ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

Implementación de un sistema de vídeo vigilancia IP y un sistema de seguridad WiFi WPA2 Enterprise mediante un servidor radius, para mejorar la seguridad física y tecnológica en las oficinas del GAD Municipal del Cantón Saquisili.

Lagla Chiluisa, Erick Patricio y Malan Naula, Cristhian Marcelo

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Trabajo de integración curricular, previo a la obtención del título de Tecnólogo Superior en Redes y Telecomunicaciones

Ing. Moreta Changoluiza, Janneth Elizabetn

8 de diciembre del 2022

Latacunga

ESPE2022_Trabajo_titulacion_Lagla_Malan.pdf

Scanned on: 19:8 December 2, 2022 UTC

Overall Similarity Score

Results Found

Total Words in Text

Identical Words	110
Words with Minor Changes	25
Paraphrased Words	220
Omitted Words	0

COPYLEAKS Website | Education | Businesses

Ing. Moreta Changoluiza, Janneth Elizabeth

C. C.: 0503078974

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Certificación

Certifico que el trabajo de integración curricular: "**Implementación de un sistema de vídeo vigilancia IP y un sistema de seguridad WiFi WPA2 Enterprise mediante un servidor radius, para mejorar la seguridad física y tecnológica en las oficinas del GAD Municipal del Cantón Saquisili.**" fue realizado por los señores **Lagla Chiluisa, Erick Patricio y Malan Naula, Cristhian Marcelo,** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizada en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Latacunga, 8 de diciembre del 2022

.....

Ing. Moreta Changoluiza, Janneth Elizabeth

C. C.: 0503078974

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Responsabilidad de Autoría

Nosotros, **Lagla Chiluisa, Erick Patricio**, con cédula de ciudadanía n° 0550455562, y **Malan Naula, Cristhian Marcelo**, con cédula de ciudadanía N° 1727579714, declaramos que el contenido, ideas y criterios del trabajo de integración curricular: "**Implementación de un sistema de vídeo vigilancia IP y un sistema de seguridad WiFi WPA2 Enterprise mediante un servidor radius, para mejorar la seguridad física y tecnológica en las oficinas del GAD Municipal del Cantón Saquisili.**" es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Latacunga, 8 de diciembre del 2022

Lagla Chiluisa, Erick Patricio
C.C.: 0550455562

Malan Naula, Cristhian Marcelo
C.C.: 1727579714

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Autorización de Publicación

Nosotros **Lagla Chiluisa, Erick Patricio**, con cédula de ciudadanía n° 0550455562, **y Malan Naula, Cristhian Marcelo**, con cédula de ciudadanía N° 1727579714, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de integración curricular: "**Implementación de un sistema de vídeo vigilancia IP y un sistema de seguridad WiFi WPA2 Enterprise mediante un servidor radius, para mejorar la seguridad física y tecnológica en las oficinas del GAD Municipal del Cantón Saquisili.**" en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Latacunga, 8 de diciembre del 2022

.....

Lagla Chiluisa, Erick Patricio

C.C.: 0550455562

.....

Malan Naula, Cristhian Marcelo

C.C.: 1727579714

Dedicatoria

Este proyecto va dedicado para las personas importantes como son mis padres, quienes han estado apoyándome constantemente en el proceso de mi vida y ser la persona que soy.

Se lo dedico también a una persona muy especial, que siempre estuvo conmigo en las buenas y en las malas, que me enseño que la vida es una lucha constante, que siempre confió en mí y que lamentablemente ya no está a mi lado para ver realizado su sueño, pero que siempre vive en mi mete y en mi corazón.

Lagla Chiluisa, Erick Patricio

Dedicatoria

El presente proyecto está dedicado a mi familia ya que son las personas más importantes en mi vida, quienes me han apoyado en cada proceso de mi formación académica, gracias a ustedes he logrado llegar hasta aquí con el apoyo que me brindan día con día para cumplir mis metas, A mis hermanos que por medio de su alegría me motivaron a seguir adelante para alcanzar mis metas.

A todas las personas importantes en mi vida quienes con sus palabras de aliento no me dejaban decaer para que siguiera adelante con mi educación para poder adquirir nuevos conocimientos durante esta etapa de mi vida.

Malan Naula, Cristhian Marcelo

Agradecimiento

Primeramente, quiero agradecer a Dios fuente de amor y sabiduría, por guiarme en el camino, y porque solo el sabe todo el esfuerzo y dedicación que puse en este trabajo. Le agradezco por la gran familia que me ha dado, por todas esas experiencias que viví junto a ellos para poder alcanzar la meta y cumplir uno de mis sueños.

A mi madre la Sra. Myrian Chiluisa por darme la vida y brindarme todos esos momentos de alegría y tristeza, por la paciencia y el apoyo incondicional que me ha brindado en todos estos años de la vida.

A mi padre el Sr. Franklin Lagla esfuerzo que hace cada día para poder apoyarme en todo momento, por esa imagen paterna que me ha enseñado a nunca rendirme y seguir en adelante.

A mis amigos que siempre estuvieron para mí en todas las circunstancias, por los consejos, por nuevas enseñanzas.

Lagla Chiluisa, Erick Patricio

Agradecimiento

Quiero empezar agradeciendo a dios, por haberme otorgado una familia maravillosa quienes han creído en mí siempre dándome enseñanzas de humildad, respeto y sacrificio para lograr mis metas. Agradezco por haberme cuidado y protegido en cada momento de mi vida. En cada una de mis decisiones tomadas dándome la fortaleza para cumplir cada uno de mis sueños planteados.

A mi gran familia Malan Naula por todo el apoyo que me brindaron durante el trayecto de mi vida, dándome sabios consejos, enseñándome a valorar todo lo que tengo ya que ellos han fomentado un mí el deseo de superación y de triunfo en la vida. Es por esto que siempre estoy agradecido con ellos ya que siempre cuento con su valioso e incondicional apoyo.

Agradezco a mis docentes quienes compartieron nuevos conocimientos, experiencias y consejos para seguir adelante con mi educación, por tal razón fueron personas muy valiosas que me motivaron para seguir adelante con mi educación.

A mis amigos que siempre me apoyaron en todo momento para poder cumplir mis sueños y por su amistad sincera que siempre lo tendré presente en mi vida. Muchas gracias.

.

Malan Naula, Cristhian Marcelo

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Resumen

El objetivo de este proyecto es implementar un sistema de seguridad de video vigilancia IP y un sistema de seguridad Wifi empresarial WPA2 utilizando un servidor radius para mejorar la seguridad física y tecnológica en las oficinas del GAD Municipal del Cantón Saquisili. El proyecto se inició con un análisis del establecimiento, un reconocimiento del sistema de video vigilancia y del sistema de seguridad Wifi actual; mediante esto, se determinó que el sistema inalámbrico no tiene cobertura en varias de las oficinas y la información que se maneja ahí es demasiada delicada; también, existen espacios en la localidad que no cuentan con video vigilancia y donde es necesario implementar el sistema de seguridad. Para ello, se establecieron y seleccionaron los elementos necesarios tanto de software como de hardware que presentan las mejores características para la implementación. Finalmente, una vez implementado los sistemas propuestos, se puede verificar una conexión segura, rápida y eficiente a través de pruebas de conexión Wifi de los usuarios desde sus smartphones, además se obtuvo un sistema de video vigilancia más eficiente y confiable, brindando tranquilidad al personal, ya que se puede acceder a las imágenes y grabaciones de las cámaras vía internet, desde cualquier parte del mundo.

Palabras clave: Video Vigilancia, Sistema de Seguridad, WPA2 Enterprise, Servidor Radius, Conexión Segura.

Abstract

The objective of this project is to implement an IP video surveillance security system and a WPA2 enterprise Wifi security system using a radius server to improve physical and technological security in the offices of the GAD Municipal del Cantón Saquisili. The project began with an analysis of the establishment, a recognition of the video surveillance system and the current Wifi security system; through this, it was determined that the wireless system does not have coverage in several of the offices and the information that is handled there is too sensitive; also, there are spaces in the locality that do not have video surveillance and where it is necessary to implement the security system. For this purpose, the necessary software and hardware elements were established and selected that have the best characteristics for implementation. Finally, once the proposed systems have been implemented, a secure, fast and efficient connection can be verified through Wifi connection tests of the users from their smartphones, in addition to obtaining a more efficient and reliable video surveillance system, providing peace of mind to the staff, as the images and recordings of the cameras can be accessed via the internet from anywhere in the world.

Key words: Video Surveillance, Security System, WPA2 Enterprise, Radius Server, Secure Connection.

Capítulo I

Planteamiento del problema

Tema

Implementación de un sistema de vídeo vigilancia IP y un sistema de seguridad WiFi WPA2 Enterprise mediante un servidor radius, para mejorar la seguridad física y tecnológica en las oficinas del GAD Municipal del Cantón Saquisili.

Introducción

En estos últimos años se ha visto como la tecnología ha evolucionado de manera acelerada, cada vez siendo más accesible yendo a la par con nuevas formas de corromperlas, con la finalidad de acceder de forma ilegal a información privada, esto ha llevado que la mayoría de establecimientos públicos y privados tengan la necesidad de adquirir equipos que mantengan la seguridad física y lógica.

Hoy en día las empresas o establecimientos necesitan de un sistema de video en red que puede reducir significativamente los hurtos, mejorar la seguridad de los empleados y agilizar la administración del establecimiento. El sistema permite la detección rápida de posibles incidentes y falsas alarmas.

En la última década se ha observado que la mayoría de las comunicaciones, ya sean inalámbricas o por cable se envían a través de redes en un esfuerzo por proteger la información que allí se procesa. Este tráfico tiene como objetivo evitar el procesamiento de información confidencial por parte de personas malintencionadas.

Es por ello que, con la planificación y la implementación de este proyecto, se busca mejorar las zonas vulnerables que no cuentan con la vigilancia y la expansión de red

inalámbrica en las oficinas del Gad Municipal de Saquisilí, cumpliendo con los requisitos que una institución pública necesita para llevar una vigilancia correcta, además brindar al personal una nueva red wifi en la sala de reuniones y las oficinas de la jefatura, secretaría, personal técnico y dirección. Esto no solo aumenta la cobertura de la red principal, sino que también brinda total seguridad al ver o compartir información confidencial.

Antecedentes

Estamos constantemente impulsados a querer aprovechar el consumo, uso y mejoras que ofrecen las redes inalámbricas ampliamente utilizadas hoy en día en el monitoreo continuo, lo que nos lleva a querer probar varios de sus servicios y, al mismo tiempo enviar y recibir diversos formatos de datos, lo que nos lleva a querer probar y, al mismo tiempo, dando respuesta sobre la capacidad de conectividad de las tecnologías inalámbricas con un sistema de seguridad WiFi WPA2 Enterprise mediante un servidor radius, es por ello que es necesario sustentar nuestro tema de investigación mediante los antecedentes de trabajos investigativos ante hechos, los cuales deben contar con un respaldo de información preexistente caracterizados por cumplir con todos los criterios científicos los cuales se presentan a continuación.

En su proyecto de tesis elaborado por (Suquillo, 2020) Con el tema “Diseño e implementación de una red inalámbrica y el sistema de videovigilancia sobre IP para la Unidad Educativa Cristiana Verbo Mañosca en la ciudad de Quito” de la Universidad Internacional SEK; manifiesta que: El proyecto nace de la necesidad de solventar las vulnerabilidades y las amenazas de seguridad que presenta la institución, ya que no disponía de un sistema de video vigilancia, por ello se implementó el sistema de videovigilancia IP inalámbrico para mejorar la seguridad y brindar mayor confianza a sus estudiantes y docentes, luego de haber culminado el proyecto se ha notado una disminución de la inseguridad dentro de la institución.

Por otro lado, el trabajo de grado realizado por Medina (2019) con el tema “Red de videovigilancia utilizando cámaras IP para el monitoreo del proceso de producción en la empresa de AGGROCUEROS S.A. de la ciudad de Ambato”.; menciona que: Para que la empresa mejore su producción y entregue productos de buena calidad a sus clientes, es debe diseñar un sistema de control con una red de vigilancia IP, de tal manera que se pueda controlar tanto los procesos de producción así como la responsabilidad de los trabajadores en el desempeño de sus áreas de trabajo, además de ello este sistema sirve para la video vigilancia de la seguridad del personal y de los bienes materiales que existe en las instalaciones ya que cuentan con software que permite tener acceso a las cámaras las 24 horas del día y así identificar posibles robos, los cuales pueden ser detenidos.

Del mismo modo el proyecto elaborado por (Fuentes, 2020) Con el tema “Implementación de un prototipo de red inalámbrica que permita elevar los niveles de seguridad a través de la autenticación de un servidor Radius para los usuarios que accedan a internet en el edificio Francisco Morazán de la UTEC”.; menciona que: El objetivo de este proyecto de investigación es aumentar el nivel de seguridad de acceso a la red inalámbrica en el edificio Francisco Morazán de la Universidad Técnica de El Salvador, al mismo tiempo que se brinda un control más directo a cada usuario universitario, en el cual utilizaron el servidor de autenticación Radius, ya que este servidor era el encargado de autenticar las credenciales del usuario para dar acceso a la red inalámbrica del edificio.

Como se puede evidenciar en los trabajos anteriormente descritos es de gran interés que se implemente un sistema de vídeo vigilancia IP y un sistema de seguridad WiFi WPA2 Enterprise mediante un servidor radius, para mejorar la seguridad física y tecnológica en las oficinas del GAD Municipal del Cantón Saquisili, ya que hoy día es necesario tener una mejor seguridad tanto en los interiores como en la parte externa de las instalaciones de la municipalidad.

Planteamiento Del Problema

En base a la argumentación de la seguridad se analizó y se comparó los distintos sistemas de seguridad que actualmente se encuentran instalados en las oficinas del GAD Municipal del Cantón Saquisili. Así como también se evidenció puntos vulnerables dentro de las diferentes áreas del municipio los cuales se encuentra la problemática de seguridad, y por ende son vulnerables ante actos delictivos.

Así también por la falta de una tecnología actualizada en el circuito informático se corre el riesgo de perder archivos, sufrir el robo de información confidencial o bloqueo de los datos de los diferentes equipos informáticos, que son utilizados en los departamentos del GAD Municipal.

La tecnología está avanzando de forma acelerada, así también de forma paralela surgen nuevos métodos para violentar la red, por este motivo cada vez más instituciones públicas, empresas privadas, locales comerciales, domicilios, y entre otros, han sido víctimas de la delincuencia; y se han visto en la necesidad de buscar alternativas de seguridad.

Es por esta razón que se debe expandir esta tecnología dentro de las oficinas más importantes como son la sala de reuniones, donde constantemente ingresan las personas, también en el área de TIC´S, y aún más importante en bodega donde se encuentran varios objetos de valor. Así mismo, por medio del sistema de seguridad WiFi WPA2 Entreprise ayudara en el control de acceso a la red inalámbrica en la sala de reuniones y oficinas cercanas, del mismo modo el sistema de video vigilancia IP podrá ser vigilada mediante el segmento de red por el personal autorizado, esta persona podrá observar imágenes captadas por dicho sistema o verificar novedades suscitadas en un lapso de fechas que se encontrara almacenado dentro del disco duro del dispositivo (NVR).

Justificación

Como resultado de los avances tecnológicos, el uso de los sistemas de seguridad basados en la tecnología IP, la seguridad física y la vigilancia se han incrementado significativamente a nivel nacional en sus últimos años. Debido a que la tecnología IP está enfocada al bienestar humano, este proyecto se enfoca en la seguridad física e informática de las instalaciones del municipio de Saquisili.

La aplicación de un sistema de video vigilancia IP y un sistema de seguridad

WiFi WPA2 Enterprise a través de un servidor RADIUS, así como cualquier otro dispositivo de red, es importante para la seguridad y se puede realizar a bajo costo utilizando la infraestructura existente, como servidores, computadoras y cableado estructurado, que se encuentra dentro de los edificios del GAD Municipal. Esta ampliación ayudaría a supervisar y proteger, de forma local y remota las oficinas vulnerables, con lo cual se podrá evitar delitos tanto físicos como informáticos y detectar al causante de diversas acciones ilícitas cometida o de un comportamiento indebido. Garantizando un trabajo correcto de sus empleados.

Es así, que este proyecto de titulación se justifica en el área tecnológica ya que se estará ampliando un sistema de video vigilancia mediante cámaras IP de última tecnología, debido que actualmente existen áreas vulnerables y de suma importancia como son el salón de reuniones, la bodega donde se almacena todo tipo de material de la institución. También, se aumentará un sistema de seguridad WIFI WPA2 Enterprise, el cual es necesario para la protección de los archivos informáticos que se encuentran en las diferentes oficinas del Municipio del cantón Saquisili.

Así mismo, se justifica considerar la economía del proyecto en términos de costo-efectividad. Esto se debe a que se protege a las personas y bienes del sector correspondiente con una inversión mínima para su implementación.

El presente proyecto de investigación es viable, ya que presenta características de escalabilidad para futuras implementaciones sobre el mismo sistema de video vigilancia IP, a su vez mejorar la calidad de seguridad en otras zonas que necesiten de esta herramienta necesarias en la actualidad para la seguridad.

Objetivos

Objetivo General

- Implementar un sistema de vídeo vigilancia IP y un sistema de seguridad WiFi WPA2 Enterprise mediante un servidor radius, para mejorar la seguridad física y tecnológica en las oficinas del GAD Municipal del Cantón Saquisili.

Objetivos Específicos

- Establecer los requerimientos teóricos prácticos necesarios para la implementación de un sistema de videovigilancia IP.
- Implementar las cámaras de videovigilancia IP, el Access Point y el servidor Radius en los puntos estratégicos.
- Realizar pruebas de funcionamiento del sistema de video vigilancia IP, el Access Point y la autenticación de usuarios del servidor radius.

Alcance

La ampliación del sistema de video vigilancia IP y un sistema de seguridad WiFi WPA2 Enterprise se realizará en el GAD Municipal de Saquisili el cual cuenta con diferentes áreas al servicio de la comunidad. Así mismo se realizara una análisis del sistema de video existente, debido a que el alcance que tiene este sistema no cubre los algunos puntos vulnerables y esenciales es por ello que se implementará un NVR con más capacidad de canales con

tecnología actual al igual que las cámaras teniendo en cuenta el tipo el tipo de lente, la distancia focal entre muchas otras características permitiendo obtener una mejor captación de la imagen, además se realizara un sistema de seguridad WiFi WPA2 Enterprise utilizando un servidor radius, el cual ayudaría a controlar y administrar el acceso a la red inalámbrica a los usuarios que se encuentran registrados en el servidor el cual se encargara de verificar la autenticidad de la información, siendo una red segura debido a la configuración del protocolo de seguridad cliente-servidor. Obteniendo una mejor seguridad en el área donde no llega este protocolo, evitando las consecuencias de un posible robo de archivos informáticos, además de obtener ahorros en la inversión.

