado de label se definió como “Selecciones el canal de Frecuencia a Intervenir”, en este escenario el valor por defecto de la frecuencia estableció en 2.417GHz, de modo que el comenzar el programa se inicia en el canal 7, valores antes descritos, se realizó un listado de las frecuencias que se podrán analizar, para labels corresponden a los canales generados en las variables previa, y finalmente asignamos la posición que tendrá dentro de las ventanas en ejecución, los valores antes descrito se lograrán apreciar en la siguiente ilustración 133.

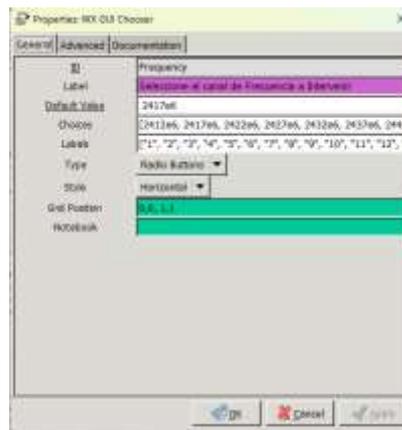


Ilustración 412. Configuración del bloque WX GUI Chooser

. Fuente: Elaboración propia.

4. Noise Source: en este caso, determinamos el tipo de ruido a producir un ruido gaussiano con una amplitud de 1, este valor puede variar en función de la frecuencia a tratar, como sugerencia se establece el valor de 1 de manera predeterminada, este valor influye en la superposición de los canales con un ancho de banda superior, para realizar un análisis más preciso dicho valor de la amplitud se debe cambiar por 0.45.

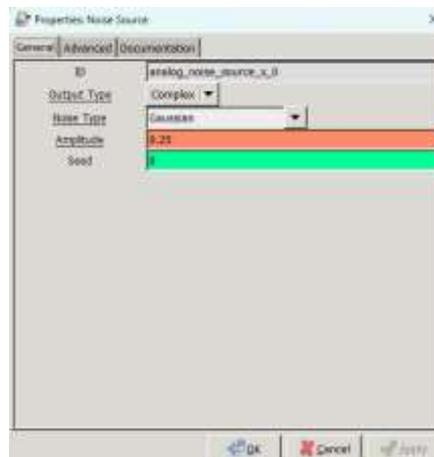


Ilustración 415. Configuración del bloque Noise Source.

. Fuente: Elaboración propia.

5. Wx Fosphork Sink: Se identifico el bloque con el ID fosphor_wx_sink_c_0, dicho bloque nos ayudara con la visualización del espectro de la red en tiempo real, se estable una frecuencia central para el análisis, y para final en la opción de spam (Hz) se especifica el ancho de banda para este se defino con la variable Tasa_de_muestreo.

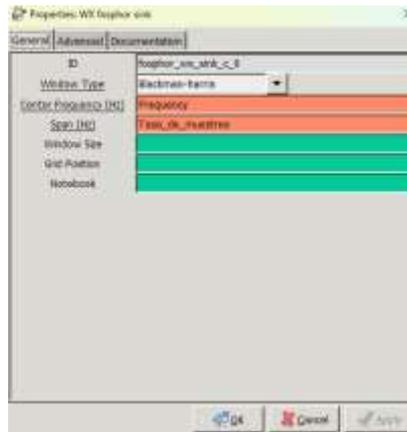


Ilustración 418. Configuración del bloque WX Fosphork Sink

Fuente: Elaboración propia.

6. Osmocon Sink: Identificamos el dispositivo con el que esperamos, determinamos la tasa de muestreo, la frecuencia a la que transmitirá con los valores de RF Gain, IF Gain, BBGain y el ancho de banda que dispondrá al inicio de la ejecución.

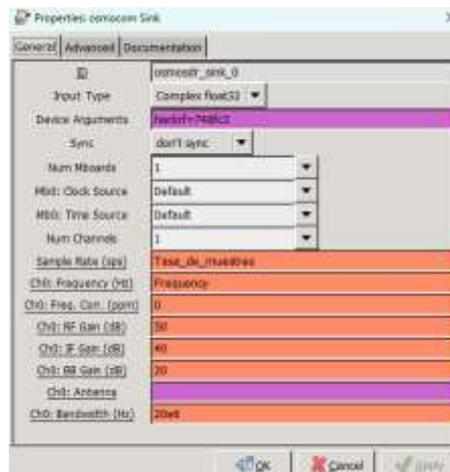


Ilustración 421. Configuración del bloque Osmocon Sink.

Fuente: Elaboración propia.

7. WX GUI FFT Sink: representación de la señal del ruido por medio de la transmisión, la transformada rápida de Fourier se utiliza para el dispositivo SDR, asignando la tabla de valores de ID, Título, tasa de muestreo, la frecuencia a graficar y los datos correspondientes a la FFT, tal como se ilustra en la ilustración 137.



Ilustración 424. Configuración del bloque WX GUI FFT Sink.

Fuente: Elaboración propia.

3.3.6 Propuesta de generador de ruido en 5GHz en GNU radio.

Dentro de la propuesta se presenta el diseño físico para la elaboración de un generador de ruido en frecuencia de 5GHz mediante el uso del software GNU radio, el objetivo en la realización del generador de ruido es crear una señal de interferencia controlada y amplificada con el fin de realizar pruebas en entornos de redes inalámbricas y estudios de susceptibilidad de dispositivo antes dichas interferencias generadas por el HackRF One.

Diseño del sistema

En la elaboración del diseño se basó en una arquitectura modular que permite el control preciso de la señal y ruido es una fácil adaptación a diversos medios entorno. En la ilustración 138 podemos observar el diseño físico de las conexiones entre el HackRF One y el amplificador así mismo de la manera cómo se conecta desde un computador o laptop, dichas conexiones explicarán a continuación:

- + **Conexión mediante USB:** el computador que ejecuta GNU Radio se conecta al HackRF One mediante un cable USB, inicia la conexión que permite a GNU Radio transmitir parámetros y configuraciones al HackRF One, GNU Radio proporciona una interfaz gráfica de usuario para la configuración de la señal de ruido facilitando el ajuste de los parámetros como frecuencia, ancho de banda y tipo de señal.
- + **HackRF One:** el equipo HackRF One funciona como emisor de la señal de ruido produciendo la señal en la banda de 5 GHz, al tener tecnología SDR, el HackRF One brinda una amplia adaptabilidad para generar diversos tipos

de señales lo que convierte en una herramienta versátil para aplicaciones de prueba, el uso de la frecuencia de 5 GHz puedes ajustarse a anchos de bandas variables permitiendo regular el alcance y el área de impacto de la señal de ruido.

- ✚ Amplificador EPUP: la señal generada por medio del HackRF One es enviada mediante el amplificar que previamente se encuentra conectado al HackRF One mediante conectores coaxiales, el amplificador se encarga de potenciar la señal lo que permite que el ruido abarque un área mayor o alcancen niveles de potencia mucho más alto lo cual permite intervenir en diferentes redes de 5GHz dichos parámetros son ajustados de acuerdo con las necesidades de cada prueba.
- ✚ Antena de 5GHz: finalmente la señal amplificada se propaga a través de una antena de 5GHz, es vital seleccionar la antena pues establece el patrón de radiación de la señal y puede ajustarse a sus aplicaciones específicas.



Ilustración 427. Esquema propuesto de conexiones física para el generador de ruido en 5Ghz.

Fuente: Elaboración propia.

Para metros tomar en cuando en el desarrollo del código en GNU radio:

- ✚ Creación de la señal ruido: Dentro del software de GNU Radio, se creará a través de bloques la señal ruido, el cual permite producir ruido blanco o también producir un espectro de ruido específico, además configurar la frecuencia de salida para la propuesta se estableció en 5GHz, mientras que el ancho de banda se establece en base al requerimiento de cada práctica.
- ✚ Configuración de parámetros: En las configuraciones nos enfocaremos en 3 partes importante dentro de la creación del programa, lo cuales son:

- Frecuencia: Se debe de tener especificado el tipo de frecuencia a usar para el programa se estableció en 5Ghz, una banda comúnmente utiliza por redes Wi-Fi y otros dispositivos IOT, lo cual facilita las pruebas de interferencia.
- Potencia de salida: La potencia de salida inicial se configura tanto en GNU Radio como también en el amplificador de 5GHz, lo que permite realizar pruebas con valores variado dentro de los niveles de potencia, con el fin de evaluar el comportamiento de los dispositivos bajos diversas condiciones de interferencia.
- Ancho de banda: El ancho de banda se ajusta dentro de GNU Radio en los bloques correspondiente, lo que permite generar un ruido d espectro capar de afectar una varia del rango de frecuencia de 5GHz, o bien un ruido configurado a la una frecuencia especifica.

Guía de uso y configuración de bloques

Se desarrollo una guía sobre el uso del generador de ruido en frecuencia de 5GHz y configuración de cada bloques y parámetros para tener en cuenta, el mismo cuenta con instrucciones específicas para la configuración de GNU Radio, HackRF One y el amplificador, consulte el siguiente enlace para obtener la guía: https://docs.google.com/document/d/1OPdO_itUJqaq-hCnNI5zLuggALZMhJjnKcjC7lsEVtQ/edit?usp=sharing

3.4 PRESUPUESTO

Para que la elaboración de la propuesta se ha considerado el siguiente presupuesto, el cual se detallará los equipos utilizados dentro de la implementación de la propuesta. Dentro de la planificación se destacan los costos directos del equipamiento utilizado dentro de la propuesta, proporcionando una perspectiva clara e integrar la inversión necesaria para ejecutar la implementación.

Tabla 18. Presupuesto para el desarrollo de la propuesta

Fuente: Elaboración propia.

TABLA DE VALORES		
DESCRIPCIÓN	CANTIDAD	PRECIO
Ubiquiti NanoStation Loco 5AC	2 Units	\$200
Cámaras Reolink RLC-510WA	2 Units	\$200
Reolink NVR Wi-Fi 4k	1 Units	\$200
Router Tenda Tx2 PRO-WIFI 6	1 Units	\$90
Transceiver TP-link MC111CS	2 Units	\$80
Fibra Drop	50 metros	\$35
Conector mecánico SC/APC	1 paquete	\$10
Cable UTP cat6	1 bobina	\$180
PoE Power	2 Units	\$100
Adaptador SMA a PSMA	1 Units	\$25
TOTAL		\$1120

De la misma manera, se contó con equipamiento existen en el laboratorio de telecomunicaciones los cuales se especificarán en la siguiente tabla:

Tabla 19. Recurso utilizado del laboratorio de telecomunicaciones.

Fuente: Elaboración propia.

EQUIPAMIENTO UTILIZADO DEL LABORATORIO
Ubiquiti LiteBeam 5AC Gen 2
Ubiquiti NanoStation
Ubiquiti NanoStation Loco M2
HackRF One
Monitor

CAPITULO IV

4 Análisis de resultado obtenidos.

Al finalizar las configuraciones de todos los escenarios planteado, se procedió a un análisis en profundidad de cada uno de ellos, teniendo en consideración un conjunto de características específicas de redes implementadas, así como los diversos códigos creados en diferentes entornos de software el análisis a realizar tiene como objetivo evaluar minuciosamente el comportamiento y rendimiento de acuerdo con cada uno de los escenarios experimentales planteado al comienzo de la realización de la propuesta.

Para obtener una comprensión más profunda y precisa de los resultados, se adoptó por utilizar una metodología que permita analizar los resultados de cada escenario de forma independiente, esto nos permitirá identificar de manera clara las características clave y las diferencias en el rendimiento de cada red, de acuerdo con los parámetros específicos propuesto en cada escenario.

En las siguientes secciones, se presentarán los resultados de cada análisis obtenido de la propuesta desarrolla.

4.1 Análisis de resultado obtenido del escenario

Una vez culminado con la implementación del escenario, se realizó un análisis a detalle del rendimiento de los dispositivos de la red y cámaras utilizadas en el sistema mediante pruebas específica de ancho de banda y calidad de vídeo dentro del escenario. Para ello, se examinaron hp las 2 antenas y la inalámbricas utilizada de modelo Loco m2 y NanoStation m2 con sus respectivas cámaras conectadas de forma inalámbricamente al sistema de videovigilancia.

4.1.1 Análisis de Rendimiento mediante Test de Ancho de Banda para el Dispositivo LOCO M2

Con el objetivo de evaluar el rendimiento de la antena LOCO M2, se llevó a cabo un test de ancho de banda, lo cual facilito evaluar la estabilidad y la capacidad de transmisión de la red inalámbrica generada por el dispositivo. La evaluación se ejecutó bajos condiciones contraladas, vinculando el sistema directamente con la red inalámbrica que proporciona la antena, los resultados proporcionados muestran una tasa de transmisión de datos de apropiadamente 50 a 70 Mbps, lo cual es

adecuado para una transmisión en la banda de 2.4 GHz, cumpliendo con las especificaciones del fabricante. Este desempeño indica que la antena LOCO M2 ofrece una transmisión apropiada para el tipo de datos requeridos en el sistema, la ilustración 144 muestra la estabilidad detectada en el enlace, dónde se ilustra el resultado del test realizado.