Capítulo II

Marco Teórico

Sistema de video vigilancia IP

Con el paso de los años y con el avance tecnológico, los sistemas de CCTV van perdiendo posicionamiento en el campo de la videovigilancia debido a su infraestructura cableada, actualmente la videovigilancia IP va ganando terreno en el mercado con gran aceptación entre los usuarios y debido a sus ventajas. El cual nos permite combinar con los sistemas análogos, facilitándonos el seguimiento constante de la información contenida en un sistema de videovigilancia IP.

Como señala García (2019) “Las cámaras IP pueden brindar una resolución hasta 16 veces mayor y un zoom digital superior facilitando cubrir áreas más grandes en las zonas donde se encuentran ubicados los equipos”.

Por eso es la solución de seguridad que ha ido tomando fuerza en el mercado global en los últimos años, especialmente en América Latina, por sus ventajas y por tener características especiales. Tecnología CCTV o sistema de seguridad de video analógico. La calidad de imagen, la robustez, la relación precio/rendimiento razonable, el sistema abierto y el análisis inteligente que hacen un mejor uso del video son muchos de los factores que lo hacen destacar. CCTV o parte de un sistema de CCTV, que es ante todo una ilusión de seguridad, pero han demostrado ser insustanciales.

Como afirma Austerberry (2019) ”Los sistemas de videovigilancia IP brindan de manera extensa soluciones para una amplia gama de aplicaciones industriales y segmentos para el mercado”. Ya sea que necesite unas pocas cámaras o más para la instalación permitiendo satisfacer los requerimientos del cliente.

Por otro lado Baltazar (2019) señala que “El costo inicial de las cámaras de red en realidad puede ser elevado en comparación al resto de equipos”. Sin embargo, al comparar el costo por canal y las cámaras IP, su capacidad y rendimiento superior se oponen aceleradamente los sistemas analógicos con los DVR.

Por lo tanto, podemos concluir que las cámaras IP se pueden conectar fácilmente en las redes IP existentes. A través de la red de área local, se puede monitorear remotamente los cuartos de servidores, y, además, los sistemas que se encuentran implementados.

Video IP

Según García (2019) “La video vigilancia IP, comúnmente conocida como video IP, es un tipo de comunicación que tiene lugar a través de redes cableadas o inalámbricas”.asi también teniendo en cuenta este criterio, la información, ya sea de audio o video, se enruta a través de la misma infraestructura de red.

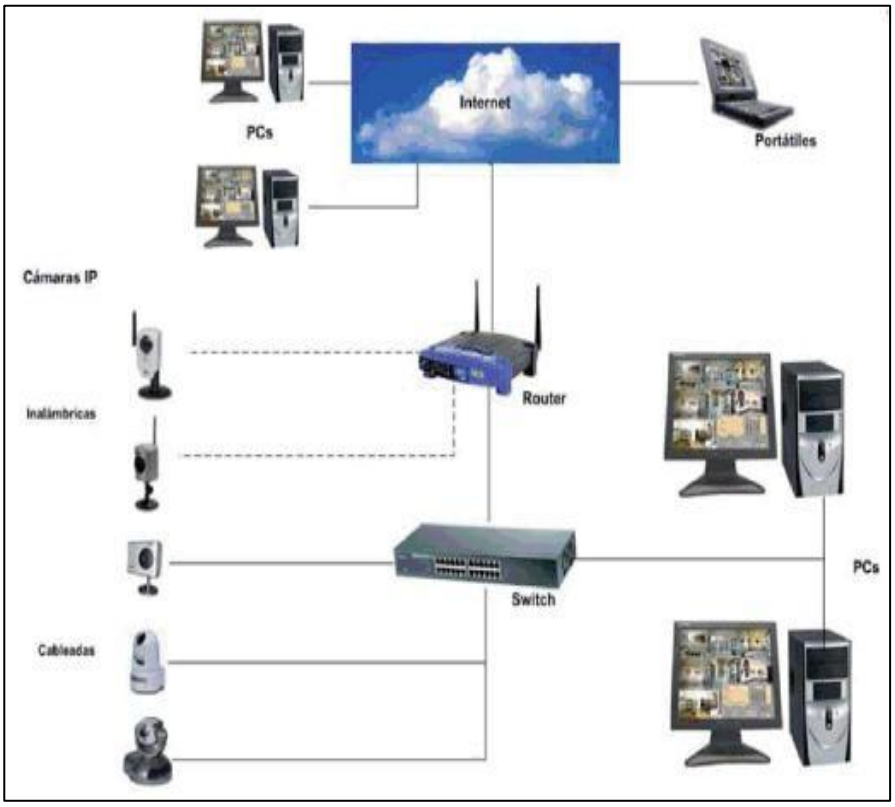
Una característica muy relevante de las redes IP es que se utilizan para alimentar algunos dispositivos como cámaras IP gracias a PoE (Power Over Ethernet) que también permite el monitoreo remoto en tiempo actual.

Elementos de un sistema de videovigilancia IP

- Cámaras IP
- Cámaras análogas
- Servidor de video
- Gestión de video (Servidores de almacenamiento)
- Sala de monitorización
- Componentes de la red de datos

Figura 1

Sistema de video vigilancia IP



Nota. Esquema de una red de video vigilancia IP. Tomado de (Mata, 2019)

Ventajas de sistema de videovigilancia IP

Acceso remoto seguro a video

Un acceso a las cámaras de red se puede dar en diversos momentos desde cualquier dispositivo conectado a la misma red, permitiendo garantizar una gestión de video confiable aumentando la seguridad de usuario. (Gaybor, 2018)

Imagen nítida para identificación confiable

Las cámaras de red tienen resoluciones significativamente más altas. Para reducir la distorsión causada por el movimiento, así también, muchas cámaras de red emplean barrido progresivo.

Gestión de eventos con video inteligente

Como expresa Juan (2018) “Los sistemas con cámaras de red pueden buscar y responder automáticamente a varios eventos o amenazas “Como resultado, hay una carga de trabajo significativamente menor para el personal, disminuye requerimientos de ancho de banda, almacenamiento, facilitado videovigilancia más confiable.

Funcionalidad

Usada mediante plataforma tecnológica abierta, estas cámaras de red pueden ser instaladas fácilmente en otros sistemas existentes, como en diferentes sistemas de control de acceso, además proporcionan mayor funcionalidad. (Londoño., 2020)

Menor coste total de propiedad

Estas soluciones de vigilancia IP funcionan mediante servidores, computadoras y redes IP, los cuales son accesibles con la tecnología Power over Ethernet, lo que supone un importante ahorro en costes de hardware, gestión e instalación.

Accesibilidad remota

Permite observar videos en vivo y grabados desde cualquier ubicación de red, facilitando la configuración y acceso de forma remota a diferentes cámaras IP ubicadas en una zona determinada. (Gaybor, 2018)

Calidad de imagen

La alta calidad de imagen es indispensable para visualizar claramente el incidente y del mismo modo, identificar a las personas involucradas, así también de acuerdo con Sistemas (2022) “La cámara de red produce una imagen de mejor calidad y mayor resolución gracias a la tecnología del mismo y los mega pixeles”. Por el cual mantener la calidad de imagen es más fácil en los sistemas de video en red que en sistemas analógicos.

En los sistemas de video vigilancia IP, las imágenes se digitalizan una vez y se conservan en forma digital sin conversión innecesaria o pérdida de calidad debido a la distancia de red. (Sistemas., 2022)

Gestión de eventos y video

Por otro lado, España (2022) señala que “Dado a las grabaciones no deseadas, las cuales no contienen información relevante, se utiliza un software inteligente con funciones integradas, una de ellas como la detección de movimiento de video, y las funciones de administración de video se configuran a través de la interfaz de usuario del dispositivo por seguridad”.

Estandarización

Conformados por estándares abiertos, estos dispositivos de red se pueden integrar de manera fácil en sistemas de datos confidenciales y Ethernet, audio, seguridad y otros equipos digitales. De forma que el ejemplo más eficaz es el video de una cámara web se puede colocar en una caja registradora o al sistema de administración de diferentes áreas de un edificio. (España, 2022)

Escalabilidad y flexibilidad

La videovigilancia IP se va incrementando debido a las necesidades del usuario, estos sistemas tienen la capacidad de compartir datos de red inalámbrica y también, agregar cualquier cantidad de dispositivos de video en red al sistema sin la necesidad de cambiar la infraestructura de la red. (García, 2019)

Importancia de video vigilancia IP

Los criterios más importantes son el acceso remoto, la calidad de imagen, la gestión de video basa en diferentes eventos, almacenamiento, la integración de tecnología, la escalabilidad, la flexibilidad y la rentabilidad. (Nosteal, 2022)

Gracias al acceso remoto facilita a los usuarios previamente autorizados ver los videos en tiempo real desde cualquier punto y en cualquier lapso de tiempo.

Como señala Nosteal (2022) “En términos de resolución de imagen, las cámaras IP son superiores a las cámaras analógicas utilizadas en los circuitos de CCTV. De hecho, las imágenes pueden digitalizarse sin conversión, guardarse y recuperarse en una computadora”.

En resumen, administrar el video mediante un software que incluye características como detección de movimiento, alarmas, conexiones E/S de entrada y salida.

De manera, que existe una gran posibilidad de colocar un determinado número de cámaras IP, tanto inalámbricas como cableadas, facilitando al sistema de video vigilancia sea más escalable y flexible.

Cámara IP

Conocido como un dispositivo el cual graba señales de audio/video digitales y las envía a través de la red a otros dispositivos de red, ya sea como computadoras o teléfonos inteligente. Con las direcciones IP respectivamente, servidores web y los protocolos de transmisión de video correspondientes, gracias a esto los usuarios pueden ver, grabar y administrar video de forma local o remotamente. Facilitando la protección de activos para brindar un sistema más confiable la seguridad. (Colobran, 2022)

Figura 2

Cámara IP TRENDNET TV-IP345PI INDOOR

Nota. Cámara IP modelo TRENDNET TV-IP345PI INDOOR. Tomado de (TRENDnet, 2021)

Imágenes y audio

Como lo hace notar Fernández (2022) "Una cámara IP no envía video, sino que envían el video o las imágenes como datos, además de transmitir una gran cantidad de datos tales como el estado de la cámara, el estado de la conexión, alarmas de entrada o salida para controlar dispositivos externos, unidireccional o bidireccional".

En general, las cámaras IP no requieren un micrófono externo porque están integrados, sin embargo, algunos modelos sí lo necesitan, según los requisitos particulares de la solución que se ofrece." En el caso de una función de portero eléctrico, por ejemplo, tener un micrófono integrado no proporciona una solución ideal ya que, cuando se aloja en un entorno acústicamente ruidoso, el micrófono pierde sensibilidad y funciona de manera inadecuada. En ciertos casos, se utiliza un micrófono externo que se conecta a la cámara por separado, pero utiliza su canal de transmisión de audio". (FERNÁNDEZ, 2022)

Componentes de Cámara IP

Internos

Los componentes que forman parte de una cámara IP se describen en términos muy generales, variando en consecuencia el precio y la funcionalidad adicional que se puede proporcionar al cliente o usuario. Consta de un lente, un sensor de imagen, un procesador de imagen, chip de compresión de video y un chip Ethernet de red. (Redatel S.A.S., 2016)

Externos

Una cámara IP tiene básicamente los siguientes componentes que permiten configurarla en un sistema de CCTV. (Colobran, 2022)

Una cámara fija, como sugiere el nombre, es una cámara que se fija frente a un objeto y es ideal para operaciones al aire libre en puntos de interés o considerados importantes en una ubicación particular. Así mismo, la cámara de red domo fija, igual que una cámara fija, pero en

una carcasa resistente al vandalismo que se monta en el techo de forma predeterminada. Sus principales características son discrecional y tolerante a las manipulaciones a las que pueda ser objeto.

Especificaciones de cámaras IP

- Procesador de 32 bits con RSCIS integrado
- Protocolos: TCP/IP, UDP, IMCP, SMTP, HTTP, FTP, DHCP Y PPPoE
- Formato de archivo comprimible M-JPEG
- Wifi integrado
- Control de movimiento ajustable de 270 horizontalmente y 120 verticalmente
- Audios de dos canales
- Sensor CMOS de colores ¼
- Distancia de visión nocturna de 5 a 10 metros
- Configuración de red LAN/WAN/Internet
- Captura y grabación en tiempo real y remotamente
- Detección de movimiento
- Alertas de E-mail
- Encriptado wifi web, wpa y wpa2 y estándar wifi 802.11b/g

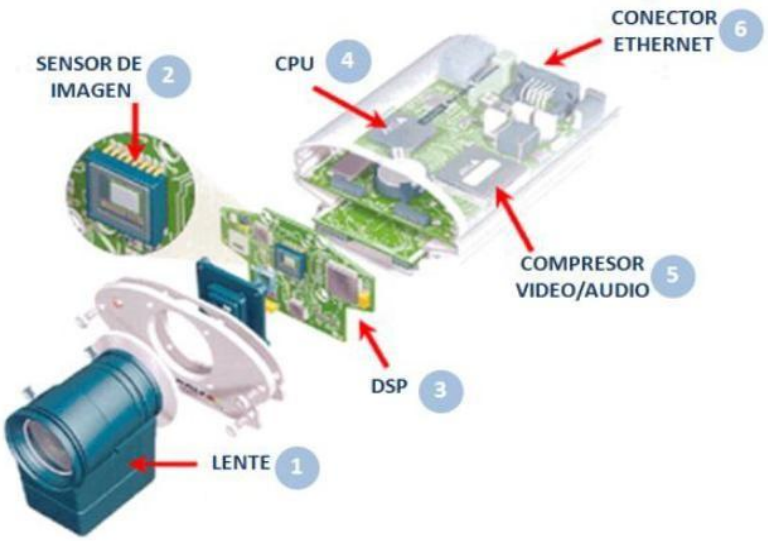
Aplicabilidad de las cámaras IP

A la hora de implementar un sistema de videovigilancia con cámaras IP, tenga en cuenta que el prototipo puede incluir vigilancia en tiempo real, vigilancia por alarmas, análisis de imágenes y, posiblemente, dispositivos de almacenamiento de video. (Juan, 2018)

Partes de una cámara IP

Figura 3

Partes de una cámara IP



Nota. Elementos que componen una cámara IP. Tomado de (Martí, 2013)

Lente

En videovigilancia, la lente es el ojo de todo el sistema, también es parte fundamental de la calidad de la imagen, la lente puede ser de los siguientes tipos: Solo un campo de visión es fijo, porque la distancia focal es fija, muestra diferentes campos de visión cambiables ópticamente, por lo que hay un rango de distancia focal, ver el campo se puede regular manualmente, la distancia focal es entre 3 y 8 mm, el zoom consta de una distancia focal variable, si se cambia el campo de visión, no es obligatorio volver a centrar la lente, este tipo de lente puede tener una distancia focal entre 6 y 48 milímetros. La distancia focal larga facilita la observación de un campo de visión más pequeño, pero más detalladamente, mientras que una distancia focal corta le permite observar un campo de visión más extenso pero menos detalle. (FERNÁNDEZ, 2022)

Sensor de imagen

Las cámaras digitales utilizan dos tipos de sensores. Un CCD o CMOS que consisten básicamente en un semiconductor de óxido de metal (MOS) distribuido en una matriz que actúa para almacenar carga en cada celda. de la matriz se llama píxel, la cantidad de luz que cae sobre cada píxel determina el peso de la carga respectivamente, tamaño del sensor el cual se mide de manera diagonal, por lo que puede ser 1/4, 1/3, 1/2 o 2/3. Los sensores CCD, el amplificador es externo y común a todas las celdas, mientras que en los sensores CMOS, el amplificador es de forma interna a cada celda correspondiente.

Procesador de imagen

Una vez que el sensor trasforma la imagen a formato digital, la imagen es envía al procesador de imágenes para su proceso correspondiente y luego se envía a una etapa de compresión para obtener una mejor resolución de la imagen enfocada.

CPU

La CPU de una cámara IP consiste en un procesador basado en Linux que controla y administra las funciones y los procesos internos de la cámara, como la compresión, distribución de imágenes y el manejo de alarmas.

Etapa de compresión

Este es un paso de gran importancia en él envió de imágenes y videos sobre redes IP, para que las redes no se saturen durante sus respectivos periodos de uso. Por lo tanto, el estándar H.264 proporciona una resolución de video más alta que los dos estándares anteriores con la misma tasa de bits y ancho de banda. (Sarabia Buñay, 2018, pág. 33)

Tarjeta Ethernet

El chip ethernet de una cámara IP es el encargado de proporcionar conectividad de red para que las imágenes capturadas puedan transmitirse a través de la red. De igual manera la

tarjeta ethernet proporciona un alto rendimiento del equipo ya que a través de los cables ethernet la red suele ser mucho más potente. (Martí, 2013)

Características de una cámara IP

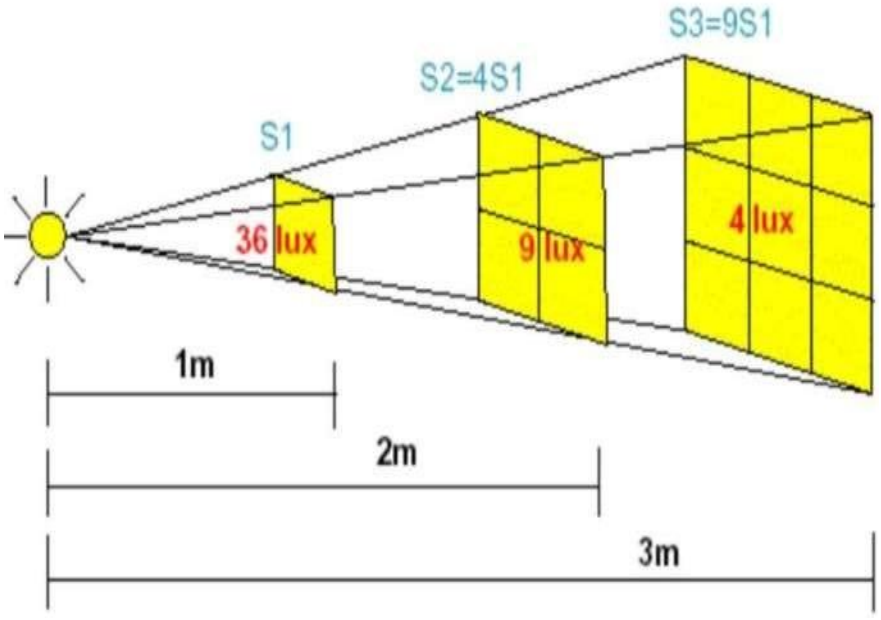
Del mismo modo para la elección de las cámaras IP, es de gran importancia tener en cuenta otros detalles sumamente importantes sobre estos dispositivos los cuales se describirán a continuación:

Sensibilidad

Como señala Sarabia Buñay (2018) “La sensibilidad consiste en la intensidad de luz necesaria para trabajar en condiciones de baja calidad de iluminación, de forma que el valor de lux será menor a mayor sensibilidad y se mide en LUX”.

Figura 4

Sensibilidad de luz



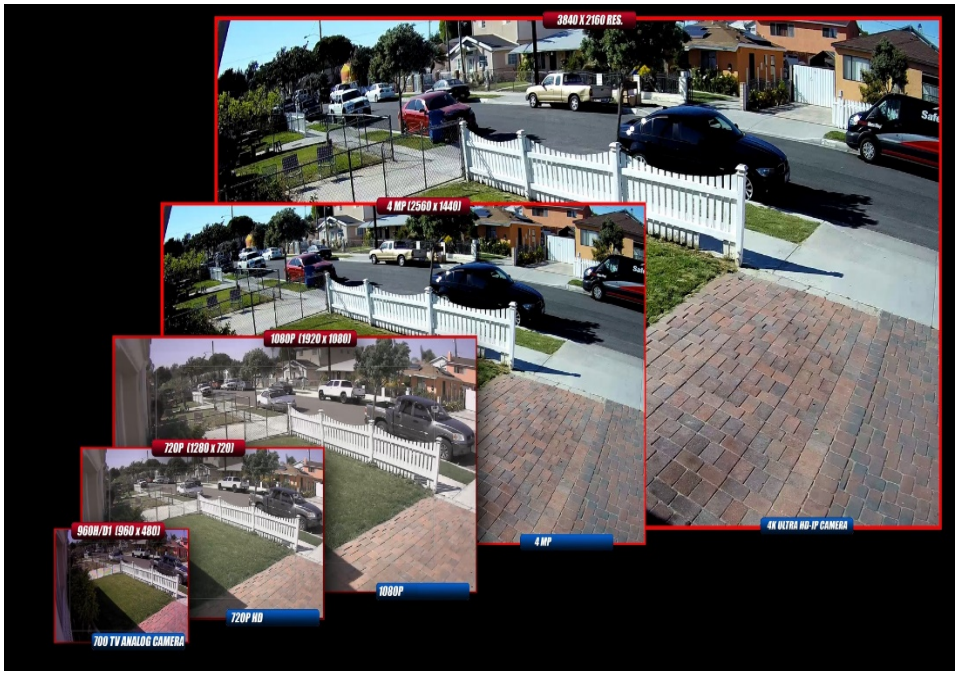
Nota. La figura representa la iluminación que existe entre la fuente de luz y la superficie iluminada. Tomado de (Sarabia Buñay, 2018)

Resolución

La resolución se mide en pixeles, los pixeles de una cámara web deben medirse horizontal y verticalmente. Cuanto mayor sea el número de píxeles, mayor será la resolución de la imagen que genera la cámara IP.

Figura 5

Resolución en megapíxeles de una imagen



Nota. La figura muestra la resolución de imagen en megapíxeles de una cámara. Tomado de (ARGSEGURIDAD, 2017)

Conmutación

En distintos sistemas de videovigilancia IP, las cámaras diurnas y nocturnas presentan diferentes funcionalidades es decir durante el día captan las imágenes a color y cambian a funcionamiento en blanco y negro durante la noche para aumentar la sensibilidad y resolución. (Sarabia Buñay, 2018)

Compensación de contra luz (BLC)

Una cámara habilitada para BLC analiza la escena digitalmente o manualmente en algunos modelos permitiendo ajustar automáticamente el brillo y el contraste de la imagen para hacer que las áreas oscuras sean más claras. (Sanchez, 2022)

Ajustes de blancos

Esto es muy importante porque la cámara necesita tener una referencia de blanco para que los demás colores tengan el tono correcto, podemos decir, que también hay correcciones de color blanco, por ejemplo: AWC es automático solo si se hacer la configuración adecuada y ATTW automático el seguimiento se hace a menudo. (Sarabia Buñay, 2018)

Control automático de ganancia

Básicamente, es el circuito electrónico responsable de mantener la señal de video en un nivel adecuado para ver y grabar la imagen grabada. Esto es especialmente útil para cámaras con poca luz.

Hutter

Este es un circuito electrónico en el sensor de muchas cámaras CCD que ayuda a aumentar el tiempo de exposición y, a menudo, aumenta la sensibilidad de la cámara.

Tipos de cámaras IP

Cámara IP fija

El campo de visión es fijo y el ángulo en el que se coloca también es fijo. Bueno, si quieres ver la cámara claramente. De modo que estos tipos de cámaras se pueden instalar en una variedad de ubicaciones, ya que están diseñadas para uso en interiores o exteriores.

Cámara IP domo fija

Este tipo de cámara también se denomina mini domo porque es una cámara fija remontada en una pequeña carcasa domo, por lo que tiene un diseño discreto. Esta cámara se basa en enfocar un punto seleccionado en cualquier dirección. Una de sus ventajas es la invencibilidad. Sin embargo, no hay lentes intercambiables, y cuando se trata de la selección de lentes, el pequeño espacio dentro de la carcasa del domo limita la selección de lentes.

Su diseño es resistente a los impactos y por tanto tiene un grado de protección IP66. donde IP es el grado de protección. Los primeros 6 dígitos brindan protección contra el ingreso de personas y polvo, mientras que los siguientes 6 dígitos protegen contra chorros de agua omnidireccionales.

Cámara IP PTZ (Pan tilt-zoom)

Se puede mover horizontal o verticalmente, se puede hacer zoom dentro del área y se puede ajustar de forma manual o automática, por lo que se utiliza principalmente en grandes espacios o superficies.

Cámara IP domo PTZ

Estas cámaras le permiten cubrir un área más amplia, brindándole más flexibilidad para el desplazamiento y hacer zoom continuamente 360 grados en horizontal y 180 grados en vertical. Su diseño lo hace muy útil para instalaciones discretas. Su función es la operación continua, ya que la cámara se mueve automáticamente de un preset a otro, y se pueden programar hasta 20 rondas de vigilancia. (SAQUIRAY, 2018)

Figura 6

Tipos de cámaras IP

Nota. La figura muestra los tipos de cámaras IP. Tomado de (García, 2019)

Cámaras Full Color

Características principales

- Monitoreo a color 24/7: Presenta imágenes en color y captura detalles vividos en condiciones de poca luz.
- Excelente calidad de video en oscuridad: Proporciona una luz auxiliar cálida e inteligente para garantizar la claridad de la imagen incluso en la oscuridad total.
- Mayor precisión de IA por la noche: Filtra falsas alarmas y permite que la clasificación de personas y vehículos se centre solo en el objetivo de interés.

Inteligencia Artificial

La inteligencia artificial es la capacidad que tienen distintos dispositivos tecnológicos para exhibir habilidades similares a las humanas, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planificación. Así mismo permite que los sistemas técnicos perciban y se relacionen con su entorno, resuelvan problemas y actúen con un propósito. de tal manera que los equipos reciben datos preparados o recopilados por sus propios sensores, una de ellas son las cámaras, los procesan y responden. (Parlamento Europeo, 2020)

Importancia de la inteligencia artificial

La IA permite la automatización de procesos que normalmente se harían manualmente, lo que garantiza que los procesos sean más eficientes, Además, permite la optimización de productos, la planificación de inventarios, los procesos logísticos y más. Sin embargo, aún se necesita investigación humana para configurar correctamente el sistema y mantener la inteligencia artificial realizando un aprendizaje óptimo. (CTA, 2021)

Beneficios de las soluciones con tecnologías IA

- Acelera las instalaciones
- Ahorrar esfuerzo
- Reduce complicaciones
- Aumenta la satisfacción del cliente

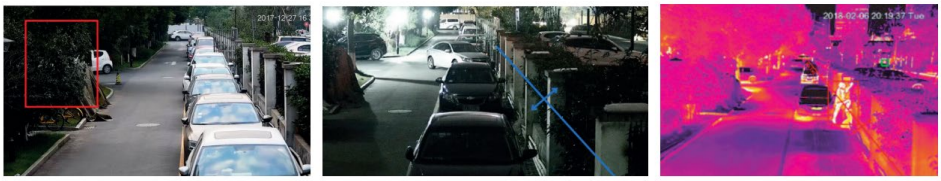
Protección perimetral

Se realizan análisis adicionales de los comportamientos o eventos observados, se clasifican objetivos humanos y de vehículos, y se eliminan automáticamente las falsas alarmas debido a factores como animales, hojas que se balancean, luces brillantes, lluvia, nieve y otros factores, lo que mejora en gran medida la precisión de las alarmas. Además, las cámaras PTZ

pueden acercarse a los objetos y desplazarse alrededor de ellos para obtener más detalles. (ICO INTERNACIONAL S.A., 2020)

Figura 7

Protección perimetral



Nota. Protección perimetral de diferentes lugares captados por el equipo. Tomado de (ICO INTERNACIONAL S.A., 2020)

Reconocimiento Facial

Cuando ingresa una imagen o video, puede usar la función de reconocimiento de rostros para ver si hay algún rostro presente, una vez que se extraen las crestas faciales extraídas de los rostros capturado, se modela el rostro humano. Para ser identificado, cada modelo facial se compara con modelos faciales conocidos almacenados en la base de datos. (ICO INTERNACIONAL S.A., 2020)

Figura 8

Reconocimiento facial

Nota. La figura representa la identificación de clientes, persecuciones, asistencias, control de ingresos, control de visitantes entre otros. Tomado de (ICO INTERNACIONAL S.A., 2020)

Recuento de personas

Calcula el número de personas que entran, salen o pasan por un área determinada durante un período de tiempo determinado después de filtrar objetivos no críticos en la zona.

Figura 9

Recuento de personas

Nota. la cantidad de personas que ingresan salen o pasan por un área específica durante un periodo de tiempo específico. Tomado de (Acosta, 2015)

ANPR

ANPR (reconocimiento automático de matrículas) tecnología que utiliza el reconocimiento óptico de caracteres en imágenes para permitir que ANPR lea las matrículas de los vehículos con alta precisión. Este tipo de aplicaciones ANPR incluye monitoreo y seguridad del tráfico, medición de velocidad y estacionamiento y control de ingreso. (Dahua Technology, 2021)

Figura 10

Reconocimiento automático de número de placa

Nota. Son aplicaciones colocadas para la conexión de puertas y recuperación de vehículos basado en el respaldo de ANPR. Tomado de (Dahua Technology, 2021)

Medios de transmisión

Se considera como un canal a través del cual viaja la señal que transmite información desde el emisor y llega al receptor. Actualmente, gracias a las investigaciones realizadas, los sistemas de comunicación pueden utilizar una gran variedad de tecnologías, lo que permite elegir uno u otro medio en función de los requisitos de facilidad de instalación y capacidad de soportar diferentes tecnologías a nivel de enlace.

Gracias al desarrollo de la tecnología de telecomunicaciones y las demandas de los usuarios de más acceso a más ancho de banda, hoy en día se ha inventado una amplia gama de medios de transmisión, tanto por cable como inalámbrica. En el campo de los medios de transmisión alámbricos se pueden encontrar desde el cable telefónico, pasando por el cable coaxial y el par trenzado, hasta la invención de fibra óptica de vidrio o de plástico.

Figura 11

Tipos de conexiones a internet

Nota. La figura representa algunos modos de acceder al internet usando diferentes dispositivos. Tomado de (SANTANA HERNANDEZ, 2021)

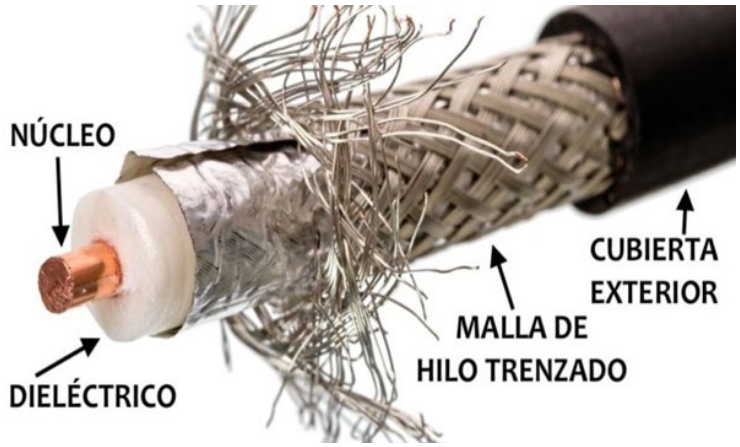
Por otra parte, en el campo de los medios de comunicación inalámbricos el medio que se sigue usando es sin duda alguna la atmosfera, aquí solo se ha evolucionado en cuanto al tipo de tecnología usada, empezando por el Bluethooth, el wifi, Wimax, hasta el Life, entre otras.

Cable coaxial

Un cable coaxial consta de cinco capas que se fusionan para formar un cable cilíndrico, desde el centro hacia afuera, que consta de un solo alambre de cobre rodeado por un polímero de bajo grado que actúa como aislante, láminas delgadas de aluminio, una malla metálica como el exterior. un conductor con plástico colocado en el extremo como revestimiento o protección.

Figura 12

Cable coaxial



Nota. La figura muestra las partes que compone un cable coaxial. Tomado de (Etecé, 2021)

El cable coaxial es uno de los primeros medios de transmisión que se utilizó, se espera que su popularidad continúe, por tal razón aún se encuentran en uso los siguientes:

Tabla 1

Uso del cable coaxial

USOS DEL CABLE COAXIAL	
Circuitos cerrados de videovigilancia	Se emplea en la conexión de cámaras dentro de un circuito cerrado de vigilancia
Entre el cable y Modem	Son conexiones basado en una combinación de cables coaxiales y otros tipos de cables.

USOS DEL CABLE COAXIAL

Distribución de señal de televisión	Ya sea en televisión analógica, digital o satelital, para llevar la señal desde la antena hasta en decodificar y luego hasta el televisor, se usa cable coaxial

Nota. La siguiente tabla muestra los usos más comunes del cable coaxial. Tomado de (Vásquez, 2015)

Cable par trenzado

Sin duda, estos cables son los soportes de datos físicos más populares, ya que se utilizan ampliamente en los sistemas de comunicación modernos y, más comúnmente, en redes de datos como las computadoras. Para explicar mejor la construcción o la forma en que se construye el par trenzado, dos hilos de cobre u otro material conductor se trenzan o se trenzan juntos, combinados de manera simplificada para reducir los efectos electromagnéticos y la diafonía.

Tipos de cable par trenzado

UTP (Unsshielded twisted pair) (Par trenzado sin apantallar)

Esta formados por un par de hilos aislados y trenzados entre sí, el cual no constan de ningún tipo de recubrimiento metálico que lo proteja frente a interferencias electromagnéticas o diafonías. Su costo económico es muy bajo, es fácil de manejar y su peso es reducido lo que lo

convierte en un elemento fácil de instalar tanto en interiores como en exteriores donde no es recomendado ya que su exposición al medio lo destruiría rápidamente. (RNDS, 2021)

Sin embargo, aunque mejora la inmunidad de línea abierta a las emisiones de ruido y diafonía, es relativamente sensible a estos y otros fenómenos. Hoy en día se pueden encontrar ocho tipos de cables, cuanto mayor sea el número de categoría, mejor protegidos y más duraderos son. (RNDS, 2021)

Figura 13

Cable de red UTP

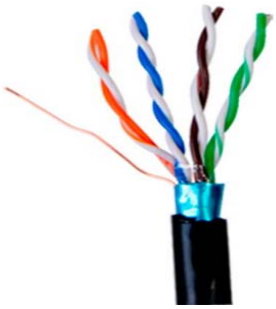
Nota. Cable par trenzado sin apantallar. Tomado de (Arango, 2021)

FTP (Foiled Twistwd Pair, par trenzado con pantalla)

Este tipo de cables de par trenzado brindan una mayor protección, los 4 pares de cables se recubren en conjunto con una capa de plástico o cualquier otro material que actúe como aislante y se remata con otra capa metálica que se encarga de evitar interferencias eléctricas. Ciertamente no es el tipo de cable más ideal, pero es una mejora con respecto a los cables UTP.

Figura 14

Cable de red FTP



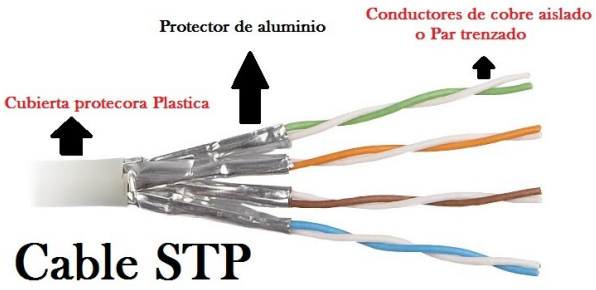
Nota. La figura representa la protección que presenta el cable con el blindaje plástico y metálico que recubren los pares de cables. Tomado de (Castillo, 2019)

STP (Shielded Twisted Pair, par trenzado apantallado)

Este tipo de cable cada par de cables tendrá una cubierta metalica diseñada para su protección. Presentan mejores prestaciones por lo cual están destinadas a ser usadas en redes donde se requiere mayor robustez en la seguridad, por lo que permiten instalaciones a mayores distancias sin causar muchas pérdidas presentan un mayor costo económico.

Figura 15

Cable de red STP



Nota. Cable par trenzado con apantallado individual para cada uno de los pares. Tomado de (Castillo, 2019)

SFTP (Screeened Foiled Twisted Pair) (Laminado apantallado individual)

El cable SFTP se basa o toma como referencia a la estructura del cable FTP, pero con cambios sumamente importantes. En este sentido, se ha mejorado el blindaje y se ha añadido un laminado de malla metálica LSZH libre de halógenos de baja emisión de humos que cubre los cuatro pares de cables para una protección adicional.

Figura 16

Cable de red SFTP

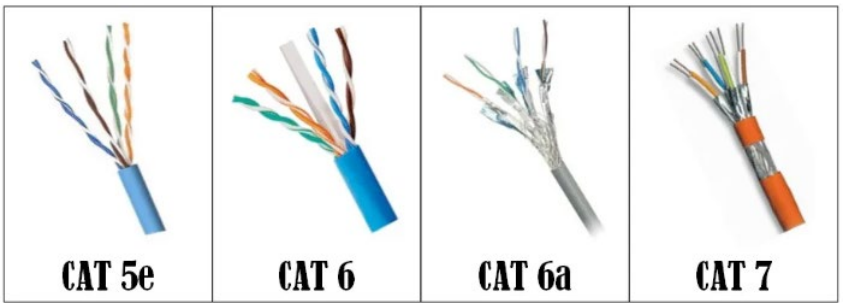
Nota. el siguiente cable posee una guía plástica ubicado en el centro y su respectivo apantallado metálico. Tomado de (Castillo, 2019)

Categorías de cable par trenzado

Cada vez los usuarios de las redes requieren de mejores velocidades de navegación y mayor seguridad en sus redes, es por esto que se han creado a lo largo de la historia diferentes tipos de cables mejorando sus características, mismo que se han organizado por categorías.