Ilustración 430. Análisis de ancho de banda mediante test de velocidad.

Fuente: Elaboración propia.

4.1.2 Análisis de Rendimiento mediante Test de Ancho de Banda para el Dispositivo NanoStation M2

De manera posterior, se evaluó el rendimiento de la antena NanoStation M2 instalada a una distancia aproximada de 60 metros, los resultados de la prueba de ancho de banda revelaron una tasa de transmisión inferior al registrado en el equipo LOCO M2 lo que podría deberse a la distancia y a las condiciones particulares del ambiente de transmisión inalámbrica. En la ilustración 145 muestra con la transmisión está por debajo de ser apropiada para que no exista interrupción en la transmisión de video.



Ilustración 433. Estudio de ancho de banda mediante tes de velocidad en la antena NanoStation M2.

Fuente: Elaboración propia.

4.1.3 Análisis de Transmisión de Video de la Cámara 1 (Conectada a LOCO M2)
Respecto a la cámara 1, que se encuentra vinculada de forma inalámbrica a la antena LOCO M2, se realizó un estudio sobre la transferencia de vídeo hacia el sistema NVR. Mediante los resultados obtenidos, fueron favorables observando una transmisión de vídeo fluida, sin distorsiones, o disminución de la calidad de imagen en tiempo real. Demostrando que la incorporación de la antena LOCO M2 fue la adecuada para el escenario, ya que dicha antena mantenía una transferencia adecuada lo que permitió obtener los resultados mencionados.

Los datos obtenidos corroboran que en la circunstancia preestablecida, la antena LOCO M2 es adecuado para el monitoreo de vídeos sin comprometer la integridad de la imagen, mediante la ilustración 146, podemos observar como la imagen de la transmisión de video se muestra sin interrupción.



Ilustración 436. Visualización de cámara 1 sin interrupción de transmisión.

Fuente: Elaboración propia.

4.1.4 Análisis de Transmisión de Video de la Cámara 2 (Conectada a NanoStation M2)

Posteriormente en la cámara 2, la cual se encuentra vinculada de manera inalámbrica a la antena NanoStation M2, demostró un comportamiento distinto al transmitir video a la NVR. En esta situación, se detectaron interrupciones en la señal con un retraso significativo y cerca del 30% de pixelación en la imagen, además descongelaciones ocasionales. Esta reducción en la calidad de transmisión se atribuye al medio de conexión que se encuentra conectado la cámara, la cual previamente ya presentaba problemas en la transmisión de datos debido a la instancia en la que se encuentra instalada la antena lo que afecta las posibilidades de pérdida y degradación de señal en la conexión inalámbrica.

Este resultado destaca la relevancia de la cercanía en las configuraciones de red inalámbrica para aplicaciones de vídeo en tiempo real, sugiriendo que la distancia y las posibles interferencias en el medio pueden afectar negativamente el rendimiento y la calidad de transmisión, en la siguiente ilustración 147, donde se muestra la imagen con pequeñas partes pixeladas.



Ilustración 439. Visualización de cámara 2 con interrupciones en la transmisión.

Fuente: Elaboración propia

4.1.5 Análisis e interpretación de datos obtenido mediante código de seguimiento de objetivos.

Al ejecutar el código, se obtuvo resultado para cada cámara evaluando la efectividad del sistema para detectar y medir distancias con precisión en entornos de monitoreo. El proceso de ejecución se realizó por separado garantizando una medición precisa y específica de acuerdo con las características del entorno y dispositivo.

Cámara 1

En la cámara 1, se obtuvo una detección clara y precisa de los objetivos presentes en el campo de visión, además el sistema fue capaz de identificar a cada persona y mostrar la distancia relativa a la cámara en tiempo real, lo cual puede mantener una actualización constante de los objetos detectados sin interrupción.

Los valores obtenidos visualizado en la ilustración 148, la distancia calculada por el programa es consistente y se encuentra en el rango esperado según la disposición espacial de los objetivos en el entorno, el programa cuenta con rango muy bajo de discrepancia de valor de distancia en relación con los valores recogido de

mediciones manuales, el porcentaje de margen de error se calcula entre los datos tomado del valor brindado por el programa y el valor de la medición manual.

$$\text{margen de error} = \frac{\text{Medicion programa} - \text{Medicion manual}}{\text{Medicion manual}} \times 100$$

$$\text{margen de error} = \frac{|14.16 - 13.50|}{13.50} \times 100$$

$$\text{margen de error} = \frac{0.66}{13.50} \times 100$$

$$\text{margen de error (\%)} = 4.89\%$$

El porcentaje obtenido del margen de error es muy bajo lo cual verifica el óptimo funcionamiento del código empleado, dicho datos se ven reflejado en la transmisión fluida de la cámara lo permitió que el cálculo de distancia se realizada sin interferencias.



Ilustración 442. Visualización de ejecución de código de seguimiento en tiempo real.

Fuente: Elaboración propia

Cámara 2

En la ejecución del código para la segunda cámara, mediante la recolección de datos de distancia, se pudo capturar la distancia de igual manera que en la detección anterior, pero con algunas diferencias en la estabilidad de la transmisión de datos debido a déficit que presenta la conexión inalámbrica donde se encuentra conectada.

La cámara fue capaz de identificar y medir distancia de los objetivos dentro del campo de visión; sin embargo, se identificó diferente variación al momento de la

presión de la distancia calculada debido a el retardo ocasional en la transmisión, los cuales quedan en evidencia en el margen de error.

$$\text{margen de error} = \frac{\text{Medicion programa} - \text{Medicion manual}}{\text{Medicion manual}} \times 100$$

$$\text{margen de error} = \frac{|13.01 - 18.55|}{18.55} \times 100$$

$$\text{margen de error} = \frac{5.54}{18.55} \times 100$$

$$\text{margen de error (\%)} = 30\%$$

El porcentaje obtenido es considerable lo cual solo demuestra cómo está afectando la conectividad con la detección de objetos, los retardos ocurridos afectada de manera directa en la actualización de distancia en tiempo real, especialmente si el objeto se encuentra a una ubicación lejana a la cámara.



Ilustración 445. Ejecución del código de seguimiento en tiempo real en la cámara 2.

Fuente: Elaboración propia

4.1.6 Análisis e interpretación al utilizar un generador de ruido para redes WLAN 2.4GHZ.

El SDR es un dispositivo fundamental en este estudio debido que recibe y emite señales en el espectro de frecuencia, por lo que permitió analizar y modificar las ondas de radio, para lograr medir la resistencia de la red WLAN evaluada, este dispositivo tiene una adaptabilidad ya que puede abarcar un rango extenso de frecuencias, además, la programación permite tener un control detallado de los parámetros en tiempo real. El análisis del generador de ruido en redes WLAN en 2.4 GHz, su objetivo principal es simular entornos complejos dentro de las redes

inalámbricas en el rango de esta frecuencia, con esto se logra generar señales de ruido que emiten interferencias.

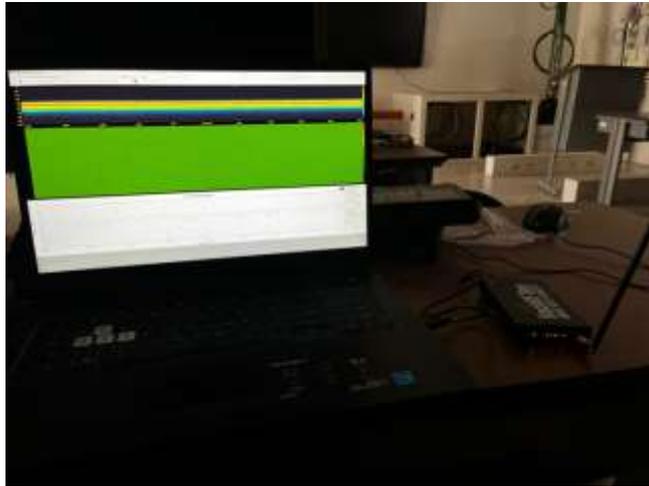


Ilustración 448. Ejecución de generador de ruido optimizado a antena emisora de cámara 1.

Fuente: Elaboración propia

Esto permitirá capturar datos de la densidad espectral de potencia dentro del rango determinado de frecuencias, además el dispositivo utiliza una técnica avanzada denominada la transformada rápida de Fourier (FFT), con el fin de poder visualizar picos y las diferentes formas de onda, una vez emitida la señal de ruido se neutraliza la señal emitida del dispositivo Loco M2, ya una vez efectuado el ruido se corta la transmisión de la señal interrumpiéndola en un intervalo de 1 a 2 minutos lo que no permite la comunicación directa con el NVR, así tal como se muestra en la ilustración 151.

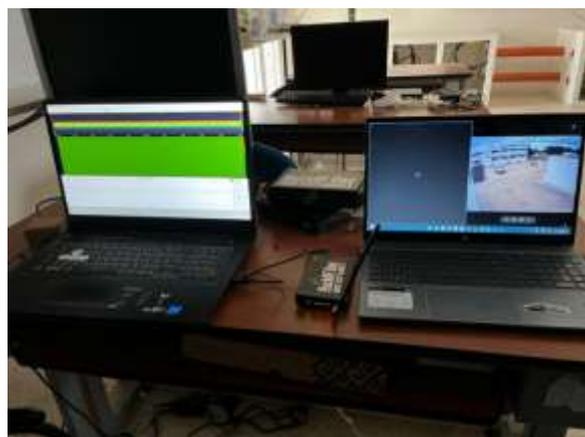


Ilustración 451. Verificación de intervención efectiva en la red.

Fuente: Elaboración propia

Como se puede observar en la ilustración que al estar en funcionamiento del HackRF One generando el ruido, la señal transmitida ha provocado que la señal se pierda, por lo tanto, hay pérdida de paquetes de datos, lo que es perjudicial para un sistema de videovigilancia, además se observa la otra cámara esta activa ya que está trabajando con la frecuencia de 5 GHz, esto es posible ya que el sistema de video vigilancia trabaja en dos bandas de frecuencia, con esto se busca que la comunicación sea constante y de buena calidad para de esta manera garantizar que no haya pérdida de paquetes de datos. Una vez que ya no exista ruido la señal vuelve y muestra la imagen de la cámara de seguridad, recalcando que las cámaras son de doble banda, buscaremos el mejor método para poder transmitir el audio y video.

4.2 Análisis de resultado obtenido del escenario 2.

En el segundo escenario de radio enlace punto a multipunto, se evaluó el rendimiento de la red, en las antenas emisora y receptoras, además la calidad de transmisión en cada cámara conectada al sistema de radio enlace. En las antenas receptoras se incluyó un router independiente logrando un enlace dedicado para mejorar la conectividad de las cámaras. Los resultados a obtener se realizan en base a pruebas de velocidades y calidad de transmisión de video.

4.2.1 Análisis de rendimiento de la antena emisora LiteBeam 5AC

El análisis se realizó mediante la ejecución de test de velocidad a la antena emisor permitiendo evaluar la capacidad de transmisión en un radio enlace punto a multipunto, dicho test dio como resultado tasas de transferencia de datos de 100 a 200 Mbps, los valores obtenidos de transmisión de datos son los adecuados para poder mantener una transmisión de datos de alta velocidad. Los resultados emitido antena LiteBeam 5AC nos brindas múltiples conexiones de alta calidad, lo cual es necesario para el uso de sistema para la transmisión de vídeo en tiempo real. Mediante la interfaz de la antena tienes la particular de poder visualizar la capacidad de transmisión de la antena en el enlace realizado, lo cual se muestra en la ilustración 152.



Ilustración 454. Rendimiento de transmisión de antena emisora.

Fuente: Elaboración propia

4.2.2 Análisis de Rendimiento de la antena receptora 1 Loco 5AC

Como se indicó anteriormente para la antena receptora se instaló un router adicional, proporcionando un enlace dedicado, en la prueba de velocidad se obtuvo la tasa de transferencia de 100 a 150 Mbps, garantizando la transmisión de video estable y de alta calidad hacia el NVR, sin tener pérdidas ni interrupciones. La antena receptora 1 junto a su rock del asociado, demuestra ser una solución eficaz en un radio enlace multipunto asegurando una conectividad fiable y una reproducción de video fluida.

De igual manera se utilizó la misma interfaz de antena para verificar la tasa de transmisión de la primera antena receptora, los datos se corroboran en la ilustración 153.



Ilustración 457. Rendimiento de tasa de transmisión de la primera antena receptora.

Fuente: Elaboración propia

4.2.3 Análisis de Rendimiento de la antena receptora 2 Loco 5AC

Para evaluar el rendimiento de la antena receptora 2 de modelo LOCO 5AC y la calidad de transmisión de video, se empleó un router independientemente de la misma red para la cámara 2, el test de velocidad realizado en esta configuración mostró una tasa de transferencia entre 100 y 150 Mbps, como lo muestra en la ilustración 154. El rendimiento que presenta la red es óptimo para soportar la transmisión continua de datos de video en excelentes calidades.

La estabilidad y capacidad de transmisión correspondiente a la antena receptora 2 conjunto a su router asociado, lo cual proporciona una efectividad del sistema multipunto en entornos alejados se requieran de fiabilidad de transmisión y altas velocidades.



Ilustración 460. Rendimiento de tasa de transmisión de la segunda antena receptora.

Fuente: Elaboración propia

4.2.4 Análisis de Rendimiento y calidad de transmisión de video de la Cámara 1
Continuando con el análisis en la cámara 1, que se encuentra conectada de forma inalámbrica al router asociado en antena receptora a 1, dicha cámara demostró tener una transmisión de vídeo de alta calidad. Durante las pruebas, no hubo pérdidas de paquetes ni interrupciones lo que indica una alta estabilidad en la transmisión de vídeo, la calidad de la imagen se mantuvo estable y sin irregularidades, por ello se atribuye a la a una alta capacidad de transmisión superior a 100 megas que ofrece la red puesta en marcha con la antena LOCO 5AC y el router de igual capacidad.

Estos hallazgos corroboran que la cámara 1 tiene la capacidad de funcionar de manera eficiente en el escenario punto a multipunto proporcionando una visualización en tiempo real de excelente calidad, mediante la ilustración 155 podemos visualizar que la imagen recibida del NVR es nítida, sin interrupciones.



Ilustración 463. Visualización de cámara 1 desde el NVR mediante el radio enlace PTM.

Fuente: Elaboración propia

4.2.5 Análisis de Rendimiento y calidad de transmisión de video de la Cámara 2
Respecto a la cámara 2, que de igual manera se encuentra vinculada de forma inalámbrica al router de la antena receptora 2, se experimentó un incremento considerable en la calidad de transmisión de vídeo en comparación con el escenario anterior. Dado a la estabilidad del enlace y a una velocidad de transmisión superior a los 100 Mbps que dispone la antena receptora y el router. La cámara registró una transmisión fluida, sin pérdida de paquetes y manteniendo una calidad de imagen estable.

La configuración de la antena receptora 2 con un router exclusivo para la cámara ayudó a asegurar la conexión de excelente calidad, solucionando inconvenientes de retraso o pixelación y asegurando una visualización en tiempo real viable. El resultado recolectado del optimo funcionamiento de la segunda cámara se muestran en la ilustración 156.



Ilustración 466. Visualización de cámara 1 correspondiente al segundo escenario analizado

Fuente: Elaboración propia.

4.2.6 Análisis e interpretación de datos obtenido al ejecutar código de seguimiento de objetivos en tiempo real para frecuencia de 5GHZ

Con el propósito de evaluar el rendimiento del sistema de cálculo de distancia de objetos en tiempo real en un contexto de radioenlace punto a multipunto en la banda de 5 GHz, se ejecute el programa de forma individual como en el escenario anterior. para este análisis cada cámara está vinculada de forma inalámbrica a un router autónomo vinculada a su correspondiente antena receptora lo cual facilita una conexión exclusiva para cada cámara mejorando así la estabilidad y calidad de la transmisión, este análisis se realizó con el objetivo de examinar el efecto de la banda 5 GHz y la infraestructura de una red en la precisión y estabilidad de la detección de objetos y calcula la distancia en tiempo real.

Cámara 1

al momento de la ejecución del código en la primera cámara evidenció una mejora significativa en la estabilidad y precisión de los cálculos de distancia, el enlace de la cámara con el router dedicado de la antena receptora, sumando a la utilización de la banda de 5GHz caracterizada por su menor interferencia y mayor capacidad de transmisión, posibilitó una identificación exacta de los objetos dentro del área de visión de la misma cámara. En este caso, el sistema detectó varios objetos, incluyendo vehículos y personas, teniendo cálculos de alta precisión dado que el vehículo más próximo registra una distancia de 5.30 metros y mientras que la persona situada a la distancia más grande se registra de 14.14 metros, dichos datos son visualizado en la ilustración 157.

Para obtener un margen de error y verificar si está calculando de manera exacta el programa, se realizara el siguiente calculo tomando la distancia más alejada para mayor comparación.

$$\text{margen de error} = \frac{\text{Medicion programa} - \text{Medicion manual}}{\text{Medicion manual}} \times 100$$

$$\text{margen de error} = \frac{|14.14 - 13.35|}{13.10} \times 100$$

$$\text{margen de error} = \frac{0.79}{13.10} \times 100$$

$$\text{margen de error (\%)} = 5.92\%$$

El porcentaje de error se elevó un poco comparado con el margen obtenido en el escenario anterior con la misma cámara, aunque el porcentaje no es tan elevado cabe recalcar la posibilidad de modificar el parámetro de altura dentro del código para disminuir el porcentaje de error y ser más exacto en el cálculo.

Mediante la conexión en la banda 5 GHz demostró una transmisión sin pérdida de paquetes de vídeo y sin interrupciones, mejorar dichos parámetros facilitó la precisión en los cálculos de distancia lo cual quedo evidenciando en el cálculo realizo previamente



Ilustración 469. Visualización de ejecución del código de seguimiento en la banda de 5GHZ.

Fuente: Elaboración propia.

Cámara 2

De igual manera que en la anterior cámara, se ejecutó el código donde arrojo resultados similares a los obtenidos en la cámara 1, mostrando un cálculo óptimo al momento de medir las distancias de los objetos, en la imagen capturada el sistema detectó y midió la distancia de varios objetos, entre ellos vehículos y personas documentando distancia de 13.04 metros para un vehículo y de 9.48 m para una persona en el área monitorizada.

Para obtener el margen de error en la distancia entre lo obtenido por el programa y los datos obtenidos de manera física, se emplea el siguiente cálculo con el dato de distancia más lejano obtenido del programa.

$$\text{margen de error} = \frac{\text{Medicion programa} - \text{Medicion manual}}{\text{Medicion manual}} \times 100$$

$$\text{margen de error} = \frac{|13.04 - 12.55|}{12.55} \times 100$$

$$\text{margen de error} = \frac{0.49}{12.55} \times 100$$

$$\text{margen de error (\%)} = 3.91\%$$

El porcentaje de error ha disminuido considerablemente, comprando con el porcentaje obtenido en el primer escenario en la misma ubicación, lo cual pone en evidencia la mejoría en la transmisión de vídeo que obtuvo al aplicar una frecuencia de 5 GHz, la baja interferencia y la capacidad de transmisión de la banda de 5 y

junto con el router garantizó una conexión estable y precisa en la transmisión de vídeo de la segunda cámara



Ilustración 472. Visualización de ejecución del código de seguimiento en la banda de 5GHZ.

Fuente: Elaboración propia.

4.3 Análisis de resultado obtenido del escenario 3.

Culminando el análisis de los escenarios planteado, el ultimo escenario propuesto se enfoca en la evaluación de cinco parámetros esencial para medir el rendimiento de las mayores transacciones conectado directamente al NVR y a las cámaras. El presente análisis permitirá determinar la eficiencia de cada medio y comparar uno al otro para comparar cuál medio tienes mejor transmisión en un sistema de videovigilancia, así poder identificar cuál medio puede satisfacer los requerimientos de calidad y estabilidad de transmisión de datos en tiempo real.

4.3.1 Análisis e interpretación de datos obtenido mediante el medio de transmisión wireless

El análisis por el medio de transmisión inalámbrico (wireless) se segmento en dos parámetros para su posterior análisis, los parámetros fueron la frecuencia de operación centrándose en las dos bandas más utilizadas y comúnmente empleada en dispositivos IOT: 2,4GHz y 5GHz. Estas bandas fueron analizadas con el objetivo de determinar su rendimiento y capacidad para satisfacer los requisitos que presenta un sistema de videovigilancia, cada banda será analizada en base a los protocolos de compresión de video H.264 y H.265.

4.3.3.1 Análisis de latencia y retardo

Transmisión inalámbrica en 2.4GHz

El primer parámetro, es evaluar la latencia y retardo el cual podemos realizar el análisis mediante la captura de paquetes en wireless, el cual debemos de filtrar la

información a los paquetes que deseamos analizar, como se explicó en la guía realizar en los puntos anteriores, en ellos debemos ser énfasis al primer paquete que detectemos que este transmitiendo datos entre los dispositivos, el número de paquete que se detectó conexión entre ambos en la transmisión de video, fue el paquete identificado con el número 248, el cual tienes un tiempo de 1.443 segundo este valor representa el inicio de la transmisión. (véase ilustración 159)

No.	Time	Source	Destination	Protocol	Length	Info
248	0.324817	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011800 Win=1824 Len=0
249	0.3008300	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011790 Win=1824 Len=0
250	0.3008387	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011810 Win=1824 Len=0
251	0.3008423	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011820 Win=1824 Len=0
252	0.3008457	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011830 Win=1824 Len=0
253	0.3008491	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011840 Win=1824 Len=0
254	0.3008525	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011850 Win=1824 Len=0
255	0.3008559	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011860 Win=1824 Len=0
256	0.3008593	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011870 Win=1824 Len=0
257	0.3008627	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011880 Win=1824 Len=0
258	0.3008661	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011890 Win=1824 Len=0
259	0.3008695	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011900 Win=1824 Len=0
260	0.3008729	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011910 Win=1824 Len=0
261	0.3008763	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011920 Win=1824 Len=0
262	0.3008797	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011930 Win=1824 Len=0
263	0.3008831	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011940 Win=1824 Len=0
264	0.3008865	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011950 Win=1824 Len=0
265	0.3008899	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011960 Win=1824 Len=0
266	0.3008933	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011970 Win=1824 Len=0
267	0.3008967	192.168.1.42	192.168.1.43	TCP	64	55113 → 5000 [ACK] Seq=164011980 Win=1824 Len=0

Ilustración 475. Captura de paquete mediante wireshark para banda de 2.4GHz

Fuente: Elaboración propia.

De igual manera debemos de identificar el paquete de respuesta entre los dispositivos para ellos se debe utilizar el filtro, pero modificando las IP. El paquete de respuesta queda identificado 250, el cual tiene un tiempo de 1.457 considero el tiempo del paquete para calcular la latencia del paquete. Para calcular el valor de latencia se empleó la siguiente formula.

$$latencia = tiempo\ de\ respuesta\ del\ paquete - tiempo\ de\ paquete\ inicial$$

$$latencia = 1.457 - 1.443$$

$$latencia = 0.014s = 14ms$$

El valor obtenido de latencia en el medio de transmisión wireless en frecuencia de 2.4GHz es un valor aceptable para la banda transmitida, para obtener un porcentaje de latencia más exacta se debe de tomar más paquetes y realizar el mismo análisis y calcular el promedio mediante una suma del resultado obtenido y dividirlo por el número de datos (Promedio de latencia = Suma de todas las latencias obtenidas / número de mediciones).

El mismo análisis se realizó para el estándar de compresión H.265, dicho cambio se empleó en la cámara y en el NVR, se realiza un nuevo proceso de captura de

paquete que corresponda al estándar, el cual de igual manera se identificó el primer paquete enviado el cual fue identificado como número 524, con un tiempo de espera de 2.513 como se muestra en la ilustración 160.