Figura 17

Categorías de cables par trenzados



Nota. en la siguiente grafica podemos observar cuatro categorías de cable que se utilizan.

Tomado de (Telectronika, 2018)

Tabla 2

Categorías de cable par trenzado

Categoría	Velocidad de envió	Frecuencia	Velocidad de Descarga
ethernet cat 5	100 Mbps	100 MHz	15,5 MB/s
ethernet cat 5e	1000 Mbps	100 MHz	150,5 MB/s
ethernet cat 6	1000 Mbps	250 MHz	150,5 MB/s
ethernet cat 6a	10000 Mbps	500 MHz	1.250 MB/s ó 1,25 GB/s
ethernet cat 7	10000 Mbps	600 MHz	1,25 GB/s

Categoría	Velocidad de envió	Frecuencia	Velocidad de Descarga
ethernet cat 7a	10000 Mbps	1.000 MHz	1,25 GB/s
ethernet cat 8	40000 Mbps	2000Mhz	5 Gb/s

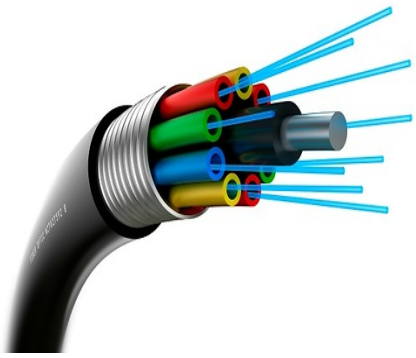
Nota. La siguiente tabla representa las categorías del cable ethernet, junto con sus respectivas características, como velocidad de transferencia, frecuencia y velocidad de descarga respectivamente. Tomado de (ELPA, 2019)

Cable de fibra óptica

La fibra óptica es un medio de transmisión por cable que transporta un haz de luz a través de una fuente de luz láser o LED el cual es introducido en un extremo del cable. Cuando se introduce el haz de luz, esta queda retenida en su parte interior o núcleo evitando así que se escape de la fibra y pueda viajar largas distancias a velocidades mayores que la que pueden alcanzar sus homólogos. (Chan García, 2020)

Figura 18

Cable de fibra óptica



Nota. En la figura visualizamos el cable de fibra con varios hilos. Tomado de (Chan García, 2020)

Este medio de transmisión, al igual que los cables pares trenzado y los cables coaxiales, está formado con sus respectivas protecciones las cuales son el núcleo o core, el revestimiento o cladding y la cubierta o buffer.

Núcleo o Core

Está ubicado en el centro, es la parte más pequeña en dimensión del diámetro el cual mide de 8 a 12,5 micrómetros, es por donde viaja el haz de luz de forma confinada y rebotando en las paredes sin poder escaparse gracias a la diferencia de densidades que tienen el núcleo con respecto al revestimiento.

Revestimiento o Cladding

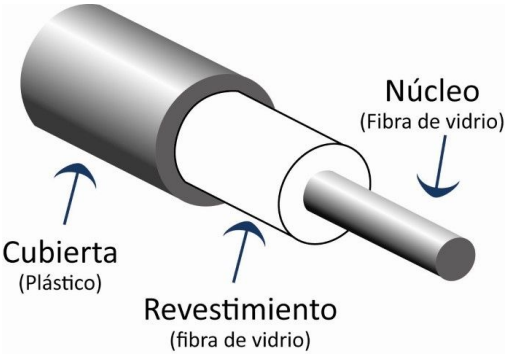
Esta capa, tiene como objetivo primordial el no permitir que el haz de luz que viaja por la fibra se escape del núcleo. Su diámetro es superior al del núcleo y va desde los 62.5 a los 125 micrómetros.

Color o coating

Está formada por un material plástico o polímero, cuya misión es la de proteger al núcleo y al revestimiento de posibles daños ocasionado por el manejo o manipulación de la fibra durante la instalación, además de acuerdo al color que se le asigne, en ocasiones donde existen múltiples cables de fibra óptica, como un diferenciador. Su diámetro es de 245 micrómetros.

Figura 19

Partes de un cable de fibra óptica



Nota. La imagen representa de cómo está formado internamente el cable de fibra óptica. Tomado de (Ordoñes, 2015)

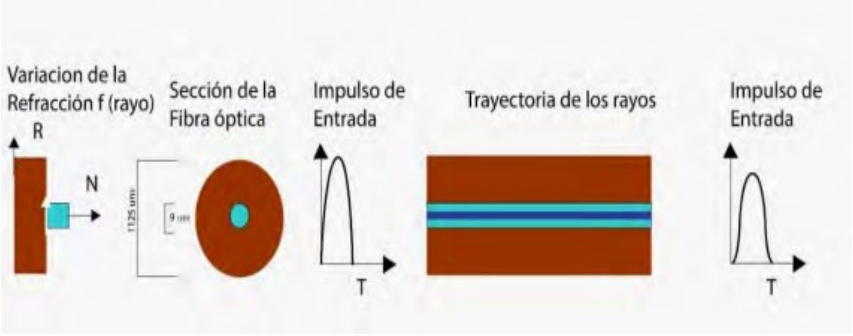
Tipos de fibra óptica

Monomodo

Posee un núcleo de diámetro muy pequeño lo cual permite que los rayos de luz viajen por un solo trayecto, eliminan la dispersión modal por lo que es apta para transmisiones a altas velocidades a distancias mayores.

Figura 20

Fibra óptica monomodo



Nota. Funcionamiento de fibra monomodo y como viaja un haz de luz por el núcleo. Tomado de (Chan García, 2020)

Multimodo

Los rayos de luz generados por la fuente viajan dentro de la fibra a por diferentes trayectos lo cual produce dispersión modal el cual consiste en el ensanchamiento del pulso final con respecto al inicial, es por esto que se usa para distancias menores a los 4 kilómetros y además por que las velocidades de transmisión en comparación con las aceptadas por la fibra monomodo son mucho menores. El diámetro del núcleo es de 50 a 62,5 micrómetros.

Figura 21

Fibra óptica multimodo

Nota. La figura representa la forma en que viajan los haces de luz por el núcleo, así mismo permite varias rutas para la luz. Tomado de (Chan García, 2020)

Codificador de video

En los sistemas de videovigilancia, los codificadores de video permiten la migración de sistemas de video analógicos a sistemas de video en red. Esto garantiza que no se excluya la infra estructura existente para la video vigilancia analógica. Finalizado el proceso el codificador de video se conecta a la cámara análoga con un cable coaxial, convirtiendo en un video digital que posteriormente será enviado por la red.

Figura 22

Codificador de video

Nota. Se observa una red de video vigilancia utilizando un codificador de video permitiendo obtener el video en la red. (Axis Communications, 2019)

Con la introducción de este codificador de video, los NVR y VCR se volvieron innecesarios ya que requieren un computador para grabar y ver el video digital. De manera que, se puede acceder y controlar de forma remota a cada cámara de análisis de video a través de una red.

Grabación y almacenamiento

Cuando se trata de procesamiento de información, la grabación y el almacenamiento es una parte esencial de cualquier sistema de videovigilancia. Por lo tanto, los principales tipos de almacenamiento son:

- Almacenamiento interno de la cámara: estos equipos contienen una memoria interna tarjeta SD o memoria USB, en el que se puede grabar un determinado periodo de tiempo.

- Almacenamiento en computadora: Este tipo de almacenamiento es adecuado para sistemas pequeños, porque los registros de las grabaciones se almacenan en el disco duro de la computadora.
- Almacenamiento NVR**:** Similar a un disco duro, pero es un grabador de video en red de alta resistencia, por lo que está hecho principalmente para instalaciones robustas. Puede conectar un monitor al NVR para ver las imágenes captadas de igual forma, usar un teclado para controlar la panorámica y zoom desde la grabadora. Del mismo modo, el NVR requiere de una IP fija para conectarse a internet. (Terabyte, 2020)

Además del almacenamiento, la grabación también juega un papel importante. Porque sus funciones incluyen monitorear la cámara o controlar el zoom, obtener una copia de la grabación, conectarse a Internet y controlar remotamente todas las funciones. Desde el punto de vista estas imágenes también se pueden tomar en diferentes modos, se realizan las siguientes configuraciones de acuerdo a las necesidades del usuario:

- Grabación continua**:** La grabación es siempre en tiempo real.
- Grabación programada: La grabación inicia de acuerdo a los periodos de tiempos programados.
- Grabación por eventos: La grabación comienza tan pronto como se detecte movimiento.

Así mismo la capacidad de almacenamiento que genera el equipo se basa por la cantidad de cámaras en su respectiva instalación, resolución, fotogramas por segundo, método y factor de compresión y tiempo total de grabación en días. Y la alarma en porcentaje, el cual es la cantidad total de su tiempo de grabación. (Sarabia Buñay, 2018, pág. 22)

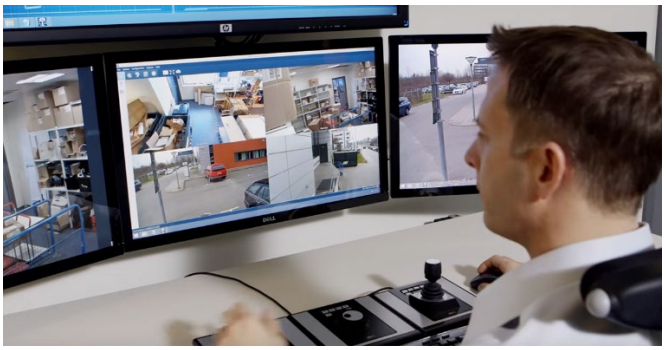
Software de gestión de video

En cualquier sistema de videovigilancia es importante instalar un software especial que le permita administrar, monitorear, gestionar eventos y configurar dispositivos que están

integrados en el NVR e instalados en la computadora personal del usuario autorizado, por ejemplo, al no tener integrado el software en el mismo elemento de Red, para acceder a las configuraciones del dispositivo simplemente ingresamos la dirección IP del dispositivo, se usa solo para sistemas con una pequeña cantidad de cámaras instaladas en una computadora que controla, administra y almacena imágenes. (Sarabia Buñay, 2018, pág. 22)

Figura 23

Software para la gestión de video



Nota. Este tipo de aplicaciones se encuentran diseñados para el monitoreo y administración de equipos de videovigilancia. Tomada de (usecim, 2022)

Audio

Una parte muy importante de los sistemas de videovigilancia es el audio, que permite investigaciones más específicas y poder controlar actividades ilegales, pero tiene una cierta desventaja que aún no se ha extendido al campo de la videovigilancia. Además del campo de visión de la cámara, el audio puede cubrir un rango de 360 grados para mayor cobertura. (Sarabia Buñay, 2018, pág. 23)

Modos de transmisión del audio

- Simplex: El audio se lo envía en una sola dirección.
- Semidúplex: El audio se transmite de manera secuencial en ambas direcciones.

- Full Dúplex: El audio es enviado y recibido simultáneamente por el operador.

Compresión de video.

Para una transmisión y un almacenamiento eficientes, la señal analógica debe convertirse en audio digital a través de un proceso de muestreo y comprimirse para reducir el tamaño. (Axis Communications, 2019)

Video

En un sistema de videovigilancia, el video grabado puede contener información innecesaria que no es de mucha utilidad para los administradores. Por lo que esta información debe ser eliminada mediante compresión de video.

Compresión de video

Se trata de eliminar información no requerida de los datos almacenados para reducir el tamaño del video, manteniendo la calidad de imagen para enviar por red y guardar nuevamente con menos peso. (Pérez Vega, 2019, pág. 3)

Estándares de compresión

Básicamente los estándares de compresión nos ayudan a reducir el tamaño de los datos, sin perder la calidad de imagen, pero en cierta forma si se reduce mucho puede afectar su calidad, esto se basa de acuerdo al modo de compresión que se utilice, entre las cuales se detallan a continuación:

- Motion JPEG: Basada en una secuencia de video digital que consta de una serie de imágenes JPEG únicas, cuya ventaja es el uso de imágenes fijas.
- MPEG-4: Compatible con aplicaciones que solicitan imágenes de alta calidad con bajo ancho de banda.
- H.264: Su objetivo esencial consta en la reducción del peso de los archivos de video digital en más de 80% por archivo. (Sarabia Buñay, 2018, pág. 24)

Sincronización audio y video

Esta sincronización se realiza mediante el uso de un reproductor multimedia. El audio y el video se envían a través de la red como paquetes individuales, lo que permite al usuario reproducir tanto el audio como el video en perfecta sincronización. Los formatos más utilizados son MPEG-4 o H.264.de hecho, las transmisiones de audio y video se envían a través RTP (Red Time Protocol). (Sarabia Buñay, 2018, pág. 24)

Red inalámbrica

Es una red que permite que varios dispositivos se comuniquen o compartan información si la necesidad de una conexión cableada, una de las ventajas más sobresalientes de las redes inalámbricas son la capacidad de los usuarios de permanecer conectados a la red mientras permanezcan en un área determinada. La red inalámbrica no utiliza cableado estándar, está basado mediante ondas electromagnéticas de la red “infrarrojas o de radio” así mismo, se basan en conexiones que diferencien en la frecuencia de transmisión, velocidad o el enlace. (Salazar, 2016, pág. 7)

Figura 24

Red inalámbrica

Nota. La figura representa la conexión de otros dispositivos a la red inalámbrica médiate el WIFI. Tomada de (Tecnología Informática, 2021)

Tipos de redes Inalámbricas

Redes WPAN

Son redes de corto alcance, cubren áreas de solo algunas decenas de metros, ofrecen menos cobertura y, además:

> “Estas redes de área personal inalámbricas son basadas en el estándar IEEE 802.15. Estas redes inalámbricas les servirán a los clientes para comunicarse en distancias muy cortas, aproximadamente en una forma ideal unos 10 metros. La conexión WPAN no requiere infraestructura ni una conexión directa fuera de un canal fijo. Por lo tanto, puede crear soluciones pequeñas, económicas y de bajo consumo que se pueden colocar en varios dispositivos inteligentes. Un ejemplo claro de esta tecnología es Bluetooth el cual permite conexiones con poco alcance”. (Salazar, 2016, pág. 9)

Redes WLAN

Estas redes corresponden a áreas de la red local de una compañía con un alcance de aproximadamente 100 metros. Igualmente:

> “Están diseñadas para brindar acceso sin la necesidad de usar cables, se utilizan principalmente en el hogar, la escuela, el laboratorio de computación o en las oficinas. Esto brinda a los usuarios la capacidad de moverse dentro de su área de cobertura local mientras permanecen conectados a la red. Las WLAN se venden bajo la marca WiFi y se basan en el estándar IEEE 802.11. Debido a la competencia, entre otros estándares, hiperLan nunca ha tenido un uso comercial tan extendido. El estándar IEEE 802.11 fue el más fácil de implementar y se comercializo más rápido para los usuarios”. (Salazar, 2016, pág. 13)

Redes WMAN

Las redes inalámbricas metropolitanas forman el tercer grupo de redes inalámbricas. WMAN es basado en el estándar IEEE 802.16, a menudo llamado WIMAX. La tecnología WIMAX está basada en la arquitectura punto a multipunto creada para facilitar la transmisión de datos a alta velocidad sobre redes inalámbricas de área metropolitana. (Salazar, 2016, pág. 14)

Esto permite que las LAN inalámbricas pequeñas se interconecten a través de WIMAX para crear una WMAN grande. Las redes interurbanas se pueden construir sin costosos cableados. (Salazar, 2016, pág. 14)

Redes WWAN

Las redes inalámbricas de área amplia logran alcanzar en condiciones ideales una distancia superior de los 50 kilómetros y suelen utilizar frecuencias con licencia, es decir que requieren que se requiere de un permiso y costo económico para poder usar. Este tipo de red se usa en grandes áreas como ciudades o países debido a los diferentes sistemas satelitales o posiciones de antenas proporcionadas por diferentes ISP. Ejemplo más claro e importante en la actualidad de este tipo de redes son la telefonía celular y los servicios satelitales. (Salazar, 2016, pág. 15)

Figura 25

Tipo de redes inalámbricas

Alcance de las Diferentes Conexiones Inalámbricas

+

Nota. la siguiente figura representa los cuatro tipos de redes inalámbricas que se utiliza en la actualidad. Tomado de (redesinalambricas, 2017)

Normativas

Las normativas son el conjunto de reglas que se deben cumplir para realizar una determinada actividad, esto tiene como finalidad que los procesos se estandaricen y poder trabajar así de forma globalizada.

EIA/TIA 568A

Esta norma identifica los requisitos que se deben implementar, y en este caso se centra en el tema de construir, diseñar y la gestión de un sistema de cableado estructurado. Establecen además una herramienta fundamental en el campo de las conexiones de redes o planeación e implementación del cableado de una red. Además, los extremos del cable UTP ya sean estos de la categoría 5 o categoría 6, que llevaran conectores RJ45 con un orden de colores especificados por la norma los cuales, partiendo desde la izquierda hacia la derecha, blanco verde-blanco-blanco naranja-azul-blanco azul-naranja-blanco marrón- marrón. (Castellón Arenas, 2014)

EIA/TIA 568B

Esta norma es apropiada para cualquier práctica específica del diseño de cableado estructurado en el centro de datos. Tiene tres subcategorías: ANSI/TIA/EIA 568-B1, TIA/EIA 568-B2 y TIA/EIA 568-B3. (Castellón Arenas, 2014)

Wifi (Wireless fidelity)

Su acrónimo es Wireless Fidelity, también conocido como Red de Área Local. La transmisión inalámbrica es por ondas de radio con buena calidad de radiación, y la distancia corta puede alcanzar los 100 m, lo cual está estandarizado por IEEE. Es necesario una antena

integrada en la etiqueta para transmitir la señal, y las ondas de radio pueden atravesar obstáculos, por lo que no es necesario que el transmisor y el receptor estén uno frente al otro.

Estándar IEEE 802.11

El estándar IEEE 802.11 es un conjunto parámetros desarrollado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) enfocado a regular la gestión o implementación de redes inalámbricas.

Figura 26

Estándares IEEE 802.11

Nota. Estándares IEEE 802.11 y sus variantes para el wifi. Tomado de (RedesInalambricas, 2020)

Estándar 801.11a

“La primera carta siguió a la aprobación del estándar 802.11 en junio de 1997 para operar en la banda de frecuencia de 5 GHz con una tasa de transferencia de datos de hasta 54 Mbps". (Ros, 2021)

Estándar 802.11 b

"Fue lanzado en septiembre de 1999 y permitió que computadoras que tenían este estándar operaran a 2,4 GHz y permitieran velocidades de hasta 11 Mbps. Curiosamente, este estándar es el sucesor del 802.11a que era antes". (Ros, 2021)

Estándar 802.11 g

Este estándar fue autorizado par a publicarse en junio de 2003, siendo el sucesor del estándar 802.11b, alcanzando una velocidad de más de 54 Mbps en banda de transmisión de 2.5 GHz.