No.	Time	Source	Destination	Protocol	Length	Info
407	2.348257	192.168.1.42	192.168.1.43	TCP	54	54832 → 9000 [ACK] Seq=1. Ack=278725 Win=1818 Len=0
408	2.359187	192.168.1.42	192.168.1.43	TCP	54	54832 → 9000 [ACK] Seq=1. Ack=273294 Win=1818 Len=0
409	2.370221	192.168.1.42	192.168.1.43	TCP	54	54832 → 9000 [ACK] Seq=1. Ack=273394 Win=1818 Len=0
482	2.421218	192.168.1.42	192.168.1.43	TCP	54	54832 → 9000 [ACK] Seq=1. Ack=274811 Win=1818 Len=0
507	2.440208	192.168.1.42	192.168.1.43	TCP	54	54832 → 9000 [ACK] Seq=1. Ack=278295 Win=1818 Len=0
589	2.459085	192.168.1.42	192.168.1.43	TCP	54	54832 → 9000 [ACK] Seq=1. Ack=278794 Win=1818 Len=0
514	2.479085	192.168.1.42	192.168.1.43	TCP	54	54832 → 9000 [ACK] Seq=1. Ack=288454 Win=1818 Len=0
518	2.481289	192.168.1.42	192.168.1.43	TCP	54	54832 → 9000 [ACK] Seq=1. Ack=282141 Win=1818 Len=0
524	2.513221	192.168.1.42	192.168.1.43	TCP	54	54832 → 9000 [ACK] Seq=25. Ack=288454 Win=1818 Len=0
530	2.558158	192.168.1.42	192.168.1.43	TCP	54	54832 → 9000 [ACK] Seq=25. Ack=288188 Win=1818 Len=0
523	2.562239	192.168.1.42	192.168.1.43	TCP	54	54832 → 9000 [ACK] Seq=25. Ack=288454 Win=1818 Len=0
537	2.570274	192.168.1.42	192.168.1.43	TCP	54	54832 → 9000 [ACK] Seq=25. Ack=288736 Win=1818 Len=0
547	2.630356	192.168.1.42	192.168.1.43	TCP	54	54832 → 9000 [ACK] Seq=25. Ack=291398 Win=1818 Len=0

Ilustración 478. Captura de paquete mediante wireshark para banda de 2.4GHz en estándar H.265

Fuente: Elaboración propia.

Antes de realizar cálculo de la latencia debemos de identificar el paquete de respuesta, para ellos seguir lo realizado en la captura de paquetes en estándar H.264, el paquete previo identificado con numero de 526, el cual tienes un tiempo de 2.520 este valor será importante para el cálculo de la perdida de latencia, se aplica la misma formulará para obtener dicho valor.

$$latencia = 2.520 - 2.513$$

$$latencia = 0.007s = 7ms$$

El valor obtenido de perdida de latencia es significativamente más bajo que el obtenido mediante H.264, el cual muestra que a la aplicación el estándar de compresión H.265 disminuye el tiempo la respuesta de la transmisión.

Transmisión inalámbrica en 5GHz

Una vez obtenido el análisis correspondiente en la banda 2.4Ghz, se realizará el mismo análisis para la banda de 5GHz con el fin de realizar comparación entre ambas bandas dentro del aparatado de tiempo de latencia.

Siguiendo con la guía realizada previamente, se escoge el primer paquete de envío entres el NVR y la cámara dicho paquete llevo fue identificado con numero 921 para posteriormente ser analizado, el dato obtenido del paquete es el tiempo de envío el cual es de 5.110, el valor ser crucial para el cálculo de perdida de latencia, tanto el número de paquete, el tiempo y otros datos son verificado en la ilustración 161.

No.	Time	Source	Destination	Protocol	Length	Info
832	4.558249	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=384375 Win=2853 Len=0
837	4.558341	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=387277 Win=2853 Len=0
838	4.578226	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=388651 Win=2853 Len=0
839	4.722198	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=399923 Win=2848 Len=0
840	4.744744	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=392049 Win=2853 Len=0
849	4.762537	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=394528 Win=2853 Len=0
878	4.798174	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=396905 Win=2853 Len=0
888	4.848308	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=397955 Win=2858 Len=0
894	4.880030	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=399955 Win=2853 Len=0
898	4.880380	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=401831 Win=2853 Len=0
897	4.884881	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=402181 Win=2851 Len=0
891	4.898986	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=404809 Win=2853 Len=0
893	4.900531	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=406993 Win=2853 Len=0
922	5.851207	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=408019 Win=2853 Len=0
928	5.881283	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=411561 Win=2853 Len=0
928	5.88896	192.168.1.42	192.168.1.43	TCP	54	55133 → 9000 [ACK] Seq=25 Ack=412821 Win=2852 Len=0

Ilustración 481. Captura de paquete mediante wireshark para banda de 5GHz en estándar H.264.

Fuente: Elaboración propia.

De igual manera se identificó el primer paquete de respuesta entre los dispositivos, el cual también se identificó con número de paquete 922, el cual necesitaremos el valor del tiempo de respuesta dicho valor es de 5.119. Una vez teniendo dichos valores podemos proceder al cálculo de la latencia.

$$latencia = 5.119 - 5.110$$

$$latencia = 0.009s = 9ms$$

El resultado obtenido es el apropiado para la banda de 5GHz ya que tener una mayor tasa de transmisión, permite menos tiempo de latencia como lo muestra el cálculo realizado.

De igual manera se debe realizar el mismo análisis dentro de la banda de 5GHz, pero cambiando en el estándar de compresión H.264 por el H.265, teniendo en

No.	Time	Source	Destination	Protocol	Length	Info
529	2.764837	192.168.1.42	192.168.1.43	TCP	54	55881 → 9000 [ACK] Seq=1 Ack=426689 Win=1026 Len=0
536	2.824353	192.168.1.42	192.168.1.43	TCP	54	55881 → 9000 [ACK] Seq=1 Ack=427272 Win=1025 Len=0
548	2.834243	192.168.1.42	192.168.1.43	TCP	54	55881 → 9000 [ACK] Seq=1 Ack=429198 Win=1026 Len=0
548	2.864152	192.168.1.42	192.168.1.43	TCP	54	55881 → 9000 [ACK] Seq=1 Ack=431985 Win=1026 Len=0
557	2.920181	192.168.1.42	192.168.1.43	TCP	54	55881 → 9000 [ACK] Seq=1 Ack=433866 Win=1022 Len=0
561	2.934578	192.168.1.42	192.168.1.43	TCP	54	55881 → 9000 [ACK] Seq=1 Ack=434884 Win=1026 Len=0
565	2.963885	192.168.1.42	192.168.1.43	TCP	54	55881 → 9000 [ACK] Seq=1 Ack=437459 Win=1026 Len=0
571	3.016447	192.168.1.42	192.168.1.43	TCP	54	55881 → 9000 [ACK] Seq=1 Ack=438459 Win=1022 Len=0
574	3.032268	192.168.1.42	192.168.1.43	TCP	76	55881 → 9000 [PSH, ACK] Seq=1 Ack=438876 Win=1021 Len=24

Ilustración 484. Captura de paquete mediante wireshark para banda de 5GHz en estándar H.265.

Fuente: Elaboración propia.

Ilustración 485. Captura de paquete mediante wireshark para banda de 5GHz en estándar H.265.

Fuente: Elaboración propia.

cuenta lo mencionado se realiza un nuevo análisis de paquetes para obtener la información con el nuevo estándar, el número de paquete escogido fue el 574 el cual obtenemos el tiempo de respuesta del paquete valla tiempo es de 3.032, datos mencionados se visualizan en la ilustración 162.

Una vez teniendo el primer valor de envío debemos de identificar el primer paquete de repuesta ya que este tiene el otro valor del tiempo que necesitamos para calcular la latencia, dicho número de paquetes es el 575 teniendo el valor de tiempo del paquete es 3.034, a continuación, se calcula el valor de latencia.

$$latencia = 3.034 - 3.032$$

$$latencia = 0.002s = 2ms$$

El valor de latencia obtenida se adecuado para el medio de transmisión con junto con el estándar, así dando que la perdida de latencia sea mínima en un entorno controlado.

Con el fin de tener un panorama más claro de los valores obtenido mediante el análisis, se desarrolló una pequeña tabla 20, donde podemos comprar los valores óptimos en cada estándar correspondiente a su banda de frecuencia.

Tabla 20. Valores de latencia y retardo.

Fuente: Elaboración

Valores de latencia y retardo		
Bandas analizadas	Estándar H.264	Estándar H.265
Banda de 2,4GHz	14ms	7ms
Banda de 5GHz	9ms	2ms

obtenidos de cálculo

propia.

Los datos obtenidos muestran como en la banda de 5GHz el tiempo de latencia y retardo es menor en ambos estándares a comparación con el tiempo que toma en la banda 2,4GHz, aunque en el estándar H.265 mostro un valor bajo, dicho valor comparando con el que se obtuvo en 5GHZ es todavía menor que el mismo.

4.3.3.2 Análisis del ancho de banda

En el análisis realizado para determinar el ancho de banda, se empleó la guía realizara y siguiente el mismo procedimiento para ambas bandas de frecuencia y sus correspondiente estándar de compresión. Los mismos archivos de captura de paquete en wireshark utilizados para el cálculo de latencia fueron empleados para el análisis de ancho de banda, los datos obtenidos se muestran en la siguiente tabla 21 donde se mostrarán los picos más alto alcanzado por cada banda.

Tabla 21. Valor obtenido del análisis de ancho de banda mediante wireshark.

Fuente: Elaboración propia.

Valores de ancho de banda		
Bandas analizadas	Estándar H.264	Estándar H.265
Banda de 2,4GHz	2,25 Mb	5 Mb
Banda de 5GHz	2,25 Mb	2,2 Mb

Mediante los datos obtenidos, en la banda 2.4GHz el consumo mayor ancho de banda en el estándar H.265. ya que al ofrecer mejor compresión que el H.264 el ancho de banda debe de ser menor su consumo, llegando al análisis que la banda 2.4GHz realizada en esta propuesta no es ideal para trabajar con el estándar de H.265, debido a cogestión o interferencia lo cual son factores que dificulta el aprovechamiento total de la compresión H.265 en esta banda.

Dentro de la banda de 5GHz, el estándar de compresión H.265 requiere un ancho de banda de 2,2 Mb lo que ligeramente es menor a ancho de banda del estándar H.264, la banda de 5Ghz es ideal para trabajar en transmisión de H.265, el mismo permite una reducción efectiva en el ancho de banda requerido sin comprometer la calidad de video en la transmisión.

4.3.3.3 Análisis de calidad de video en base a parámetros PSNR y SSIM

En el análisis correspondiente a la calidad de video, se empleó la guía realiza previamente, aplicando el mismo procedimiento en el análisis para ambas de frecuencia, una vez grabado el video en ambos estándares, debe de considerar como parámetros esenciales que cada grabación debe de tener la misma duración y el mismo campo visual así garantiza una compresión de vídeo óptima y permite una comparación equitativa de los resultados.

Mediante el símbolo del sistema y realizado la compresión nos arrojó lo siguiente datos de PSNR:

 PSNR y = 25.84 dB

 PSNR Avg= 27.49 dB

 PSNR u = 38.23 dB

 PSNR min = 26.01 dB

 PSNR v = 38.96 dB

 PSNR Max = 29.15 dB

Los valores que destacar del análisis psnr y el cual nos dios un poco bajo por el valor requerido de 30 dB lo cual se considera como perdida en calidad de la luminancia de la compresión, otro valor es psnr Avg el cual también se encuentra por debajo de los 30 dB el cual no se encuentra tan por debajo del requerido, es aceptable en la compresión.

Los valores obtenidos para SSIM son lo siguiente:

$$\text{SSIM}_y = 0.88$$

$$\text{SSIM}_v = 0.98$$

$$\text{SSIM}_u = 0.98$$

$$\text{SSIM}_{All} = 0.91$$

De igual manera se toma en consideración dos valores el primero ssim el cual según la condición planeada en la guía es considerablemente buena compartiendo similitudes con la luminancia entre el video H.265 y el H.264, aunque hay pequeñas perdidas de luminancia, el segundo valore es ssim All el cual tiene un nivel de aceptación alto en base al rango considerado perfecto lo muestra una excelente compresión de video en H.265 durante la mayor parte del video.

Transmisión inalámbrica en 5GHz

En la banda de 5GHz se realizó el mismo análisis, utilizando el mismo procedimiento que se realizaron en la banda de 2.4GHz.

Valores obtenidos de SSIM:

$$\text{PSNR}_y = 25.92 \text{ dB}$$

$$\text{PSNR}_{Avg} = 27.63 \text{ dB}$$

$$\text{PSNR}_u = 41.57 \text{ dB}$$

$$\text{PSNR}_{min} = 25.90 \text{ dB}$$

$$\text{PSNR}_v = 39.94 \text{ dB}$$

$$\text{PSNR}_{Max} = 29.57 \text{ dB}$$

Dentro de lo valores PSNR tenemos dos datos importantes, el primero valor resultado de psnr nos evalúa la luminancia en tanto valor obtenido determina una similitud de luminancia alta pero así cuenta con perdida en instancia de la compresión, el otro valor a considerar psnr Avg, se encarga de obtener un promedio en lapso de duración del video comprimido, el resultado se considera aceptable con ciertas perdidas visuales.