Estándar 802.11 n

Este estándar fue el primero en ser creado de forma específica para la tecnología MIMO que implementa el poder trabajar dentro de un equipo con dual band, Eso significa que puede trabajar en las bandas de 2,4 GHz y 5 GHz a velocidades de hasta 600 Mbps.

Estándar 802.11ac

Fue estandarizado a fines de 2013 y opera solo en la banda de frecuencia de 5 GHz. El objetivo es brindar mayor velocidad en la red inalámbrica, la misma velocidad de transmisión es de 433Mbps y 1.3Gbps respectivamente.

Estándar 802.11 i

El estándar 802.11i supera muchas de las deficiencias de su predecesor, tanto en términos de autenticación de usuarios como en la solidez de los métodos de cifrado. Y lo logra en el primer caso a través de su capacidad para trabajar en cooperación con 802.1X, y en el segundo caso al permitir el cifrado del Estándar de cifrado avanzado (AES). Además de mejorar en gran medida la seguridad de los entornos WLAN, también reduce en gran medida la complejidad y el tiempo necesario para que los usuarios se trasladen de un punto de acceso a otro. (López Jurado, 2021)

Tenga en cuenta que 802.11i no es un punto final. Es esencialmente una evolución de las tecnologías anteriores, principalmente WPA (Acceso protegido Wi-Fi), implementadas durante mucho tiempo en la industria, hasta el punto en que el nuevo estándar todavía se conoce como WPA2. (López Jurado, 2021)

De igual manera fue el primer protocolo de seguridad aprobado por IEEE para redes inalámbricas llamada WEP (privacidad equivalente por cables). Esto hizo posible utilizar claves cifradas de 40 bits según el algoritmo de cifrado RC4 y asignar una clave a cada máquina cliente por sesión. Pero desde que fue pirateado en el verano de 2001, se lo considera el talón de Aquiles de la cadena de seguridad inalámbrica.

La combinación de WEP con el protocolo de autenticación 802.1X mejoró un poco la situación, ya que en este esquema el cliente WEP se veía obligado a solicitar acceso a la red mediante EAP (Extensible Authentication Protocol), tal como lo establece el 802.1X.

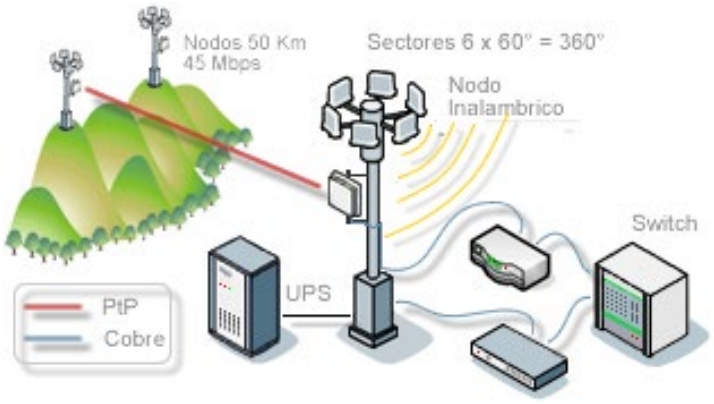
Arquitectura de redes inalámbricas

Red punto a punto

La información se transmite de un punto a otro mediante antenas directas, proporcionando la mayor capacidad de conexión, lo que se traduce en un alto nivel de seguridad que reduce las interferencias**.** (Gerlysu, 2012)

Figura 27

Red punto a punto (PtP)



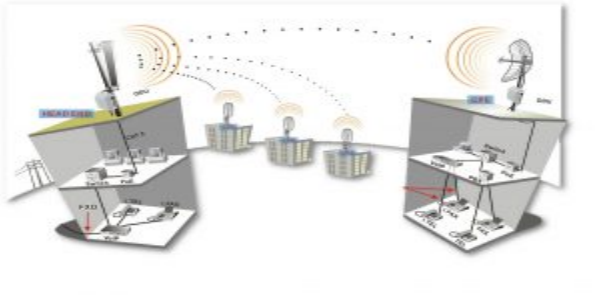
Nota. La siguiente figura representa una red punto a punto mediante antenas direccionales. Tomado de (Gerlysu, 2012)

Red punto a multipunto

Su información es transmitida de un punto a múltiples receptores, en el cual se utiliza una antena omnidireccional, generalmente la comunicación solo permanece entre el punto central y los remotos, pero la comunicación de los equipos carece entre los remotos. (ALFATELECOM, 2019)

Figura 28

Red punto multipunto (PtMP)



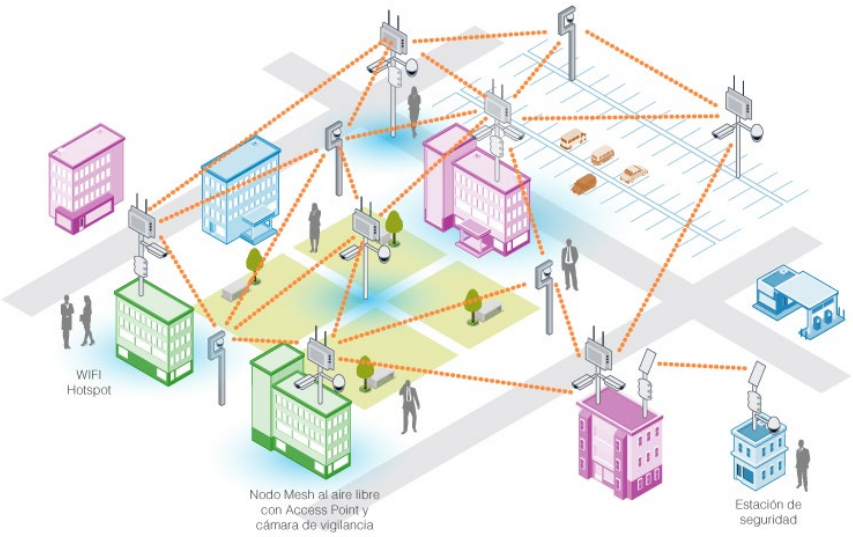
Nota. La figura representa la conexión de equipos desde un punto central hacia los demás. Tomado de (ALFATELECOM, 2019)

Red mesh

Una característica de este tipo de red es que varios nodos conectados proporcionan rutas de conexión independientes y redundantes y utilizan protocolos de enrutamiento específicos para garantizar la transmisión. (DMS, 2016)

Figura 29

Red Mesh



Nota. La figura representa la conexión de múltiples usuarios en una misma área. Tomado de (DMS, 2016)

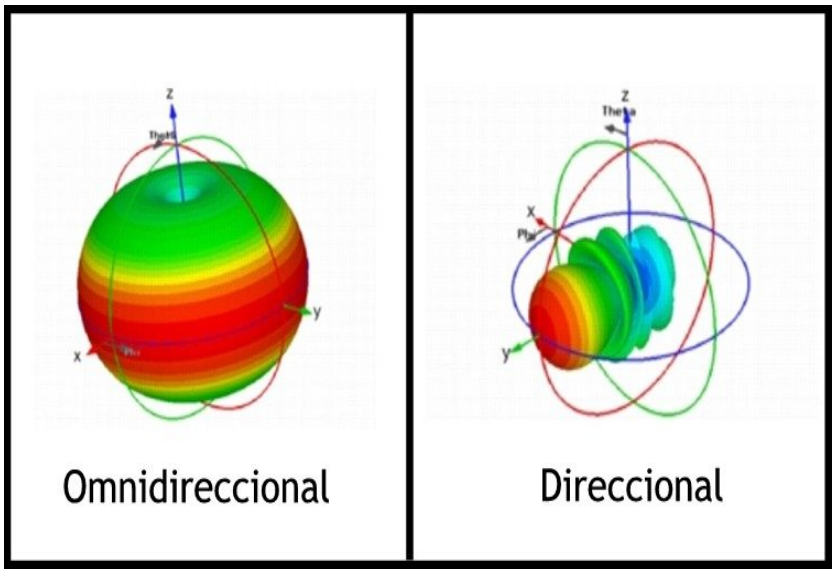
Equipos de telecomunicaciones usados en redes inalámbricas

Antenas

Las antenas son muy importantes en los sistemas inalámbricos. Puede ser una antena omnidireccional que recibe ondas electromagnéticas de todas las direcciones, tiene un área grande y se usa en redes multipunto, así mismo las antenas direccionales concentran las ondas electromagnéticas en una sola dirección. Por lo tanto, la señal llega a distancias más largas. Utilizado en aplicaciones punto a punto. (Huidobro, 2013)

Figura 30

Radiación de la antena omnidireccional y direccional



Nota. Representa el nivel de radiación que genera tanto la antena direccional como la omnidireccional. Tomado de (David, 2015)

Access point

Son uno de los elementos más comunes en conjunto con los routers inalámbricos por que presentan configuraciones interesantes que mejoran el acceso a la red, también se define que:

> Punto de acceso o WAP (Wireless Access point). Es un equipo para establecer conexiones inalámbricas entre ordenadores, formando una red inalámbrica diferente para conectar dispositivos móviles o tarjetas de red inalámbrica. Esta red se considera una red de área local inalámbrica (WLAN) y está diseñada para reducir al máximo las conexiones por cable. (Explorer, 2022)

Figura 31

ACCESS POINT WIRELESS N TP-LINK EAP115

Nota. Punto de acceso de la marca TP-LINK EAP 115. Tomado de (TECNIT, 2017)

Existen de forma general dos características más sobresalientes de un punto de acceso, las cuales son la potencia que presente el transmisor y la otra seria la sensibilidad del receptor. La primera característica se refiere a que tan fuerte es la señal que irradia las antenas del equipo en dbm o mw. La segunda característica sobre la sensibilidad del receptor hace referencia a que tan débiles o bajos pueden ser los valores de potencia que puede receptar el equipo. Por tal razón se considera que un equipo es bueno cuando su potencia de salida es alta y su sensibilidad de recepción permite detectar señales con potencias muy débiles.

Ventajas de un punto de acceso

- Los dispositivos inalámbricos como teléfonos móviles y computadoras portátiles se pueden conectar a la WLAN.

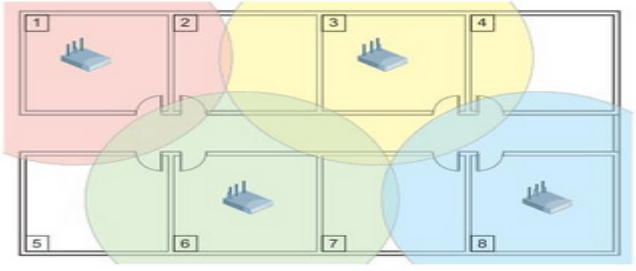
- Basado en la radiación de radio que puede penetrar las paredes, es ideal para conectar edificios vecinos en la misma red y tiene una antena potente que puede crear redes WLAN de hasta varios kilómetros.
- El radio de trabajo es de 30 metros a 100 metros.
- Proporciona información sobre el estado de la red y limpia la red dividiendo la red más rápido de lo normal y enviando información en paralelo.
- Con una conexión PoE, puede usar un solo cable Ethernet RJ-45 para proporcionar acceso a Internet sin estar enchufado a un tomacorriente de pared normal.
- Más usuarios pueden conectarse simultáneamente. (Explorer, 2022)

Ubicación del punto de acceso

Al elegir una ubicación para estos puntos de acceso, debe considerar colocarlos lo más cerca posible de sus dispositivos para obtener la mejor señal posible. Pero también tenga en cuenta que las paredes, las tuberías de agua, los bloques de agua, las placas de metal y los transmisores con frecuencias similares a los hornos de microondas interferirán con la conexión de estos dispositivos. Por eso es importante tenerlos en cuenta a la hora de colocarlos. (Explorer, 2022)

Figura 32

Mapas de calor para la ubicación de los puntos de acceso



Nota. Se observa simulaciones de los mapas de calor que generan los equipos para par obtener el lugar óptimo para la instalación del AP. Tomado de (Mareco, 2020)

Diferencia un AP y un router

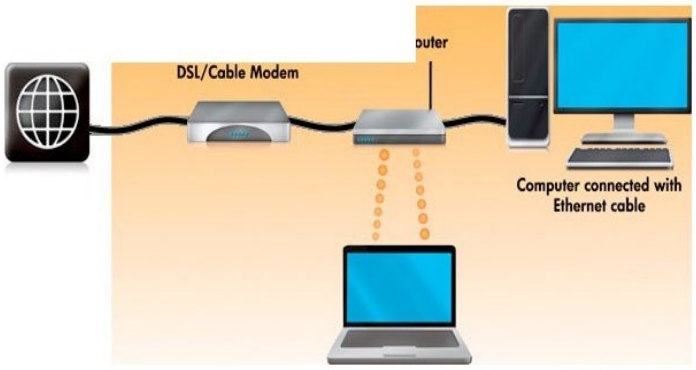
Los puntos de acceso y los routers requieren módems para convertir la señal (modular y demodular la señal). Los enrutadores brindan conectividad a los dispositivos, mientras que los puntos de acceso se utilizan para brindar conectividad a ubicaciones no conectadas. Alternativamente, puede crear una WLAN y transferir datos entre dispositivos conectados a la misma WLAN. (Explorer, 2022)

Router inalámbrico

Si dispones de una conexión ADSL que te da acceso a internet a través de nuestras líneas telefónicas, coaxial o fibra óptica, el dispositivo encargado de conectarnos será un router. Pero esta no es la única forma de poder compartir internet a los clientes, ya que además de la función de compartir internet de forma cableada, también este tipo de dispositivos, gracias a la incorporación de antenas, pueden además brindar conexión inalámbrica. Es por esto que este tipo de equipos posee gran popularidad en el mercado ya que además de estas dos conexiones, también presentan un medio de configuración y monitoreo de la red que se puede realizar vía web. (Campoy, 2016)

Figura 33

Funcionamiento del router inalámbrico



Nota. Esquema del funcionamiento de un router inalámbrico. Tomado de (Campoy, 2016)

Seguridad en redes inalámbricas

Las redes inalámbricas se han convertido en una industria de las comunicaciones en rápida evolución debido a su alto desempeño. El deseo de las personas de llevar la información más lejos sin cables, la conveniencia de la conectividad y el rápido despliegue que exhiben son algunos de los aspectos que impulsan la rápida asimilación de las personas. Desafortunadamente, los usuarios no aprecian la seguridad de estas redes y son vulnerables a varios tipos de ataques.

A medida que avanza la tecnología, se han desarrollado diversas técnicas, protocolos o algoritmos, destinados principalmente a proteger las redes inalámbricas.

Como administradores de redes debemos tener en cuenta que este tipo de redes no debería ser más vulnerables en comparación con las redes cableadas y además que el nivel de seguridad de una red es directamente proporcional al coste económico.

Figura 34

Seguridad en redes inalámbricas

Nota. Representación gráfica de seguridad en redes inalámbricas. Tomado de (Salazar, 2016)

Tipos de seguridad de redes inalámbricas

WEP (Wired Equivalent Privacy)

Considerado un algoritmo de seguridad opcional definido en el estándar IEEE 802.11 y está diseñado para proporcionar privacidad, autenticación y control de acceso para LAN inalámbricas. La finalidad de este tipo de encriptación es incrementar el nivel de seguridad en los equipos que lo tengan instalado o habilitado, con la finalidad de obtener un nivel de seguridad arecido al de los equipos cableados.

El protocolo de encriptación de datos para redes inalámbricas en mención fue desarrollado pensando en que su uso estaría dirigidos a equipos de costo bajo y que además sea de fácil configuración, es por esto que al usar WEP solo se usa una única clave de acceso para todos usuarios que se vayan a conectar a la red.

> “La función de esta clave WEP se basa, en la utilización de la misma clave simétrica y estática tanto en la estación como en el punto de acceso. El estándar no contempla ningún mecanismo externo que se encarga de la autenticación de claves, lo que obliga a escribir la clave de forma manual en cada cliente” (Suárez Gutiérrez, 2012, pág. 15)

Esto a lo largo implica riesgos en la red ya que al tratarse de redes con gran cantidad de usuarios se toma el riesgo de que la clave de ingreso sea compartida con individuos ajenos lo cual derivara el aumento de control que debe manejar el individuo encargado de la administración de la red.

WPA (wifi Protected Access)

El protocolo de acceso Wi-Fi corrige la mayoría de las debilidades del protocolo WEP y, por lo tanto, se considera más confiable en términos de seguridad. A diferencia de WEP en el cual solo se usaba una única clave para acceder a la red, en WAP se presenta al usuario o

estaciones una variedad de claves lo cual lo vuelve más robusta y mejora así la integridad de los equipos y la información que se maneje.

WAP incluye las siguientes tecnologías:

IEEE 802.11 X

Es un estándar creado por la IEEE el cual está desarrollado para redes alámbricas y en el que se manifiesta el funcionamiento del control de acceso a la red a través de los puertos físicos de esta; de forma similar se tomaría para las redes inalámbricas en donde en punto de acceso seria símil de switch y los usuarios serían los clientes, funcionaria de la siguiente manera; las estaciones inalámbricas o usuarios para poder conectarse a la red necesitara de una clave para autentificarse y el punto de acceso a través de EAP y el uso de un servidor de autentificación puedan conocer y comprobar que la información ingresada por el usuario sea la correcta, el punto de acceso habilitaría su puerto. (Suárez Gutiérrez, 2012, pág. 18)

EAP (Extensible Authentication Protocol)

Definido por sus siglas en el Registro Federal de Contribuyentes o RFC número 2284 como un protocolo de autenticación extensible que tiene como objetivo realizar tareas de autenticación, autorización y contabilidad. El protocolo de autentificación extensible (EAP) fue diseñado inicialmente por el protocolo PPP, aunque WPA lo utiliza entre estación y el servidor de autenticación AAA Radius. Esta manera de encapsulación de EAP está basada por medio del estándar 802.1X denominado EAPOL. (Suárez Gutiérrez, 2012, pág. 19)

Figura 35

Tipos de seguridad en redes inalámbricas

Nota. La figura representa los tipos de seguridad que se utiliza para el wifi. Tomado de (ACRYLICSuite, 2020)

WPA2 Personal y Enterprise

WPA2 es considerado un método basado en WPA diseñado para brindar protección sofisticada de datos y funciones relacionadas con el control de acceso a la red.