Valores obtenidos para SSIM:

SSIM $y = 0.89$

SSIM $v = 0.99$

SSIM $u = 0.99$

SSIM All = 0.3

Como en el caso anterior se encuentra dos valores en tomar en cuenta para determinar si cumple con las condiciones de SSIM, el primero valor es de ssim y , nos brinda un valor considerado aceptable, el mismo se puede mejorar ligeramente para tener una similitud total con el video H.264, el ultimo valor son los otorgado por ssim All, el mismo indica una alta calidad de similitud del video comprimido y el video H.264 es aceptable el video logro conservar una calidad visual aceptable

4.3.3.4 Análisis de la estabilidad de transmisión.

El análisis en base a la estabilidad de transmisión, como en análisis anterior se empleará la guía previamente realizada la cual lo permite aprovechar los paquetes capturados por medio de wireshark y proceder con el análisis de la estabilidad, para ellos se realizó una tabla comparativa de datos óptimos tanto físico como en wireshark, el cual tenemos más legibilidad en los datos obtenido tanto para ambas bandas analizadas como en los respectivos estándares de compresión. (véase tabla 22)

Tabla 22. Valores obtenidos para análisis de estabilidad.

Fuente: Elaboración propia.

Estabilidad de transmisión				
Bandas analizadas	Pausa / frecuencia	Pérdida de calidad visual	Pérdida de paquetes Estándar H.264	Perdida de paquetes Estándar H.265
Banda de 2,4GHz	Ocasional	Ocasiones	5%	7%
Banda de 5GHz	Ocasional	NO	2%	3%

Mediante los datos recolectados en la banda de 2,4GHz las pausa en la transmisión ocurre de manera ocasional lo cual debía a la frecuencia presenta una alta congestión al ser una banda muy concurrida por dispositivo. Esto provoca interferencia que pone en evidencia la estabilidad la conexión como también la calidad visual del vídeo, otro dato a destacar en la banda es un es un porcentaje alto de pérdidas de paquete visualiza tanto en el estándar H.264 y H.265. Se registra la mayor pérdida en el estándar H.265 presentando una mayor sensibilidad a la inestabilidad de la transmisión en banda de 2.4GHz.

En la banda de 5GHz ofrece una transmisión más estable y con menos interrupción, asimismo las pausas en la transmisión del vídeo son ocasionales, pero no causan la pérdida de calidad visual, y el apartado de las pérdidas de paquetes dentro de la banda es significativamente menor tanto en los estándares H.264 y H.265, demostrando una eficiencia mejor en la compresión de H.265.

4.3.3.5 Análisis de eficiencia de almacenamiento

Como ultimo análisis dentro del apartado de wireless tenemos el análisis de la eficiencia de almacenamiento, el cual tomo en cuenta los video utilizado para el análisis de calidad de transmisión, de los video obtenido se escogió el valor del tamaño de cada archivo, el cual se procesara mediante fórmulas para obtener valores en porcentaje de ahorro en el disco del NVR, para análisis en general se elaboró una tabla con datos del tamaño del video tanto los videos grabado en H.264 y H.265, la tabla menciona se presentara continuación.

Tabla 23. Valores obtenidos del cálculo de eficiencia de almacenamiento.

Fuente: Elaboración propia.

Eficiencia en almacenamiento			
Bandas analizadas	Tamaño del archivo H.265	Tamaño del archivo H.264	Ahorro de espacio (%)
Banda de 2,4GHz	44 Mb	46 Mb	4%
Banda de 5GHz	41 Mb	51 Mb	20%

En la banda 2,4GHz tiene un ahorro despacio del 4% al utiliza H.265 en comparación con H.264, aunque la diferencia del ahorro es leve el cual se debe a posibles congestiones mayores y una menor tasa de transmisión de datos en esta banda ya que el 2.4 GHz no tiene una mayor tasa de transmisión lo que limita la ventaja de compresión de vídeo en H.265.

En cambio, para la banda de 5GHz mostro un ahorro significativo de espacio del 20%, ya que al contar con menor interferencia y mayor capacidad de transmisión de datos permitió un aprovechamiento máximo del estándar de compresión H.265, el resultado es un ahorro notable de almacenamiento en comparación con H.265. En la banda 5 GHz es recomendable utilizar estándar de compresión de vídeo H.265

4.3.2 Análisis e interpretación de datos obtenido mediante el medio cableado UTP
El análisis del medio de transmisión cableado UTP se aplicará los mismos parámetros analizados en los medios inalámbricos de ambas bandas, al ser un medio que permite la conexión directa y estable entre NVR y cámara se espera resultados mejores que el obtenido en el apartado de medio inalámbrico.

4.3.2.1 Análisis de latencia y retardo

En la medición de la latencia y retardo, se capturo paquetes para el nuevo análisis el cual debemos de identificar tanto el paquete de envío como el paquete de respuesta como se realizó en análisis anterior en redes wireless.

El paquete de envío con número 983 de paquete, el cual debemos de tomar en cuenta el tiempo del paquete el cual es de 4.828s, datos se utilizará más adelante para el cálculo de latencia. (véase ilustración 163)

No.	Time	Source	Destination	Protocol	Length	Info
955	4.632693	192.168.1.42	192.168.1.120	TCP	54	5401E → 9000 [ACK] Seq=1 Ack=473472 Win=1023 Len=0
959	4.652934	192.168.1.42	192.168.1.120	TCP	54	5401E → 9000 [ACK] Seq=1 Ack=475140 Win=1026 Len=0
967	4.720504	192.168.1.42	192.168.1.120	TCP	54	5401E → 9000 [ACK] Seq=1 Ack=476228 Win=1022 Len=0
969	4.722824	192.168.1.42	192.168.1.120	TCP	54	5401E → 9000 [ACK] Seq=1 Ack=479140 Win=1022 Len=0
975	4.759163	192.168.1.42	192.168.1.120	TCP	54	5401E → 9000 [ACK] Seq=1 Ack=483434 Win=1026 Len=0
982	4.828566	192.168.1.42	192.168.1.120	TCP	54	5401E → 9000 [ACK] Seq=1 Ack=483840 Win=1024 Len=0
983	4.828564	192.168.1.42	192.168.1.120	TCP	78	5401E → 9000 [PSH, ACK] Seq=1 Ack=483840 Win=1024 Len=24

Ilustración 487. Captura de paquete mediante wireshark por medio UTP.

Fuente: Elaboración propia.

El siguiente paquete a identificar la respuesta entre los dispositivos el cual tiene numero de 984, obteniendo el valor de tiempo 4.830 el cual el ultimo valor para poder calcular el tiempo de latencia.

$$latencia = 4.830 - 4.828$$

$$latencia = 0.002s = 2ms$$

El valor de perdida es aceptable sabiendo que está utilizando compresión H.264 el tiende a tener valores un poco más alto de latencia, lo que significa que al usar el medio cableado UTP mejora el tiempo de retardo en el H.264.

De igual manera se realizar para compresión en H.265, para el paquete de envío identificado número 1197, de dicho paquete se toma el tiempo de envío el cual es de 5.958s. (véase ilustración 164).

No.	Time	Source	Destination	Protocol	Length	Info
1174	5.945735	192.168.1.43	192.168.1.120	TCP	54	54647 → 9000 [ACK] Seq=683415 Win=1828 Len=0
1177	5.950794	192.168.1.43	192.168.1.120	TCP	54	54647 → 9000 [ACK] Seq=680585 Win=1828 Len=0
1192	5.921654	192.168.1.43	192.168.1.120	TCP	54	54647 → 9000 [ACK] Seq=680723 Win=1828 Len=0
1194	5.930348	192.168.1.43	192.168.1.120	TCP	54	54647 → 9000 [ACK] Seq=680787 Win=1828 Len=0
1199	5.958096	192.168.1.43	192.168.1.120	TCP	78	54647 → 9000 [ACK] Seq=690783 Win=1828 Len=24

Ilustración 491. Captura de paquete mediante wireshark por medio UTP en compresión H.265.

Fuente: Elaboración propia.

El siguiente paquete es la respuesta, el paquete con numero 1199 brindando el valor del tiempo de envío de 5.960, una vez teniendo tanto el valor de envío como el de respuestas se puede calcular el valor de latencia.

$$\text{latencia} = 5.960 - 5.958$$

$$\text{latencia} = 0.002s = 2ms$$

El valor de latencia en base a compresión H.265 es igual al H.264, en base al resultado obtenido el medio de transmisión UTP es apto para trabajar en cualquier estándar de compresión ya que posee una tasa de retardo mínima. Mediante los otros análisis se evaluar cual será la mejor opción de compresión del medio.

4.3.2.2 Análisis del ancho de banda

En el análisis correspondiente al ancho de banda se realizó mediante los paquetes capturados tanto en compresión H.264 y H.265, para mejor manipulación de datos se realizó una tabla con valores de ancho de banda de cada paquete capturado en base a su estándar. (véase tabla 24)

Tabla 24. Valores de ancho de bando de cableado UTP.

Fuente: Elaboración propia.

Valores de ancho de banda		
Medio de transmisión	Estándar H.264	Estándar H.265
UTP	2 Mb	1.575 Mb

El cálculo realizado muestra que H.265 ofrece un ahorro de ancho de banda notable en comparación con H.264, el cual aprovecha de manera efectiva la eficiencia de compresión mediante el medio UTP, para un aprovechamiento óptimo del medio de transmisión UTP es recomendable usar la compresión H.265 ya que permite una

transmisión más eficiente dejarnos más ancho de banda disponible para otros dispositivos conectados al NVR.

4.3.2.3 Análisis de calidad de video en base a parámetros PSNR y SSIM

Dentro del análisis se enfoca en dos parámetros fundamentales PSNR y SSIM, los cuales serán calculando como se explicó en la guía realizada, los cuales se calcula grabando video en ambos estándares y manteniendo la misma duración en ambas grabaciones.

Valores obtenidos de PSNR:

PSNR y = 28.13 dB	PSNR Avg= 28.99 dB
PSNR u = 40.16 dB	PSNR min = 22.82 dB
PSNR v = 40.97 dB	PSNR Max = 28.88 dB

Mediante los resultado obtenido se verifica mejoría en los parámetros a tomar en consideración en el medio wireless, vemos el incremento el resultado de psnr y el cual todavía se encuentra con perdida luminancia, sin embargo manteniendo un alto porcentaje de luminancia en la compresión de video, el datos de psnr Avg el cual redondeando el valor obtenido vemos que cada vez se acerca más al valor correspondiente para tener cero perdida al momento de realizar compresión y comparación el video original.

Valores obtenidos para SSIM:

SSIM y = 0.91	SSIM v = 0.99
SSIM u = 0.98	SSIM All = 0.95

De igual manera presenta mayor es valores a comparación con los obtenido en medio wireless, tanto los valores de “ssim y” y “ssim All” al incrementado sus valores acercándose más a 1 cual el valor requerido para que la compresión se realice sin pérdida de video. Los datos obtenidos tanto en PSNR y SSIM, dan como acertado el uso de conexión UTP ya que cada vez se acerca a tener una comprensión total sin pérdida video.

4.3.2.4 Análisis de la estabilidad de transmisión

El penúltimo análisis corresponde a la estabilidad de transmisión, cual toma los paquetes capturados previamente para realizar el análisis de estabilidad, de igual manera como se realizó en el medio de transmisión wireless se compara datos físicos en conjunto a lo de generado por Wireshark, para dichos datos se elaboró una pequeña tabla para apreciar mejor los datos obtenidos. (véase tabla 25)

Tabla 25. Valores obtenidos para análisis de estabilidad del medio UTP.

Fuente: Elaboración propia.

Estabilidad de transmisión				
Medio de transmisión	Pausa / frecuencia	Pérdida de calidad visual	Perdida de paquetes Estándar H.264	Perdida de paquetes Estándar H.265
UTP	Ocasional	NO	0,5%	1%

Mediante la tabla 25, observamos menor pérdida en compresión H.264 esto debe de la conexión directa mediante UTP permitiendo una transmisión estable y confiable, en cambio la pérdida de paquetes en H.265 es ligeramente mayor, el cual puede ser por inferencia y al ser un estándar más amplio es susceptible a pequeñas inestabilidades, aunque sea mayor la pérdida en este estándar no es considerablemente alta, la transmisión mediante UTP se puede realizar en este estándar, aunque es más recomendable realizarlo en compresión H.264 por ser ligeramente más bajo que el de H.265.

4.3.2.5 Análisis de eficiencia de almacenamiento

Como último análisis para el medio UTP tenemos evaluar la eficiencia de almacenamiento, para lograr el análisis se utilizó el video grabado en el análisis de calidad de transmisión, de lo video mencionado los datos obtenidos fueron el tamaño de cada archivo, los cuales de igual manera se evaluarán mediante fórmula propuesta en la guía, con fin de optimizar el análisis se realizó una tabla donde consta los valores de cada archivo y en porcentaje el valor de ahorro en el disco del NVR. (véase tabla 26).

Tabla 26. Valores obtenidos del cálculo de eficiencia de almacenamiento.

Fuente: Elaboración propia.

Eficiencia en almacenamiento			
Medio de transmisión	Tamaño del archivo H.265	Tamaño del archivo H.264	Ahorro de espacio (%)
UTP	39	44	11%

El valor obtenido comprimiendo en H.265 muestra un ahorro del 11%, el cual es considerable en comparación con el espacio que ocupa H.264, mostrando que mediante la transmisión por UTP dará un óptimo ahorro al trabajar en compresión H.265. Dentro del sistema CCTV este ahorro es eficiencia a la hora de poder guardar más cantidad de video en el NVR sin necesidad de expandir el almacenamiento físico continuo.

4.3.3 Análisis e interpretación de datos obtenido mediante el medio de fibra óptica

El último medio de transmisión a analizar es el de fibra óptica, aplicando los mismos parámetros que en los medios anterior, la fibra óptica se espera que presente menos pérdida en todos los parámetros a ser un medio mucho más rápido y directo entre los dispositivos.

4.3.3.1 Análisis de latencia y retardo

Se realizó una captura de paquetes mediante el medio de transmisión de fibra en la cual se identificó ciertos paquetes a tomar en cuenta para realizar el cálculo respectivo de medición de latencia y retardo, de los cuales se identificó el paquete número 1117 con tiempo de envío de 8.065. (véase ilustración 165)

No.	Time	Source	Destination	Protocol	Length	Info
1115	8.064520	192.168.1.42	192.168.1.111	TCP	54	56077 → 9000 [ACK] Seq=1 Ack=230833 Win=512 Len=0
1117	8.065344	192.168.1.42	192.168.1.111	TCP	54	56077 → 9000 [PSH, ACK] Seq=1 Ack=230833 Win=512 Len=32

Ilustración 493. Captura de paquete mediante wireshark por medio fibra óptica.

Fuente: Elaboración propia.

De igual manera se identificó el paquete de respuesta entre los dispositivos el cual tiene de número de paquetes 1118 cuyo tiempo de envío es de 8.068, dichos valores se utilizarán tanto los obtenidos del paquete envío y de respuesta para el cálculo de la latencia.

$$\text{latencia} = 8.067 - 8.065$$

$$\text{latencia} = 0.002s = 2ms$$

El valor obtenido de latencia es adecuado para el medio utilizado en base a la compresión H.264, la compresión H.264 tiende a tener valores altos de latencia lo que muestra que este medio de fibra óptica tiende a mejorar el uso de compresión H.264.

A continuación, se realizó una nueva captura de paquetes en base a la compresión H.265, c identificó el paquete de envío con un número 9469, con el tiempo de envío de 66.718. (véase ilustración 166)

No.	Time	Source	Destination	Protocol	Length	Info
9403	66.543839	192.168.1.42	192.168.1.111	TCP	54	54825 → 9000 [ACK] Seq=1 Ack=2029596 Win=513 Len=0
9414	66.618675	192.168.1.42	192.168.1.111	TCP	54	54825 → 9000 [ACK] Seq=1 Ack=2031673 Win=513 Len=0
9457	66.699202	192.168.1.42	192.168.1.111	TCP	54	54825 → 9000 [ACK] Seq=1 Ack=2031753 Win=513 Len=0
9465	66.693116	192.168.1.42	192.168.1.111	TCP	54	54825 → 9000 [ACK] Seq=1 Ack=2033391 Win=513 Len=0
9469	66.718122	192.168.1.42	192.168.1.111	TCP	102	54825 → 9000 [PSH, ACK] Seq=1 Ack=2033414 Win=513 Len=128

Ilustración 496. Captura de paquete mediante wireshark por medio de fibra óptica en compresión H.265.

Fuente: Elaboración propia.

El siguiente paquete que identificar es el de respuesta dicho paquete llega con número de 9471 con un tiempo de respuesta de 66.719, Se realiza de igual manera el cálculo para saber el valor de latencia que tiene el medio a utilizar esta compresión.

$$\text{Latencia} = 66.719 - 66.6718$$

$$\text{latencia} = 0.001s = 1ms$$

El valor obtenido de latencia observamos que es el valor más bajo obtenido entre los 3 medios realizados el cual sólo evidencia más el uso de fibra óptica para mantener una transmisión sin pérdidas y con menos retardo de latencia.

4.3.3.2 Análisis del ancho de banda

Correspondiendo al análisis del ancho de banda se realizó mediante los paquetes capturados tanto en compresión H.264 y H.265, se realizó una tabla con valores de ancho de banda de cada paquete para tener una mayor facilidad en comparar los valores de cada estándar. (véase tabla 27)

Tabla 27. Valores de ancho de banda de fibra óptica.

Fuente: Elaboración propia.

Valores de ancho de banda		
Medio de transmisión	Estándar H.264	Estándar H.265
Fibra óptica	1 Mb	520 kb

El valor obtenido mediante el estándar H.265 ofrece un 48% menos de consumo de ancho de banda que el estándar H.264, el cual optimiza el uso de ancho de banda de la red y proporciona flexibilidad para añadir más flujo de vídeo o datos en la misma infraestructura de fibra, medios de transmisión de fibra óptica debe ser más usado en compresión H.265 el cual maximiza la eficiencia es transmisión permitiendo una alta calidad de video como ganar consumo de ancho de banda

4.3.3.3 Análisis de calidad de video en base a parámetros PSNR y SSIM

De igual manera se realiza el análisis de calidad de transmisión oye entonces los parámetros previamente establecidos que son los fundamentales para determinar el porcentaje de compresión que tiene cada vídeo a continuación serán los valores obtenidos mediante PSNR.

$$\text{PSNR } y = 29.98\text{dB}$$

$$\text{PSNR } u = 40.70 \text{ dB}$$

$$\text{PSNR } v = 40.2 \text{ dB}$$

$$\text{PSNR Avg} = 30.90 \text{ dB}$$

$$\text{PSNR min} = 29.5 \text{ dB}$$

$$\text{PSNR Max} = 31.41 \text{ dB}$$

Dentro de los valores obtenidos resaltamos el aumento de los valores en el cual la mayoría se encuentra sin pérdida de luminancia, el valor de psnr y en caso de redondear estaría en el rango de una compresión sin pérdida de luminosidad total pero el valor obtenido también representa una mínima pérdida, en cambio el valor de psnr Avg se encuentra por arriba del requerido el cual demuestra una compresión de vídeo totalmente sin pérdida comparación al vídeo de referencia.

Valores obtenidos para SSIM:

$$\text{SSIM } y = 1.01$$

$$\text{SSIM } u = 0.98$$

$$\text{SSIM } v = 0.99$$

$$\text{SSIM All} = 1.05$$

De igual manera que los valores obtenidos de ssim determina que no tiene valores de pérdida de luminosidad al momento de comprensión del vídeo H.265, lo que demuestra que al usar el medio de transmisión fibra óptica no existe valores de pérdida en PSNR y SSIM lo que demostraría un uso total de compresión del vídeo H.265.

4.3.3.4 Análisis de la estabilidad de transmisión

El correspondiente análisis de la estabilidad se realizó en base a los paquetes capturados previamente, de igual manera como en los anteriores análisis se elaboró una tabla donde se especifica los parámetros recolectado físico y generado por wireshark. (véase tabla 28)

Tabla 28. Valores obtenidos para análisis de estabilidad del medio fibra óptica.

Fuente: Elaboración propia

Estabilidad de transmisión				
Medio de transmisión	Pausa / frecuencia	Pérdida de calidad visual	Perdida de paquetes Estándar H.264	Perdida de paquetes Estándar H.265
Fibra Óptica	NO	NO	0,1%	0.2%

Los datos recolectados en la tabla 27, observamos como mediante el medio de fibra óptica no existe ni pausas ni tampoco pérdidas de calidad visual lo que permite una transmisión estable de vídeo, dentro de las pérdidas de paquete en los vamos estándar de compresión vemos que ligeramente es inferior la pérdida de paquetes en el estándar H.264 que el estándar H.265, los resultando mediante fibra óptica es ideal para la aplicación de vídeos en tiempo real que requieren alta confiabilidad y permitiendo una transmisión prácticamente sin pérdida de datos, esto mismo permite que fibra óptica pueda usar la compresión H.265 para obtener los otros beneficios que posee el estándar.

4.3.3.5 Análisis de eficiencia de almacenamiento

El último análisis para el medio ese evalúa la eficiencia de almacenamiento el cual se logra obteniendo el tamaño de cada vídeo grabado usado para el análisis de calidad de transmisión, para fácil manejo de datos se elaboró una tabla cuando los

valores de tamaño de los archivos generados en los diferentes estándares. (véase tabla 29)

Tabla 29. Valores obtenidos del cálculo de eficiencia de almacenamiento en el medio de fibra óptica.

Fuente: Elaboración propia.

Eficiencia en almacenamiento			
Medio de transmisión	Tamaño del archivo H.265	Tamaño del archivo H.264	Ahorro de espacio (%)
Fibra	10	15	33 %

EL valor obtenido en base a la compresión H.265 muestra un ahorro de espacio en el disco duro del NVR de 33% el cual es un valor muy alto dentro de los sistemas de CCTV al momento de guardar vídeos, el cual muestra el uso considerable de fibra óptica en los estándares de compresión H.265 para así optimizar el uso del sistema de bio vigilancia, así evita la constante expansión de almacenamiento físico del NVR.

4.4 Resultado obtenido al ejecutar código de distancia en base a círculos de referencia.

El código desarrollado para determinar instancia utilizándose el color de referencia siempre inventó con el objetivo de ofrecer una escala visual en la imagen capturada por la cámara, facilitando una rápida interpretación de la cercanía o distancia de objeto dentro del campo de visual. Esta escala, representada por círculos concéntricos simplifica el cálculo de distancias relativas desde el centro de la cámara brindando al operador la posibilidad de realizar una valoración visual de la localización de componentes en el ambiente supervisado.

La imagen obtenida en la ilustración 167, se puede observar la organización de los círculos concéntricos cada uno de ellos simboliza un aumento de distancia estable desde el centro hasta el borde de la imagen los círculos se delinean en azul, destacándose sobre el fondo y proporcionando un marco de referencia clara para la interpretación de distancia, además de proporcionar una efectividad en la distancia de objetos, el cual se comprobó para distancia entre las ubicaciones de ambas el cual se tomó como cámara centran las cámara 2, la distancia física de la cámara 1 es de 6.54 metros, en el rango de los círculos concéntricos vemos que está por

debajo del circuito con distancia de 6.65 metros el cual se interpreta que se encuentra en iguales rango de valores.

Además, permite analizar las coberturas efectivas de la cámara y detectar posibles zonas ciegas en el campo de visión, examinar las zonas abarcada por los círculos de referencia, se puede determinar si hay áreas donde la cámara carece de total visibilidad lo cual es crucial para perfeccionar la localización y el ángulo de la cámara en el sistema de videovigilancia.



Ilustración 499. Ejecución del segundo código de medición entre cámaras.

Fuente: Elaboración propia.

Mediante la ilustración 167, verificamos que al momento de ser ejecutado el código en ambas cámaras IP se genera de manera correcta y precisa los círculos de referencia, los círculos dibujando son ajustados automáticamente al campo visual de la cámara sin sacrificar resolución ni exactitud. La implementación convierte el sistema en un instrumento que permita estudiar en tiempo real, las distancias, mientras mejora el proceso de supervisión visual.

Para verificar que la generación de círculos concéntricos y la distancia de cada uno son exacto, se realizó diferentes pruebas de distancia entre ambas cámaras en los exteriores del laboratorio los cuales siguieron manteniendo una relación tanto en el valor físico como el valor próximo de la ubicación de la cámara en los círculos concéntricos, dado así que el código funcionado correctamente.

CONCLUSIONES GENERALES

En resumen, para la realización de este proyecto debemos tener en cuenta todos los conocimientos sobre redes inalámbricas, además todo sobre los estándares que serán utilizados en el mismo, junto con todos los parámetros y la logística del proyecto, sabiendo también la importancia de la elección de los equipos a utilizar ya que se pueden existir contra tiempos debido a que se pueden elegir equipos de diferentes marcas y esto ocasionaría de no se entrelazan o no haya una correcta comunicación dentro del sistema CCTV y esto nos genere errores, también es muy importante poder realizar un análisis en general del proyecto.

Una de las grandes ventajas es resaltar la estructura híbrida que se realizó en este proyecto, ya que las diferentes formas de conexión en la red tanto de cable UTP, Wi-Fi y Fibra óptica, con esto logramos aprovechar al máximo las fortalezas con el fin de mejorar la cobertura así la calidad de transmisión satisface las necesidades de nuestro sistema de videovigilancia, otro punto es la compresión de video llamado H.264 y H.265 que tiene un gran impacto en la eficiencia del ancho de banda y la definición y calidad de la imagen transmitida hacia el NVR, una parte importante fue la seguridad y robustez que posee este proyecto, ya que al ser híbrida en cada tipo de conexión tiene diferentes vulnerabilidades a tener en cuenta, agregando la importancia en la programación para reconocer y medir las distancias de objetos, personas, dando un extra de seguridad.