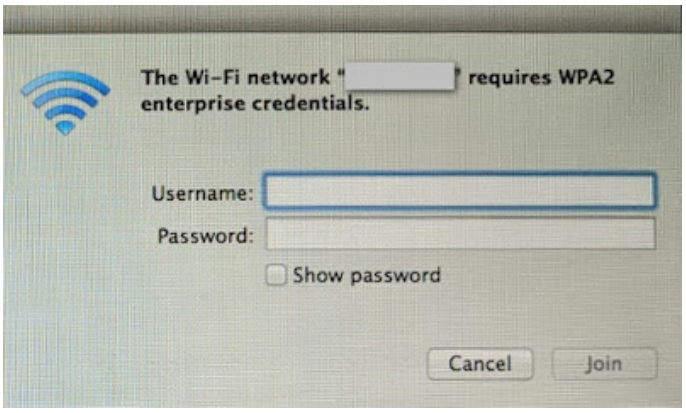
De la misma forma otro autor manifiesta que:

> En efecto, WPA2 brinda a los usuarios de WLAN domésticos y comerciales la seguridad de que solo los usuarios autorizados pueden acceder a la red inalámbrica. Esta es la intención en estos casos. WPA2 forma parte del estándar IEEE 802.11i y además proporciona la denominada seguridad de nivel gubernamental. Esto es gracias a la implementación del algoritmo de cifrado AES FIPS 140-2. Este es un algoritmo criptográfico que también es compatible con los requisitos de NIST o el Instituto Nacional de Estándares y Tecnología de América del Norte. (Olenski, 2016)

Por otra parte, el cifrado para redes wifi según Olenski “Verifica a los usuarios de la red por medio de un servidor, siendo absolutamente compatible con las versiones previas de WPA. como resultado, en cambio, logra un mayor nivel de complejidad”. (2016)

Figura 36

Acceso mediante WPA2 Enterprise



Nota. La figura representa la ventana para ingresar los datos correspondientes para la autenticación con el servido para acceder a la red. Tomado de (Blogger, 2020)

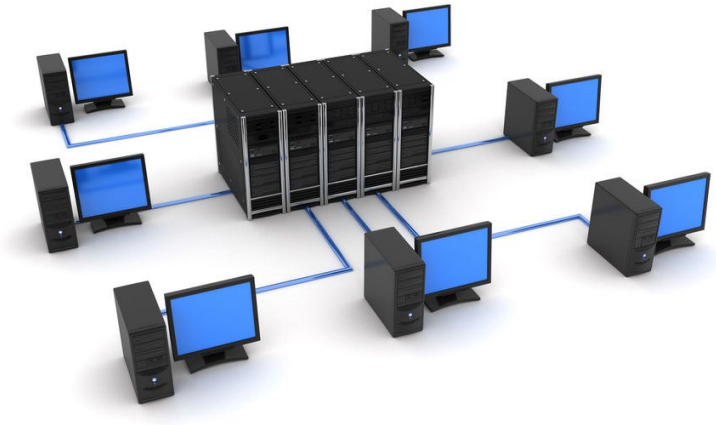
Servidor

Se entiende como servidor aquel elemento que es capaz de brindar un servicio a un usuario, de forma más detallada:

> Un servidor es un sistema que proporciona recursos, datos, servicios o programas a otras computadoras, llamadas clientes, en una red. En teoría, un equipo que comparte información con los clientes lo llamamos servidor. Un servidor sería un poderoso sistema individual conectado a través de una red a una colección de clientes menos poderosos. Esta arquitectura de red se denomina modelo cliente-servidor, donde tanto el cliente como el servidor tienen poder de procesamiento, pero algunas tareas se delegan al servidor. (Marchionni, 2011, pág. 23)

Figura 37

Servidor



Nota. Representa el funcionamiento de la arquitectura cliente-servidor. Tomado de (Blogodisea, 2018)

Tipos de servidores

Existen varios tipos de servidores por su versatilidad, pudiendo instalarse física o virtualmente. Además, estos también se clasifican de acuerdo a su capacidad, a los fabricantes o, por último, de acuerdo a los servicios que brindan al usuario. En base a esto, las siguientes secciones analizan varios tipos de servidores según los servicios que brindan.

Servidor de email

Actúa como una especie de sala de correo, permitiendo almacenar, recibir, enviar y realizar diversas tareas relacionadas con las direcciones de correo electrónico de cada usuario. Mail Server es uno de los servidores más populares del mercado gracias a la popularidad del correo electrónico en nuestras vidas debido a su eficiencia en términos de información y administración. (Colaboradores de Docusing, 2021)

Figura 38

Servidor de email

Nota. Funcionamiento de un servidor de email. Tomado de (De León, 2019)

Servidores Web

Este tipo de servidores tiene como una de sus funciones la de almacenar sitios web y posteriormente cumplir con otra de sus tareas que es la de devolver esta información a los clientes que lo soliciten.

Figura 39

Servidor Web

Nota. Concepto de la función principal de servidor web. Tomado de (Lugo, 2019)

Servidores virtuales

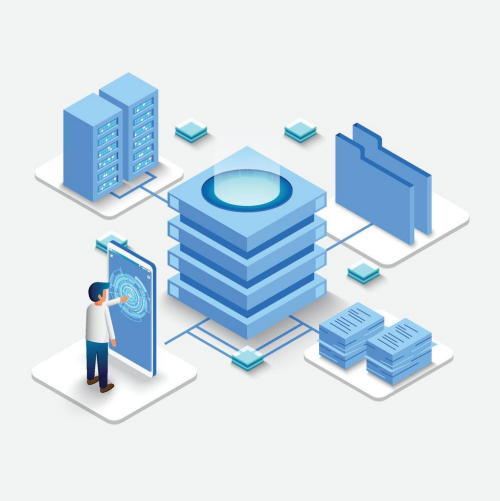
Optimiza sus costos de hardware con la flexibilidad de activar múltiples sistemas operativos y programas simultáneamente facilitando mejor uso del equipo físico en donde se instaló los servidores virtuales.

Servidores de base de datos

La importancia de este tipo de servidores radica en la capacidad de encausar enormes cantidades de datos y producir información. Para abarcar toda esta cantidad de información, suelen estar conectadas a u repositorio. También permite analizar, manipular y almacenar los datos según las necesidades del usuario.

Figura 40

Servidor base de datos



Nota. equipos que forman un servidor de base de datos. Tomado de (grupo universal, 2020)

Servidores cloud

Son utilizados por empresas que se especializan en almacenar información de forma remota, alquilando espacio en sus servidores a otras personas y empresas. Se utiliza para

almacenar grandes cantidades de datos y salvaguardar la información confidencial de una organización.

Figura 41

Servidor cloud

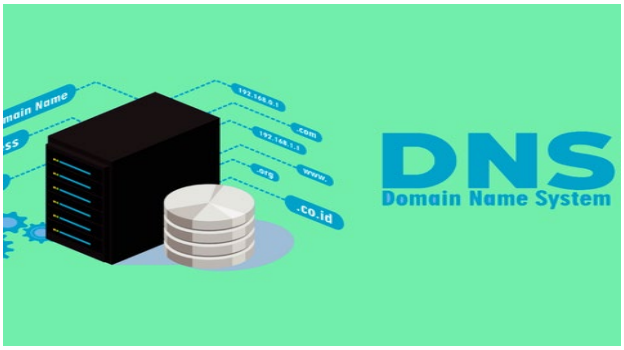
Nota. Concepto de que es un servidor cloud. Tomado de (grupo universal, 2020)

Servidores DNS

Gestiona el nombre de dominio del sitio web, por ello, estable conexión de un sitio web y su IP (una serie de números que describen de manera precisa la interfaz de red de un dispositivo). Entonces, cuando se ingresa un dominio en un navegador, el servidor lee la solicitud y devuelve la apariencia de la página.

Figura 42

Servidor DNS



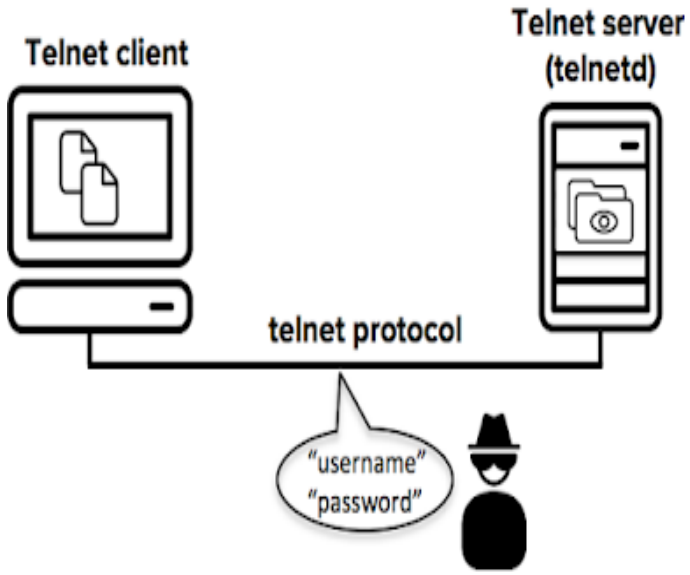
Nota. Servidores para el almacenamiento de nombres. Tomado de (Espinosa, 2022)

Servidor Telnet

Protocolo de red utilizado principalmente en telecomunicaciones que permite a los usuarios administrar, enviar y recibir datos y resolver problemas de red relacionados con la telefonía. Del mismo modo, además de las llamadas, guarda el buzón de voz, los datos del contestador y controla el internet móvil. (Colaboradores de Docusing, 2021)

Figura 43

Servidor Telnet



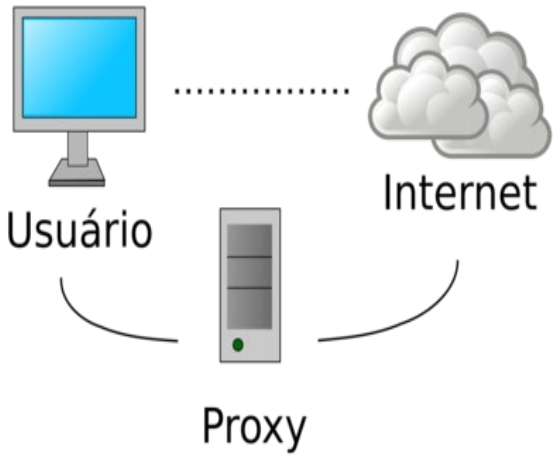
Nota. Funcionamiento de servidor telnet. Tomado de (REDES, 2018)

Servidores proxy

Brindan conexión a Internet. Por regla general, contienen cortafuegos para los que se crean reglas para permitir la visualización de determinadas páginas y bloquear otras. Pueden redirigir la navegación y mostrarnos una señal de advertencia o una violación de la política de la empresa.

Figura 44

Servidor proxy



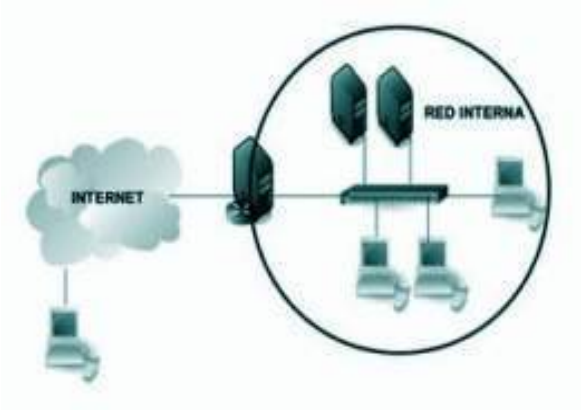
Nota. Concepto se servidor proxy. Tomado de (Fernández, 2017)

Servidor acceso remoto RAS

Supervisa la línea de módem del computador u otros medios de comunicación por Internet para que las solicitudes puedan conectarse de forma remota a su red, responder llamadas y participar en solicitudes de red. (Colaboradores de Docusing, 2021)

Figura 45

Servidor de acceso remoto RAS



Nota. La figura representa un servidor de acceso remoto RAS. Tomado de (Ecured,2021)

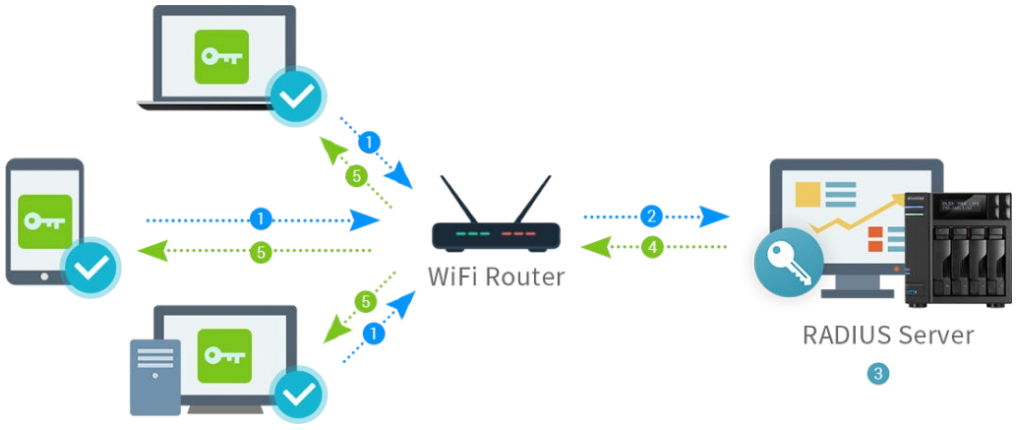
Radius

Radius son las siglas de Remote Authetication Dial-Up Server, misma que traducida al idioma español significaría Servidor de autentificación remota. De forma global RADIUS es un protocolo enfocado en cumplir las normas de seguridad en una red como lo son: la autorización, autentificación y el arqueo. Este protocolo es la continuación de AAA, la cual es una idea enfocada en la protección de las redes y que significa Authentication+ Authorization+ Accounting, con su traducción al idioma español de Autenticación+ Autorización+ Arqueo.

El protocolo en mención toma las bases de esta idea de AAA y además toma por una parte su código fuente y a parte del personal que trabajaba en dicha idea, es por esto que se podría decir que es la versión mejorada de AAA. Estas tres pautas, que son una adaptación del concepto original, permiten a los usuarios proporcionar un nivel más detallado de control sobre el acceso a la red, el tráfico, la generación de informes, el análisis estadístico y otros mecanismos de control a los administradores de red mediante la implementación de este protocolo.

Figura 46

Proceso de autenticación



Nota. Proceso de autentificación del usuario mediante el servidor Radius. Tomado de (WISPCONTROL, 2020)

Tipos de servidores Radius

Hay varios servidores RADIUS disponibles, cada uno destinado principalmente a entornos UNIX y que comparten muchas de las mismas características, aunque cada uno trata de aprovechar los factores técnicos que le otorgan una ventaja sobre los demás, por las cuales se detalla a continuación:

Servidores Radius no licenciados

FreeRADIUS

Este tipo de servidor de autenticación AAA es uno de los conocidos en la actualidad, además se puede decir que:

Free RADIUS es un paquete estándar compatible con varios sistemas operativos gratuitos y con licencia. Le permite hacer grandes instalaciones con múltiples servidores AAA.

Admite conexiones a diferentes tipos de bases de datos para autorización y contabilidad, y admite una amplia gama de métodos de autenticación, que juntos forman un sistema AAA muy estable y confiable. Un gran beneficio de Usar Ubuntu Server como su sistema operativo principal es mantener un repositorio que los desarrolladores actualizan constantemente. Acelera el proceso de instalación de cualquier software y sus dependencias y no requiere licencia para usarlo. (Cando Salme & Llumitasig Galarza, 2016, pág. 37)

Cistron

Se trata de un servidor de gestión de cuentas y autenticación de servidor terminal a través del protocolo RADIUS, lo que lo convierte en uno de los servidores más utilizados en la comunidad del software libre.

ICRadius

El servidor ICRadius utiliza una base de datos MySQL para almacenar toda la información necesaria, incluidos los archivos de usuario y directorio, así como enviar datos a la base de datos. Esto utiliza la facilidad de uso y la flexibilidad de MySQL de una manera única, lo que permite una manipulación y extracción de datos rápida y eficiente. ICRadius es totalmente gratuito y se basa en la licencia GPL. Este sistema utiliza un formato tabular que maximiza el uso de las bases de datos. (Cando Salme & Llumitasig Galarza, 2016, pág. 38)

XtRADIUS

La principal diferencia entre xtRadius y otros servidores RADIUS es la capacidad de ejecutar secuencias de comandos totalmente personalizables para administrar la autenticación y el uso de la cuenta. El beneficio de esta función es que, en lugar de usar el mismo archivo de usuario RADIUS o el mismo sistema de almacenamiento de contraseñas para la autenticación, aplicación de script para consultar cualquier fuente (como datos SQL de una base de datos) y validar la entrada del usuario antes de que se acepte. (Cando Salme & Llumitasig Galarza, 2016, pág. 39)

OpenRADIUS

OpenRADIUS tiene una interfaz de módulo externo que se comunica mediante canales y flujos prediseñados, lo que permite que los módulos se implementen en cualquier idioma que admita E/S de canalización de Unix. Su comportamiento es totalmente configurable utilizando un lenguaje incorporado simple que le brinda control total sobre las listas de solicitudes y respuestas. (Cando Salme & Llumitasig Galarza, 2016, pág. 40)

Servidores Radius licenciados

Radiator

Radiator Server es uno de los mejores servidores Radius, permite comprobar y controlar de forma segura el acceso a redes alámbricas e inalámbricas a la vez que se puede configurar de forma muy sencilla y adaptarse a trabajar con diferentes dispositivos de fabricantes distintos lo que les permite una mayor adaptación a los requisitos presente y futuros de las redes, además es uno de los servidores que ofrece gran variedad de métodos de autentificación EAP. (Cando Salme & Llumitasig Galarza, 2016, pág. 42)

Software libre

Se conoce como software libre a todos los programas en los que se permita la modificación de su código fuente, además su descarga, uso o compartición es totalmente libre de costos económicos. En otras palabras, este tipo de software le da a cualquier persona u organización la libertad de usar el programa para cualquier tipo de trabajo sin tener que entregarlo a un desarrollador u organización específica. (Souza, 2019)

Figura 47

Linux

Nota. Representación de un software libre como Linux. Tomado de (Brown, 2020)

En fin, desde el punto de vista que se intente definir este término, muchas serán sus variaciones, pero sim embargo hay algo en lo que coinciden la mayoría de personas, y es que

un software es libre cuando este pueda ser usado, modificado, estudiado y distribuido sin ninguna clase de impedimentos. El más conocido son los sistemas Linux.

Ubuntu Server

Ubuntu server es un sistema operativo desarrollado por la empresa canonical, es de licencia libre, es decir que para su utilización no se necesita disponer de una licencia con un costo económico para realizar su activación, solo basta con ingresar a las paginas oficiales de descarga de Ubuntu y buscar la versión que se desea instalar.

Ubuntu generalmente es reconocido por los usuarios gracias a su versión de escritorio debido a que es sin duda el más usado en cuanto a sistemas de GNU Linux, pero Ubuntu server está enfocado en la utilización y manejo de servicios.

Ubuntu server al funcionar como un servidor tiene la función de dar servicios, programas, archivos o datos a otros equipos que lo soliciten los cuales se denominan consumidores. Su función es la guardar los archivos para luego compartirlos, en conclusión, un servidor es un homólogo de un equipo de cómputo personal, solo que a niveles de almacenamiento y procesamiento más elevado.