Además, tener en cuenta que al poseer redes híbridas nos brindarían muchos beneficios ya que permite el transporte de grandes cantidades de video hasta su almacenamiento, con esto facilitaría las búsquedas de grabaciones para revisiones futuras, este proyecto ayudaría a diferentes estudiantes a prepararse de una mejor manera saliendo con un conocimiento extra.

Con los resultados obtenidos en los diferentes escenarios demostraron la eficiencia del sistema CCTV, ofrece una solución a la problemática a la vigilancia en entornos complejos “Laboratorio de Telecomunicaciones”, así optimizando los diferentes recursos logrando obtener un equilibrio en confiabilidad, calidad y flexibilidad.

RECOMENDACIONES

Tener conocimiento en infraestructuras CCTV, en base al área de cobertura enfocadas al número de cámaras y la calidad de vídeo que se requiera, se debe considerar los obstáculos del entorno tanto en lo físico o en interferencias, para evitar los inconvenientes mencionados, se recomienda realizar modelado en programas como SketchUp.

Considerar para el diseño híbrido combinaciones de conexiones cableadas e inalámbricas para la implementación de sistemas CCTV, además seleccionar equipos que sean compatibles con los estándares 802.11 ac/n tanto como la cámaras y antenas ya que así se puede tener el rendimiento y seguridad óptima, cuando que los equipos puedan ser capaces de manejar ancho de banda que se requiera para transmitir y almacenar imágenes y vídeo del equipo hacia el NVR.

Realizar un estudio de sitio para identificar posibles obstáculos que puedan afectar la calidad de la señal inalámbrica, como paredes de concreto o interferencias electromagnéticas.

Tener en cuenta el diferente análisis de los diferentes escenarios que están tomados en cuenta este proyecto ya que cada uno tiene sus diferentes complejidades, también las condiciones de Red ya que las cámaras trabajan en doble frecuencia.

Además, se debe tener un presupuesto tanto de una estructura híbrida, la estructura de videovigilancia y un presupuesto de mantenimiento, ya que debe tener al estar en contacto con el ambiente su vida útil se disminuye y con un mantenimiento preventivo cada 6 meses para evitar fallos en el futuro sistema de CCTV.

Realizar nuevos estudios para la prueba de nuevos protocolos de seguridad para tener robustez en la estructura híbrida y tener una respectiva encriptación de datos para así enfocarse en las vulnerabilidades y corregirlas en un futuro.

ANEXOS

Anexos 1

```

import cv2
import numpy as np
import torch
import pandas as pd
# Verificar si PyTorch está utilizando la GPU
if torch.cuda.is_available():
    device = torch.device('cuda')
else:
    device = torch.device('cpu')
# Carga del modelo YOLOv5 pre-entrenado
model = torch.hub.load('ultralytics/yolov5', 'yolov5s', trust_repo=True) # Ajustar
el modelo según se requiera
# Definir los nombres de las clases de objetos
classes = model.names
# Parámetros de la cámara
focal_length = 800 # Longitud focal estimada en píxeles
real_object_height = 3 # Altura real del objeto en metros
# URL RTSP de la cámara Reolink
rtsp_url = "rtsp://admin:admin12345@192.168.0.120:554"
# Crear un objeto de captura de video
cap = cv2.VideoCapture(rtsp_url)
if not cap.isOpened():
    print("No se puede abrir la cámara IP")
    exit()
while True:
    # Capturar frame por frame
    ret, frame = cap.read()
    # Si no se recibió ningún frame, salir del bucle
    if not ret:
        print("No se puede recibir frame (final de la transmisión?)")
        break
    # Convertir el frame a RGB para YOLOv5
    frame_rgb = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
    # Detección de objetos con YOLOv5
    results = model(frame_rgb)
    # Extraer las detecciones
    detections = results.xyxy[0].cpu().numpy()
    # Recorrer las detecciones
    for detection in detections:

```

```

# Obtener el puntaje de confianza
confidencia = detection[4]
# Filtrar por detecciones con alta confianza (por ejemplo, mayor a 0.5)
if confidencia > 0.5:
    # Obtener las coordenadas del objeto
    x1, y1, x2, y2 = detection[:4].astype(int)
    # Obtener la clase del objeto (índice)
    clase = int(detection[5])
    # Obtener el nombre de la clase
    nombre_clase = classes[clase]
    # Calcular el alto del objeto en píxeles
    alto = y2 - y1
    # Estimar la distancia usando la fórmula: distancia = (real_object_height *
focal_length) / pixel_height
    distancia_en_metros = (real_object_height * focal_length) / alto
    # Dibujar un rectángulo alrededor del objeto
    cv2.rectangle(frame, (x1, y1), (x2, y2), (0, 255, 0), 2)
    # Visualizar el nombre de la clase y la distancia en metros
    cv2.putText(frame, f'{nombre_clase}: {distancia_en_metros:.2f} m', (x1,
y1 - 5), cv2.FONT_HERSHEY_SIMPLEX, 0.5, (0, 255, 0), 2)
    # Opcional: Redimensionar el frame para una ventana específica
    frame_resized = cv2.resize(frame, (1100, 650)) # Ajusta estas dimensiones
según necesites
    # Mostrar el frame
    cv2.imshow('Video en tiempo real con detección y distancia', frame_resized)
    # Salir del bucle si se presiona la tecla 'q'
    if cv2.waitKey(1) == ord('q'):
        break

# Liberar la captura de video
cap.release()
cv2.destroyAllWindows()

```

Anexos 2

```

import cv2

import matplotlib.pyplot as plt

import numpy as np

# URL de la cámara IP 2

```

```

cam2_url = "rtsp://admin:admin12345@192.168.0.120:554"
cam1_url = "rtsp://admin:admin12345@192.168.0.111:554"

# Configurar la cámara IP

cam1 = cv2.VideoCapture(cam1_url)
cam2 = cv2.VideoCapture(cam2_url)

# Verificar que ambas cámaras están abiertas

if not cam1.isOpened():
    print ("Error al abrir la cámara IP 1")

if not cam2.isOpened():
    print("Error al abrir la cámara IP 2")

if not cam1.isOpened() or not cam2.isOpened():
    exit()

# Ajustar el tamaño de la figura para ocupar más espacio (10x10 pulgadas)

plt.ion() # Modo interactivo de matplotlib

fig, ax = plt.subplots(1, 1, figsize=(15, 15))

def draw_distance_circles(frame, center, max_radius_px, conversion_factor):
    if frame is None:
        print ("Frame vacío recibido en draw_distance_circles.")
        return frame

    num_circles = 5 # Cantidad de círculos

    font_scale = 1.0 # Escala del tamaño de fuente aumentada

    font_thickness = 2 # Grosor del texto aumentado

    # Definir el color y grosor de los círculos

    circle_color = (255, 0, 0) # Negro

    circle_thickness = 5 # Grosor de los círculos aumentado

```

```

for i in range(1, num_circles + 1):

    # Calcular el radio en píxeles para cada círculo

    radius_px = int(max_radius_px * i / num_circles)

    # Calcular la distancia en metros

    distance_m = radius_px * conversion_factor

    # Dibujar el círculo con el color y grosor especificados

    cv2.circle(frame, center, radius_px, circle_color, circle_thickness)

    # Etiqueta de la distancia en metros en el borde derecho del círculo

    label_position = (center[0] + radius_px + 10, center[1] - 5)

    cv2.putText(frame, f"{distance_m:.2f} m", label_position,

                 cv2.FONT_HERSHEY_SIMPLEX, font_scale, circle_color, font_thickness)

    return frame

def calculate_distance(point1, point2):

    return np.sqrt((point2[0] - point1[0])**2 + (point2[1] - point1[1])**2)

# Distancia de referencia en metros y píxeles

real_distance_m = 1.0

ref_distance_px = 87

conversion_factor = real_distance_m / ref_distance_px # Relación de conversión
metros/píxeles

try:

    while True:

        # Capturar frames de las cámaras IP

        ret1, frame1 = cam1.read()

        ret2, frame2 = cam2.read()

        if not ret1 or not ret2:

            print("Error al capturar la imagen de una de las cámaras.")

```

```

    break

# Calcular el centro y el radio máximo

height, width, _ = frame2.shape

center2 = (width // 2, height // 2)

max_radius_px = min(center2[0], center2[1], width - center2[0], height - center2[1])

# Dibujar círculos de distancia en la imagen de la cámara 2

frame2 = draw_distance_circles(frame2, center2, max_radius_px, conversion_factor)

# Definir el centro de la cámara 1 como el centro del fotograma

center1 = (width // 2, height // 2)

# Calcular la distancia entre los centros de las cámaras en píxeles

distance_px = calculate_distance(center1, center2)

    # Convertir la distancia a metros

distance_m = distance_px * conversion_factor

print(f" {distance_m:.2f} metros") # Solo muestra el valor en metros

# Convertir BGR a RGB para matplotlib

frame2_rgb = cv2.cvtColor(frame2, cv2.COLOR_BGR2RGB)

# Limpiar la figura previa

ax.cla()

# Mostrar la imagen capturada con los círculos de distancia

ax.imshow(frame2_rgb)

ax.set_title('Vista de la Cámara IP 2 con Escala de Distancia')

ax.axis('off')

plt.draw()

plt.pause(0.01)

```

finally:

```
# Liberar los recursos  
cam1.release()  
cam2.release()  
cv2.destroyAllWindows()
```


Referencias

- [1] Security, «Security,» 23 07 2020. [En línea]. Available: <https://www.securitycom.mx/blog/antecedentes-de-la-video-vigilancia-e-importancia#:~:text=“El%20primer%20uso%20documentado%20de,ataques%20militares%20de%20larga%20distancia.>
- [2] J. ,. V. A. Rivas, «Implementación de sistemas de seguridad con video-vigilancia y software libre.,» Mexico DF, 2021.
- [3] L. Collantes, «DISEÑO DE UN SISTEMA DE SEGURIDAD A TRAVÉS DE CÁMARAS DE VIDEOVIGILANCIA PARA EL LABORATORIO 14 DE LA CARRERA EN COMPUTACIÓN Y REDES,» JIPIJAPA, 2019.
- [4] Quinde Pomagualli, W. F., «Implementación de un sistema de videovigilancia (CCTV) para los pasillos norte de la Escuela de Formación de Tecnólogos (ESFOT),» Bachelor's thesis, Quito, 2019.
- [5] P. Pazmiño, «Implementación de un sistema de cctv con cámaras IP en las sucursales de una empresa farmacéutica a nivel nacional,» *Escuela de Formación de tecnólogos*, 2019.
- [6] Madrid Jaramillo, P. A., & Pulles Arequipa, N. D., «Diseño de un sistema de seguridad mediante cámaras para los pasajes Alberto Rodríguez, Los Pinos, Segundo Clemente y Vargas del barrio Chaupimolino de la parroquia de Pifo,» Quito, 2020.
- [7] A. E. LOOR ALVARADO, «SISTEMA DE MONITOREO CON CÁMARAS IP PARA LA SEGURIDAD DEL CUERPO DE BOMBEROS DEL CANTÓN JIPIJAPA,» (*Bachelor's thesis, JIPIJAPA-UNESUM*), 2019.
- [8] Jurado Laime, G. F., & Marquez Gonzales, L. R., « Sistema de CCTV con camaras IP y central de alarma con radio enlaces de microondas para Centro de Salud Integral Bella Vista (Doctoral dissertation).,» 2018.
- [9] Llanos Torrejón, M., & Zapata Vilchez, R. A, «Diseño de un sistema de video vigilancia bajo una red de fibra óptica para mejorar la seguridad en los ambientes de la Universidad Nacional Pedro Ruiz Gallo-Lambayeque,» 2019.
- [10] Bustillos Rojas, Byron Marcelo, «Implementación de un circuito cerrado de televisión digital para la empresa telecomunicaciones fulldata,» de *Tesis de pregrado*, Quito, Universidad de las Américas, 2018.