Figura 48

Ubuntu server

Nota. Sistema operativo de Ubuntu Server 20.04 LTS. Tomado de (Ubuntu, 2019)

Capítulo III

Desarrollo del tema

Al culminar la investigación bibliográfica realizada en el marco teórico se encuentra un diagnóstico de necesidades de poder contar con equipos adecuados para la implantación de un sistema de videovigilancia IP y el sistema de seguridad WiFi WPA2 entrerprise utilizando un servidor radius, por tal razón fue necesario realizar un reconocimiento previo de la entidad realizando entrevistas al personal encargado para poder verificar las oficinas con mayor necesidad de seguridad. Y de esta manera poder obtener la información necesaria para la implantación de estos sistemas.

Figura 49

GAD Municipal del Cantón Saquisili

Nota. La siguiente figura representa el ingreso principal al GAD Municipal del cantón Saquisili.

Una vez realizada la inspección se procede a la elaboración de cuadros comparativos de los equipos a utilizar con sus respectivas características técnicas de las diferentes

alternativas que presentan en el mercado para estos tipos de sistemas de seguridad. Además, se debe tener en cuenta que la tecnología va avanzando drásticamente por el cual tener un hardware más actual beneficiaria a implementaciones futuras.

Como primer paso, procedamos a indagar sobre las características de NVR que lo ayudarán a implementar su sistema de videovigilancia IP de tal forma que nos permita seleccionar el más óptimo. gracias al equipo nos facilita la grabación y gestión de imágenes digitales transmitidas por las cámaras IP a través de la red. Por tal razón se escogió el DHI-NVR2108HS-I ya que cuenta con ocho canales.

Tabla 3

Características de los modelos de NVR

Características	**DHI-NVR1104HS-S3/H**	**DHI-NVR2108HS-I**	**DHI-NVR4108HS-4KS2/L**
Canales De Acceso	4 CANALES	8 CANALES	8 CANALES
Capacidad De Codificación	1–ch@8MP(30FPS) 1–ch@5MP(30FPS) 2–ch@4MP(30FPS) 2–ch@3MP(30FPS) 4–ch@1080P(30FPS)	AI disabled: 1-channel 12MP@30 fps; 1-channel 8MP@30 fps; 2-channel 5MP@30 fps; 3-channel 4MP@30 fps; 6-channel 1080p@30 fps	8 × 1080p@30 fps

Características	DHI-NVR1104HS-S3/H	DHI-NVR2108HS-I	DHI-NVR4108HS-4KS2/L
		AI enabled: 1-channel 8MP@30 fps; 1-channel 5MP@30 fps; 2-channel 4MP@30 fps; 4-channel 1080p@30 fps	
Compresión de Video	Smart H.265+/H.265/ Smart H.264+/H.264	Smart H.265+/H.265/Smart H.264+/H.264	Smart H.265/H.265/ Smart H.264/H.264
Protección Perimetral	N/A	1 CANAL	8 CANALES
Reconocimiento Facial	N/A	5 CANALES	N/A
Detección Facial	N/A	5 CANALES	4 CANALES
Smd Plus	N/A	4 CANALES	8 CANALES

Nota. Esta tabla representa las características de cada uno de modelos de NVR.

Luego de haber realizado la comparación de los NVR se procede a la elección y búsqueda de las características de las cámaras IP para la utilización en el sistema de video vigilancia en el GAD Municipal del Cantón saquisili. Por tal razón escogimos el modelo DH-IPC-

HDW1230T1-S4, ya que esta cámara cuenta un lente de 2.8MM, un ángulo de vista de 105 grados y un alcance hasta de 30 metros, de la misma manera el equipo seleccionado es más económico. Por esta razón la cámara es útil para la implementación del sistema de videovigilancia en el GAD Municipal del cantón Saquisili.

Tabla 4

Tipo de cámaras IP

CÁMARAS IP			
CARACTERÍSTICAS	DH-IPC-HDW1230T1-S4	DH-IPC-HFW1431T1-ZS-S4	IPC-HFW1239S1-LED-S4
Modelo	Domo	Bala	Bala
Sensor de Imagen	1/2.7" 2Megapixel progressive CMOS	1/3 ”4Megapixel progressive CMOS	1/2.7" 2Megapixel progressive CMOS
Distancia de infrarrojos	30 mts	50 mts	N/A
Distancia LED	N/A	N/A	2.8 mm: 10 mts 3.6 mm: 15 mts
Tipo de lente	Focal fijo	Varifocal motorizado	Focal fijo

CÁMARAS IP			
Longitud Focal	2.8 mm 3.6 mm	2.8 mm 12 mm	2.8 mm 3.6 mm
Campo de visión	**2.8 mm:** Horizontal: 105° Vertical: 57° Diagonal: 125° **3.6 mm:** Horizontal: 87° Vertical: 47° Diagonal: 104°	Horizontal: 98°–31° Vertical: 55°–18° Diagonal: 116°–36°	**2.8 mm:** Horizontal 110° × Inclinación 59° × Diagonal 132° **3.6 mm:** Horizontal 91° × Inclinación 48° × Diagonal 109°
Smart Codec	Si	Si	Si
Compresión de video	H.265; H.264; H.264H; H.264B; MJPEG	H.265; H.264; H.264B; MJPEG	H.265; H.264; H.264H; H264B; MJPEG
Velocidad de fotogramas de vídeo	**Main Stream:** 1920 × 1080 (1 fps–25/30 fps) **Sub stream:** 704 × 576 (1 fps–25 fps)	**Main Stream:** 2560 × 1440 (1 fps–25/30 fps) Sub Stream: 704 × 576 (1 fps–20/25 fps)	**Main Stream:** 1920 × 1080 (1 fps–25/30 fps) **Sub stream:** 704 × 576 (1 fps–25 fps)
Protección de ingreso	IP67	IP67	IP67

Nota. En la siguiente tabla informa las características de diferentes cámaras IP.

Una vez finalizado el análisis de la cámara IP a utilizar se procede a la elección y búsqueda de las características de los Access point de acuerdo al sistema de seguridad Wifi WPA2 Enterprise, por la cual se escogió dos equipos de diferente marca para realizar las comparaciones. En este caso escogimos el equipo Access Point Eap115 Tplink Omana Wireless N300mbps Empresar, porque es un equipo más económico, y de la misma manera cuenta con el sistema de autenticación WPA2 Enterprise por tal razón será de gran utilidad para la implementación del proyecto.

Tabla 5

Tipos de Access Point

ACCESS POINT		
CARACTERÍSTICAS INALÁMBRICO		
	Access Point Eap115 Tplink Omana Wireless N300mbps Empresar	GWN7630
ESTÁNDARES INALAMBRICOS	IEEE 802.11n/g/b	IEEE 802.11 a/b/g/n/ac
TASA DE SEÑAL	11n: 300Mbps 11g: 54 Mbps 11b: 11Mbps 2,4 GHz	11ac: 6.5 Mbps a 1733 Mbps 11a: 54 Mbps 11n: 6.5 Mbps a 600 Mbps 11b: 11 Mbps 11g: 54 Mbps

ACCESS POINT		
CARACTERÍSTICAS DE SEGURIDAD		
CIFRADO WIFI	64/128/152-bit WEP / WPA /WPA2-Enterprise, WPA-PSK /WPA2-PSK	WEP, WPA/WPA2-PSK, WPA/WPA2 Enterprise
CARACTERÍSTICAS DE HARDWARE		
INTERFAZ	Puerto Fast Ethernet (RJ-45)	2 puertos Ethernet de 10/100/1000Base-T con detección automática (RJ-45)
FUENTE DE ALIMETACIÓN	PoE 802.3af o fuente externa de 9VDC /0.6A	Compatible con el estándar 802.3 az; POE 802.3af/802.3at
TIPO DE ANTENA	Antena interna omnidireccional 2* 4dBi	4 antenas internas de doble banda 2.4 GHz, ganancia 4dBi 5 GHz, ganancia 5dBi
CARACTERISTICAS SOFTWARE		
PROTOCOLOS	IPV4, IPV6	IPv4, IPv6, 802.1Q, 802.1p, 802.1x, 802.11e/WMM

Nota. Esta tabla muestra dos tipos de Access Point de diferente marca.

Finalizado con la selección del Access point, continuamos con las características de los softwares que se van a utilizar para la seguridad WPA2 Enterprise utilizando un servidor radius, por tal razón para la instalación del servidor freeradius, escogimos el sistema operativo Ubuntu server con la versión 20.04 Lts esta versión es la más estable y es de gran utilidad para estos tipos de servidores, de la misma manera cuenta con una licencia libre, y sus requerimientos son 2.5 GB en disco, 512MB en RAM mínimo y un procesador de 1GHz o superior.

Tabla 6

Sistema operativo

SISTEMA OPERATIVO	
CARACTERISTICAS	**UBUNTU SERVER**
Fabricante	GNU Linux
versión	20.04Lts
Licencia	libre
Requerimientos mínimos	2.5 GB en disco
	512 MB en RAM mínimo
	Procesador de 1GHz o Superior
Tipo de interfaz	Unity (11.04- 17.04) GNOME
	Shell(17.10-+)
Medio de instalación	DVD, memoria USB
Arquitecturas soportadas	X86, AMD64, SPARC, IA-64, HP
	PA-RISC

Nota. La siguiente tabla muestra las características de un Sistema operativo.

Como parte final en la selección de software para la implementación de una red wifi con un servidor de autentificación AAA, se optó por escoger al servidor de licencia libre Freeradius versión 3.0.20, ya que está acorde a las características del equipo de cómputo dispuesto por el Gad Municipal del cantón Saquisili y como lo mencionamos con anterioridad al ser de licencia libre limitara los gastos que tenga que abarcar la entidad.

Tabla 7

Servidor de autentificación AAA

Freeradius	
Tipo de licencia	Libre
Version	3.0.20
Kernel	5.4.0-122-generic

Nota. La siguiente tabla muestra las características del servidor de autentificación AAA.

Diagrama de la topología del sistema de video vigilancia IP

Ya finalizado con los cuadros comparativos de los equipos a utilizar se procedió a elaborar un diagrama de red del sistema de video vigilancia IP el cual nos ayudaría a comprender el funcionamiento de cada uno de los equipos que serán instalados en el GAD municipal del cantón Saquisili.

Figura 50

Topología del sistema de video vigilancia IP

Nota. La figura representa la infraestructura que se implementara en los puntos vulnerables.

De igual manera se realizó la inspección de las instalaciones de GAD municipal de Saquisili para la instalación de las cámaras en sus oficinas con mayor necesidad, dando así mayor seguridad al personal que transita en las instalaciones y de esta manera, poder establecer mayor control en los diferentes puntos evitando posibles delitos que afecten al GAD Municipal Del Cantón Saquisili.

Tabla 8

Inspección para la instalación de cámaras

Ord.	Ubicación	cámara	cantidad
1	Entrada trasera Primera planta	Cámara IP domo DH-IPC-HDW1230T1-S4	1
2	Pasillo secundario Segunda planta	Cámara IP domo DH-IPC-HDW1230T1-S4	1
3	Salón de la ciudad Tercera planta	Cámara IP domo DH-IPC-HDW1230T1-S4	1

Ord.	Ubicación	cámara	cantidad
4	Pasillo principal Tercera planta	Cámara IP domo DH-IPC-HDW1230T1-S4	1
Total			4

Nota. La tabla representa los puntos donde serán colocadas las cámaras para la seguridad de las oficinas.

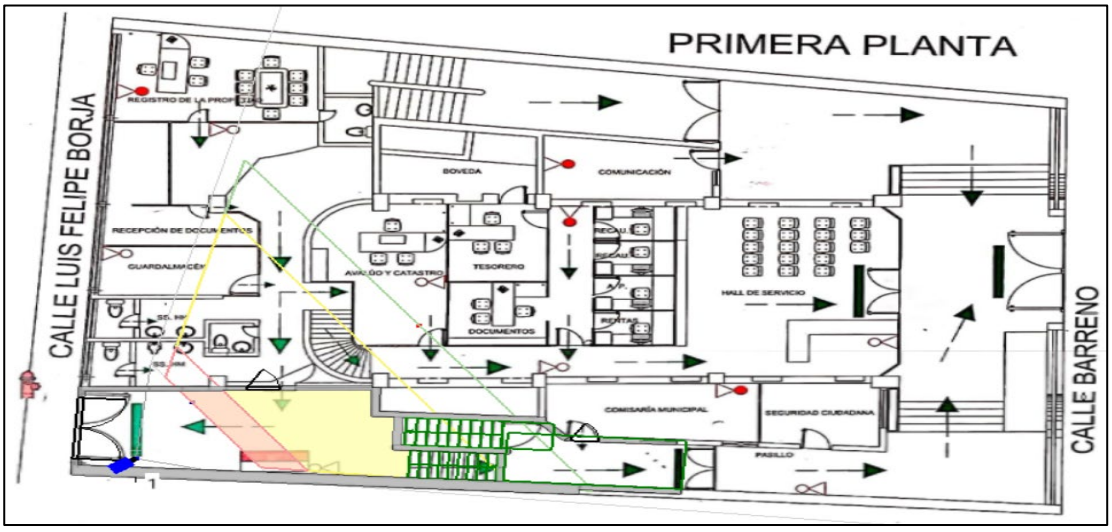
Entrada trasera primera planta

Plano en 2D

Se realiza la visualización del plano en 2D, utilizando la herramienta JVSG en cual nos permite identificar el área de cobertura que tiene la cámara, y está ubicada a una altura de 1.90 mts, permitiendo observar al personal que ingrese y salga de la bodega, así como también a los que salga de las oficinas del GAD Municipal de Saquisili.

Figura 51

Plano entrada trasera en 2D



Nota. La figura representa el área de cobertura de la cámara en la ubicación de la entrada trasera del municipio.

Visualización 3D

Para la visualización en 3D utilizamos la misma herramienta permitiendo obtener el área de cobertura que genera la cámara, de tal forma que podemos identificar el ingreso a bodega y a las diferentes oficinas de la primera planta.

Figura 52

Entrada trasera en 3D

Nota. La siguiente figura representa la visualización en 3D de la zona de la entrada trasera al municipio.

Requerimientos para la instalación de la cámara

Ubicación: entrada trasera primera planta

Altura: 2.5 metros

Resolución: 2MP

Alcance máximo de visualización: 30 metros

Marca: Dahua

Tipo: IP Domo

Modelo: DH-IPC-HDW1230T1-S4

Costo: 52.41$

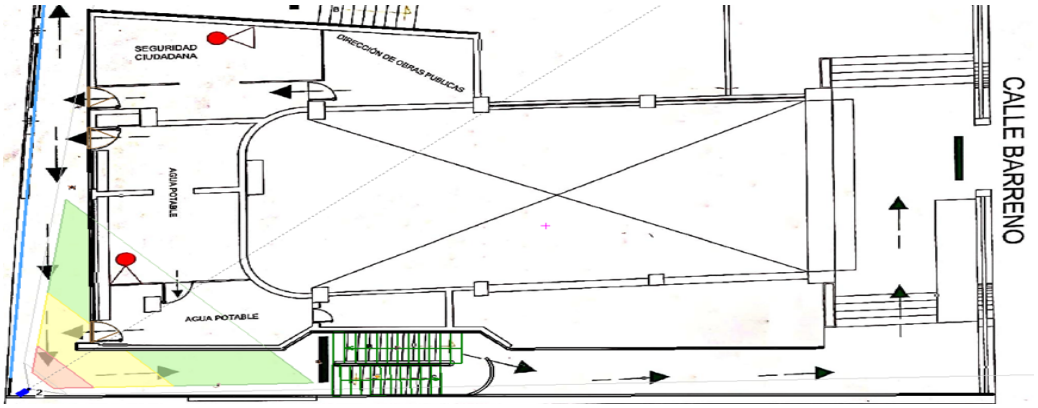
Pasillo secundario Segunda planta

Plano en 2D

Se realiza la visualización del plano en 2D utilizando la herramienta IP Video System Desing Tool, en cual nos permite identificar el área de cobertura que tiene la cámara desde el lugar donde será instalado la cámara permitiendo observar al personal que ingrese por el pasillo secundario a las oficinas.

Figura 53

Plano pasillo secundario 2D



Nota. Representa la cobertura que genera la cámara ubicada en el pasillo secundario de la segunda planta.

Visualización en 3D

De igual manera para la visualización en 3D utilizamos la misma herramienta permitiendo obtener el área de cobertura que genera la cámara, de tal forma que podemos identificar a las personas que ingresan a las oficinas ubicadas en la segunda planta y de igual manera a las personas que ingresen por las agras hacia el siguiente piso.

Figura 54

Pasillo secundario 3D

Nota. Representa la visualización en 3D en el área del pasillo secundario ubicado en la segunda planta.

Requerimientos para la instalación de la cámara

Ubicación: pasillo secundario segunda planta

Altura: 2.2 metros

Resolución: 2MP

Alcance máximo de visualización: 30 metros

Marca: Dahua

Tipo: IP Domo

Modelo: DH-IPC-HDW1230T1-S4

Costo: 52.41$

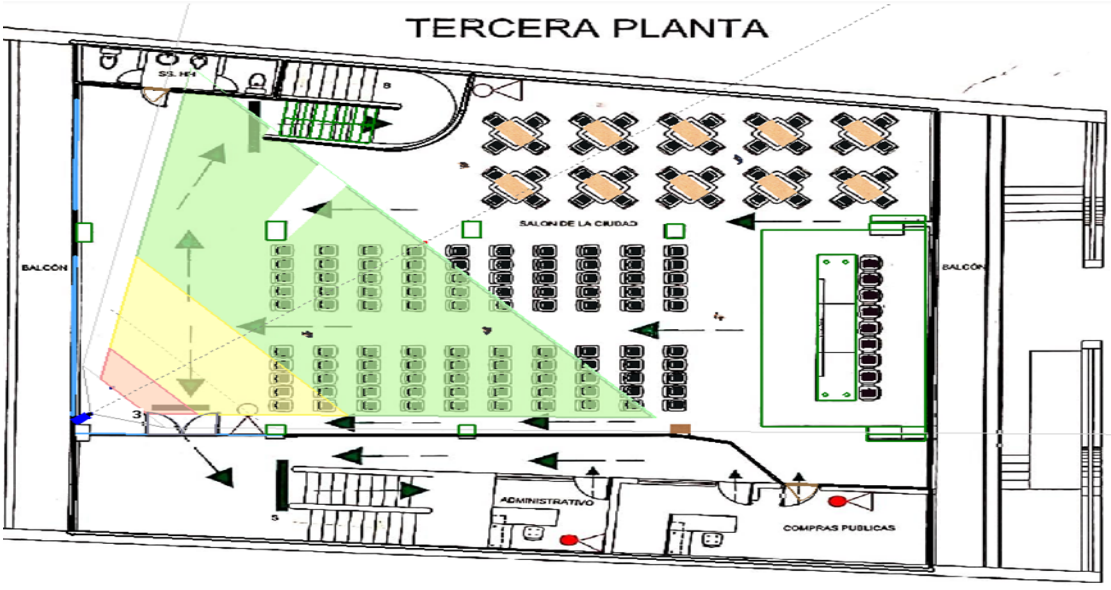
Salón de la ciudad Tercera planta

Plano en 2D

Se realiza la visualización del plano en 2D en la herramienta IP Video System Desing Tool donde se identifica el área de cobertura que tiene la cámara, desde el punto donde será instalado la cámara permitiendo identificar al personal que ingrese al salón de la ciudad como se muestra en la figura.