- [11] E. L. A. PARRALES, «Implementación de un sistema de vigilancia con cámaras IP para el control y monitoreo en los departamentos de las salas de profesores y coordinación de la carrera de ingeniería en computación y redes de la universidad estatal del sur de Manabí,» *Tesis de Licenciatura*, 2019.
- [12] O. A. I. Yadira, Rediseño de sistema CCTV e Implementación de DVR Híbrido para la conexión de cámaras analógicas y digitales del Edificio Matriz y sus Exteriores de la Universidad Tecnológica Israel en Quito, Quito: Universidad Israel: Tesis de Maestría, 2016.
- [13] Freddy Jurado Laime Gregorio, Marquez Gonzales Luis Richard, «Sistema de CCTV con camaras IP y central de alarma con radio enlaces de microondas para Centro de Salud Integral Bella Vista,» de *Tesis Doctoral*, 2018.
- [14] D. L. T. T. D. Ismael, «Implementación de un sistema centralizado de videovigilancia (CCTV) para el edificio de la carrera de Ingeniería Eléctrica (CIELE) de la Universidad Técnica del Norte (UTN),» de *Tesis de licenciatura*, 2021.
- [15] Puma Magallanes, A., & Quispe Hernández, C., «Sistema de circuito cerrado de televisión y la instrucción sobre medidas de seguridad de los cadetes de comunicaciones de La Escuela Militar de Chorrillos “coronel Francisco Bolognesi”,» de *Tesis Doctoral*, Escuela Militar de Chorrillos coronel Francisco Bolognesi, 2020.
- [16] LARGO VILLEGAS CHRISTIAN GIOVANNY, VELASCO TOAPANTA HENRY JAVIER , «Tesis de Licenciatura,» de *Diseño de un sistema de video vigilancia para los Pasajes San Pedro, San Sebastián, Andrea, Santa Rosa, Bellavista del Barrio Chaupimolino de la Parroquia de Pifo*, Quito, 2020.
- [17] DELGADO INTRIAGO JOSÉ WALTER MENDOZA ZAMBRANO FERNANDO JAVIER, «REDISEÑO DEL CABLEADO ESTRUCTURADO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CON CÁMARAS IP Y MONITOREO EN TIEMPO REAL PARA MEJORAR LOS PROCESOS DE SEGURIDAD EN EL EDIFICIO DE LA FACULTAD DE CIENCIAS INFORMÁTICAS.,» 2018.
- [18] De La Torre Torres, D. I., «Implementación de un sistema centralizado de videovigilancia (CCTV) para el edificio de la carrera de Ingeniería Eléctrica (CIELE) de la Universidad Técnica del Norte (UTN),» Bachelor's thesis, 2021.

- [19] E. L. C. S. F. & G. R. F. Bernal Zea, «Diseño de una solución global de CCTV con radio enlaces UBIQUITI,» 2018.
- [20] MADRID PACHECO, Wilson Alejandro, «Diseño de un sistema de seguridad CCTV mediante una red WIFI para el monitoreo y control del edificio de la Gobernación de El Oro,» 2020.
- [21] I. Y. ORBE AMPUDIA, Rediseño de sistema CCTV e Implementación de DVR Híbrido para la conexión de cámaras analógicas y digitales del Edificio Matriz y sus Exteriores de la Universidad Tecnológica Israel en Quito, Quito, 2016.
- [22] S. Martí Martí, Martí Martí, S. (2013). Diseño de un sistema de televigilancia sobre IP para el edificio CRAI de la Escuela Politécnica Superior de Gandia, Universitat Politècnica de València: Tesis Doctoral, 2016.
- [23] A. A. Arbulú Orozco, Mejora del sistema de vídeo vigilancia utilizando tecnología de fibra óptica para la empresa CNPC El Alto-Talara., 2020.
- [24] C. H. & S. S. H. D. Ipiales Cáceres, Ipiales Cáceres, C. H., & Sarango Solano, H. D. (2020). Estudio de un sistema de video vigilancia para el barrio Chaupimolino de Pifo, quito , 2020.
- [25] J. L. Robles Bokun, «Contribución en las metodologías matemáticas para mejorar la compresión de video bajo el estándar H.264 AVC,» 2020.
- [26] S. Drăghici, «Diseño de filtros y su aceleración para el estándar H.265/HEVC,» 2017.
- [27] Sánchez Rubio, M., Barchino Plata, R., & Martínez Herráiz, J. J., Redes de computadores, Madrid, 2020.
- [28] Álava, W. L. S., Rodríguez, A. R., Ávila, X. L. A., & Cornelio, O. M., «Redes inalámbricas, su incidencia en la privacidad de la información,» de *Journal TechInnovation*, 2022, pp. 104-109.
- [29] Primiano Rios, R., & Figueroa Salvador, A., «Detección de comunidades en redes híbridas en el campo de la microfluídica,» *Universidad de las Ciencias Informáticas.FACULTAD 6. Facultad de Ciencias y Tecnologías Computacionales*, 2022.
- [30] M. L. C. LINDAO, «Administración y control de una red ipv6 basado en Infraestructura como un servicio para modelos de Cómputo virtual en el laboratorio de Telecomunicaciones con cifrado de extremo a extremo Utilizando

- dispositivos ubiquti,» de *INGENIERA EN TELECOMUNICACIONES*, Libertad, 2022.
- [31] Sanchez, S. P., & Delgadillo, H. M, «Topología aplicada en redes ad hoc. Mare Ingenii,» 2020, pp. 18-26.
- [32] E. Bellido Medina, «Diseño de una topología de Red LAN de alta disponibilidad y redundante para mejorar el estándar de servicio y soluciones Cloud de la empresa ITG SOLUTIONS SAC.,» 2019.
- [33] J. W. Bastidas Delgado, «Análisis, diseño e implementación de balanceador de carga segmentando la red del sistema de balanzas de pequeñas y medianas empresas del sector industrial Ciudad de Guayaquil,» de (*Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones*)., 2021.
- [34] Christensen, K., Reviriego, P., Nordman, B., Bennett, M., Mostowfi, M., & Maestro, J. A., «EEE 802.3 az: the road to energy efficient ethernet. IEEE Communications Magazine, 48(11),» 2010, pp. 50-56.
- [35] E. d. I. U. T. Nacional—edUTecNe, «Estándar IEEE 802.11 X De Las WLAN.Editorial de la Universidad Tecnológica Nacional—edUTecNe,» 2013. [En línea]. Available: http://www.edutecne. utn. edu. ar/monografias/standard_802_11. pdf. [Último acceso: 02 08 2023].
- [36] Siddiqui, F., Zeadally, S., & Salah, K., «Gigabit wireless networking with IEEE 802.11 ac: technical overview and challenges,» de *Journal of networks*, 2016, p. 164.
- [37] R. N. del, «Diseño e implementación de una solución de administración de tráfico de red basada en DNS y chequeos de disponibilidad,» Tesis Doctoral. Universidad Nacional de La Plata., 2016.
- [38] Luna del Águila, F., & DEL ÁGUILA, F. L. , «Implementación del Protocolo HTTP Paralelizado en Cliente y Servidor,» 1999.
- [39] André Luis de Souza Silva, Regina Célia Marques Freitas Silva, «Protocolo HTTP x protocolo HTTPS,» Nucleus, 2009, pp. 1-8.
- [40] David Mateos Costilla, Samuel Reaño Montoro, «Streaming de Audio/Video. Protocolo RTSP,» *Curs 2007/2008 enginy@ eps*, p. 15, 2008.
- [41] Rodriguez, O. A. R, and M. D. B. Casanova, «XX SIMPOSIO INTERNACIONAL DE INGENIERÍA ELÉCTRICA SIE 2023,» 2023.

- [42] D. F. Córdova Jácome, «Diseño de un sistema de seguridad utilizando cámaras IP inalámbricas para un Centro de Rehabilitación,» QUITO/EPN/2009, 2009.
- [43] Beltran Muñoz, Kerly Malena , and Bryan Jose Rodríguez Torres, «Implementación de un módulo educativo para el análisis de la vulnerabilidad de dispositivos IoT, empleando SDR y GNU radio.,» UPSE, Matriz. Facultad de Sistema y Telecomunicaciones, La Libertad, 2023.
- [44] F. A. Corrales Christian, «Estudio de la tecnología SDR (Software Defined Radio)y posibles aplicaciones en comunicaciones inalámbricas,» QUITO/ EPN, Quito, 2009.
- [45] Mateo Guale Joel Gustavo; Mirabá Figueroa Gisell Aracely, «Aplicación óptica para el desarrollo de procesos lógicos utilizando GNU radio y tecnología SDR,» UPSE, Matriz. Facultad de Sistema y Telecomunicaciones, La Libertad, 2023.
- [46] L. Alegsa, «Alegsa, L. (2023). Alegsa.com.ar - Informática, tecnologías, web, horóscopos. Alegsa.com.ar.,» 2023. [En línea]. Available: <https://www.alegsa.com.ar/#gsc.tab=0>. [Último acceso: 2 8 2023].
- [47] Peinado García Raúl, López Rubio Ezequiel, «ESTUDIO DE LA CALIDAD EN LAS DETECCIONES DE LA RED YOLOv5 CON TRANSFORMACIÓN DE IMÁGENES,» Malaga, 2022.
- [48] RLN12W, «Reolink.com,» [En línea]. Available: <https://reolink.com/ec/product/rln12w/#specifications>. [Último acceso: 20 mayo 2024].
- [49] RLC-510WA, «Reolink.com,» [En línea]. Available: https://reolink.com/ec/product/rlc-510wa/?attribute_pa_version=rlc-510wa-5mp-1-pack. [Último acceso: 20 mayo 2024].
- [50] U. Networks, «NanoStation M: Indoor/Outdoor airMAX CPE", datasheet,» [En línea]. Available: https://dl.ui.com/datasheets/nanostationm/nsm_ds_web.pdf. [Último acceso: 20 05 2024].
- [51] U. Networks, «NanoStation AC: Indoor/Outdoor airMAX CPE," datasheet,» [En línea]. Available: https://dl.ubnt.com/datasheets/NanoStation_AC/NanoStation_AC_DS.pdf. [Último acceso: 20 05 2024].
- [52] NetWifiWorks, «Ubiquiti Networks Authorized Online Reseller,» 2021.

- [53] «TX12 pro V2.0_tenda-all for better NetWorking,» Tenda Global, [En línea]. Available: <https://www.tendacn.com/product/TX12Prov2.html>. [Último acceso: 20 05 2024].
- [54] «Tendacn.com,» [En línea]. Available: <https://down.tendacn.com/uploadfile/TX12/TX12%20Datashet.pdf>. [Último acceso: 20 05 2024].
- [55] «¿Tipos de transceiver y cuáles son las diferencias entre transceiver y transpondedor?,» Knowledge, 24 05 2021. [En línea]. Available: <https://community.fs.com/es/article/transceiver-vs-transponder-what-are-the-differences.html>. [Último acceso: 20 05 2024].
- [56] C. C. Olvera Vera, «Análisis, diseño del cable estructurado y propuesta de implementación en la Unidad Educativa PCEI de Los Ríos,» (Bachelor's thesis, Babahoyo: UTB-FAFI), 2022.
- [57] G. M. David, «Diseño de una red de fibra óptica con cable DROP para llevar Internet de la oficina central a el almacén de la Empresa Pollos Guadas SRL,» Doctoral dissertation, La Paz, 2023.
- [58] Cometa Pillimue, F. J., & González Hernández, K. S., «Diseño de una red inalámbrica para la implementación de CCTV,» *en inmediaciones en la Fundación Universitaria San Mateo*, 2022.
- [59] Musso Zapico, J. I., «Monitoreo de seguridad y medidas de prevención de contagio de Covid-19 mediante detección en sistema CCTV para la minería.,» 2021.
- [60] Quinde Pomagualli, W. F., «Implementación de un sistema de videovigilancia (CCTV) para los pasillos norte de la Escuela de Formación de Tecnólogos (ESFOT) (Bachelor's thesis),» Quito, 2019.
- [61] L. A. & M. M. Á. A. López Castellanos, «Propuesta de un plan de repuestos centralizados en confiabilidad (RCC) para mejorar la ejecución de actividades de mantenimiento correctivo en el sistema CCTV de las sedes compensar salud y caja en Bogotá y la Sabana,» 2023.
- [62] D. L. Chávez Quiroga, «Diseño de un sistema CCTV basado en tecnología IP y almacenamiento en la nube para la urbanización Eloy Alfaro (Bachelor's thesis),» 2022.

- [63] J. I. Ayala Alejo, «Implementación de video-vigilancia remota basada en camaras inalámbricas IP para laboratorio de Centro de Protección y Seguridad Radiológica-IBTEN,» Doctoral dissertation, 2018.
- [64] P. F. Pazmiño Valles, «Implementación de sistema de CCTV con cámaras IP en las sucursales de una empresa farmacéutica a nivel nacional (Bachelor's thesis, Quito, 2019.),» 2019.
- [65] Jinez Granja, R. D., & Pantoja Prado, C. H., «Diseño de un sistema de videovigilancia para el barrio los Pinos de la parroquia de Pifo (Bachelor's thesis, Quito, 2020.),» 2020.
- [66] «Knowledge,» ¿Tipos de transceiver y cuáles son las diferencias entre transceiver y transpondedor?, 24 mayo 2021. [En línea]. Available: <https://community.fs.com/es/article/transceiver-vs-transponder-what-are-the-differences.html>. [Último acceso: 20 mayo 2024].