Figura 55

Plano salón de la ciudad 2D



Nota. La figura representa el área de cobertura en el plano del salón de la ciudad.

Visualización en 3D

Para esta visualización en 3D utilizamos la misma herramienta llamada IP Video System Desing Tool, nos permite identificar el área de cobertura que tiene la cámara y la captación de la imagen en una manera de tiempo real, permitiendo reconocer a las personas que ingresen a esta área.

Figura 56

Salón de la ciudad 3D

Nota. La figura representa la visualización en 3D de la cámara en el salón de la ciudad.

Requerimientos para la instalación de la cámara

Ubicación: salón de la ciudad Tercera planta

Altura: 2.5 metros

Resolución: 2MP

Alcance máximo de visualización: 30 metros

Marca: Dahua

Tipo: IP Domo

Modelo: DH-IPC-HDW1230T1-S4

Costo: 52.41$

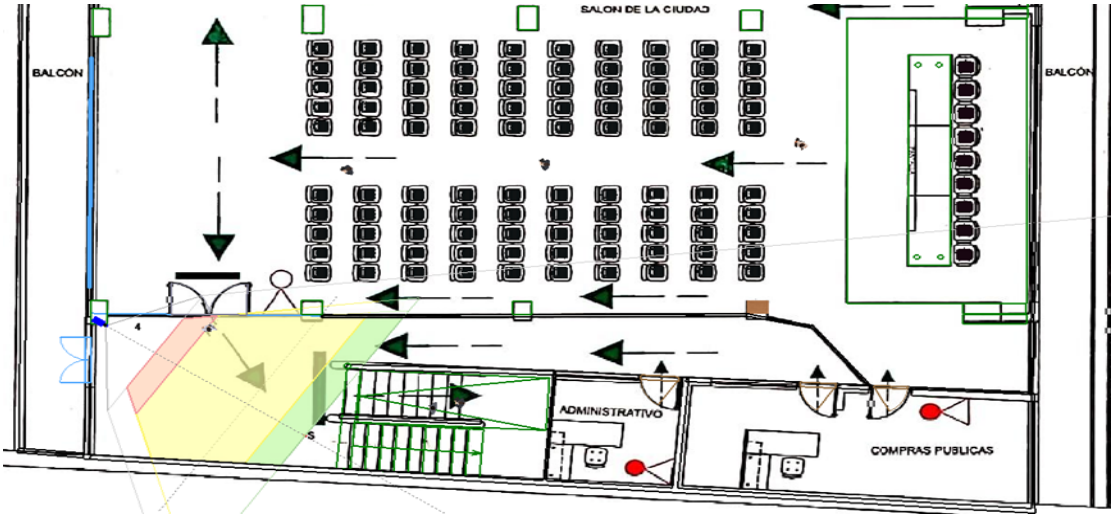
Pasillo Principal Tercera planta

Plano en 2D

Visualización en un plano en 2D, donde se identifica el área de cobertura que genera la cámara en el pasillo principal así mismo la ubicación del equipo en el lugar donde va ser implementada, de la misma manera se visualiza al personal que ingresa a salón de la ciudad, así como también a las personas que se dirijan a la oficina de Compras Públicas y a los que suban a la cuarta planta.

Figura 57

Plano pasillo Principal 2D



Nota. La figura representa el área de cobertura de la cámara en un plano en 2D del pasillo principal.

Visualización en 3D

Realización del plano en 3D con JVSG, para identificar el enfoque que tiene la cámara y la ubicación a una altura necesaria para visualizar el pasillo Principal de la tercera planta que permita la identificación de las personas que ingresen a las áreas de la tercera planta del GAD Municipal del cantón Saquisili.

Figura 58

Pasillo principal 3D

Nota. La figura representa una visualización en 3D del pasillo Principal Tercera Planta.

Requisitos para la instalación de la cámara

Ubicación: Pasillo Principal Tercera planta

Altura: 2.5 metros

Resolución: 2 MP

Alcance máximo de visualización: 30 metros

Marca: Dahua

Tipo: IP Domo

Modelo: DH-IPC-HDW1230T1-S4

Costo: 52.41$

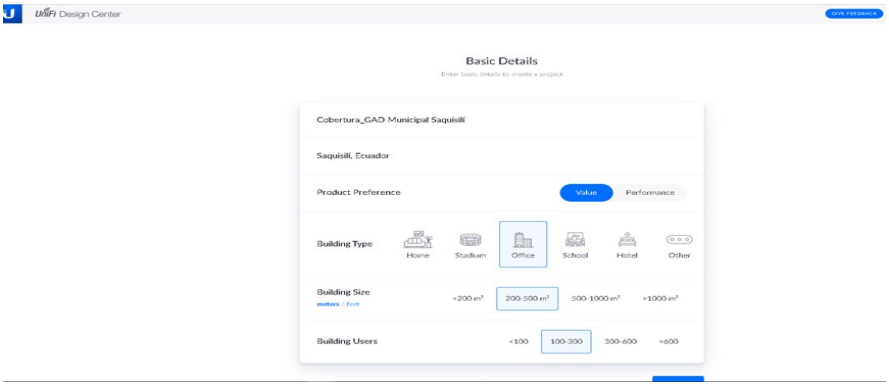
Diseño de la zona de cobertura del AP

Luego de haber escogido el equipo para la seguridad inalámbrica se procede a realizar una simulación utilizando la página web Unifi Design Center en el cual podemos subir los planos de cualquier entidad para poder diseñar la red inalámbrica, esta herramienta nos permite colocar los APs ayudándonos a tener una idea de cobertura que podemos obtener ayudándonos a tener una colocación óptima del equipo.

Para la visualización de la zona de cobertura del Access Point procedimos a crear un nuevo proyecto en el cual colocamos las especificaciones en este caso el nombre del proyecto será Cobertura GAD Municipal Saquisilí, y de esta manera llenamos los campos correspondientes con la información respectiva para la planificación de la red WLAN.

Figura 59

Especificaciones para la cobertura del GAD Municipal del cantón Saquisili

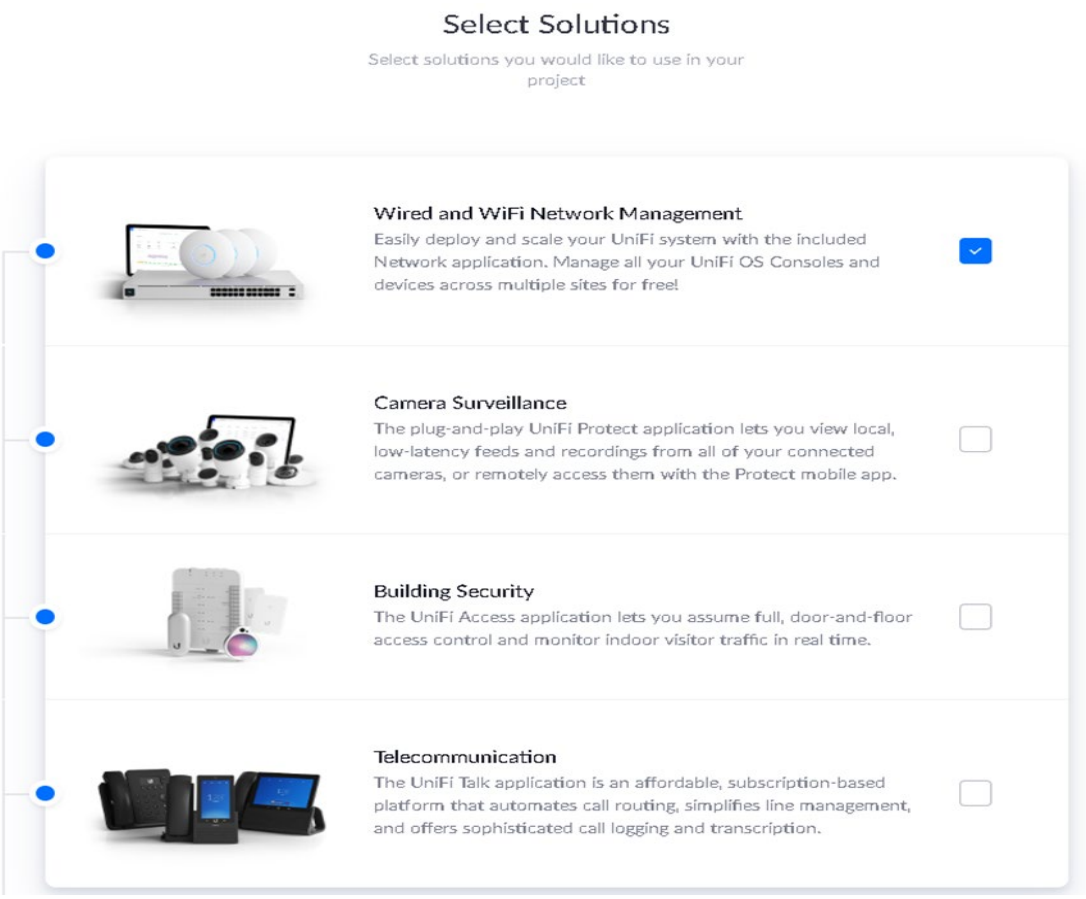


Nota. La siguiente figura representa las respectivas especificaciones para la cobertura de red del GAD Municipal de Saquisili.

Después de haber presionado next procedimos a seleccionar los equipos que se va a utilizar para la planificación de la red WLAN, en esta sección escogimos la parte de Wired and Wifi Network Management y presionamos next.

Figura 60

Selección del equipo

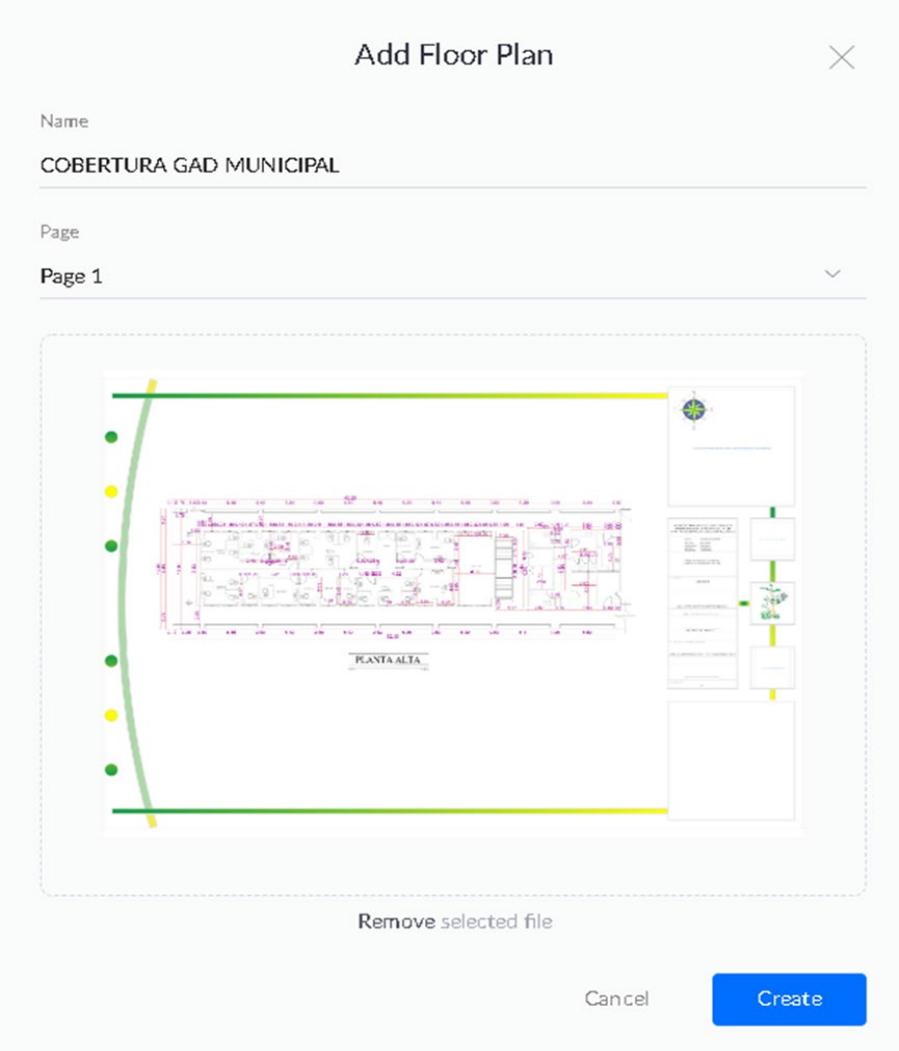


Nota. La siguiente figura representa la selección de equipos inalámbricos.

En esta ventana procedemos a seleccionar plano del municipio en este caso es de la planta alta del edificio San Juan Bautista por el motivo que la cobertura de la red WLAN se necesita para la zona de sala de reuniones, de la misma manera colocamos el nombre de COBERTURA GAD MUNICIPAL y presionamos en créate para generar el área de trabajo de la planificación de la red WLAN para las instalaciones.

Figura 61

Selección del plano



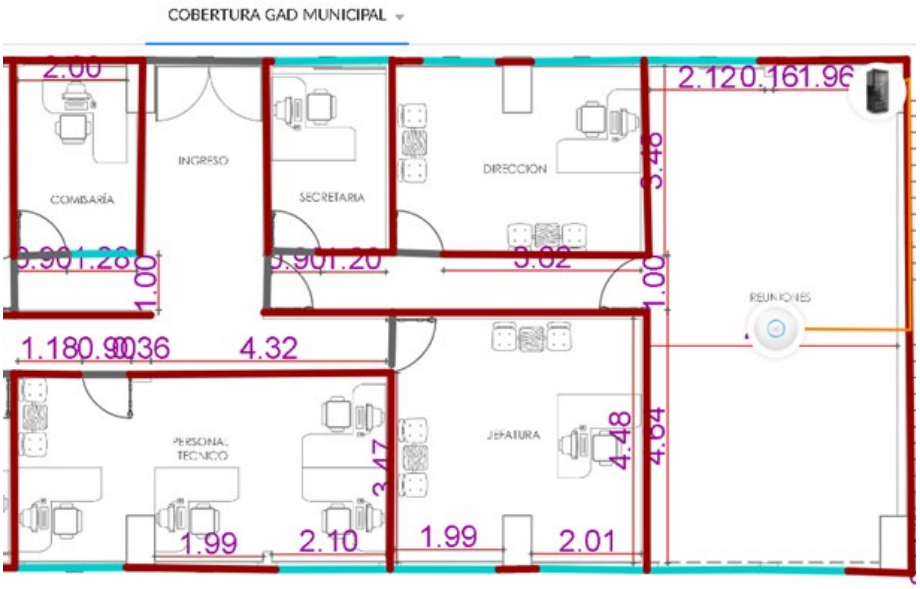
Nota. La figura representa la selección del plano para la ubicación del equipo inalámbrico.

Se procede a dibujar nuevamente las paredes en el plano, también dibujamos las puertas y ventanas para que los equipos puedan diferenciar cuales son cada uno de estos parámetros en el plano y de esta manera poner comprobar el nivel de señal que llega a cada parte del plano de la casa y poder comprobar si se necesita aumentar más puntos de acceso o moverlos previamente para que los cubra todo y no existan puntos muertos.

Una vez terminada con la elaboración de las paredes, puertas y ventanas procedimos a colocar el equipo inalámbrico en el plano con su respectivo cableado desde el rack como se muestra en la figura.

Figura 62

Rediseño del plano para la colocación del equipo inalámbrico



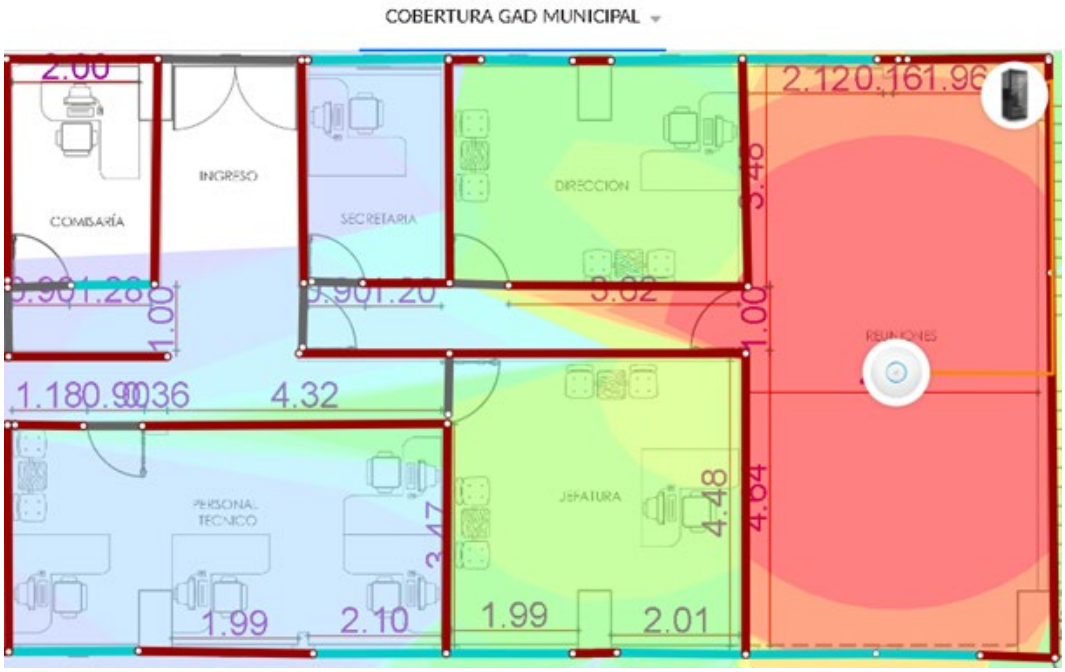
Nota. La siguiente figura muestra el rediseño del plano para la simulación de la cobertura de red que genera el equipo inalámbrico.

Como parte final se procede a simular para visualizar la señal que llega del Access point a la sala de reuniones y de esta manera ver si es necesario aumentar más Access point para

cubrir las zonas muertas donde no hay señal de la red la simulación lo realizamos en el canal de operación de 2.4 GHz tomando en cuenta que el equipo seleccionado trabaja en esta frecuencia como se muestra en la figura.

Figura 63

Simulación del Access Point



Nota. La figura representa la cobertura que genera el equipo inalámbrico ubicado en sala de reuniones.

Configuración de las cámaras IP

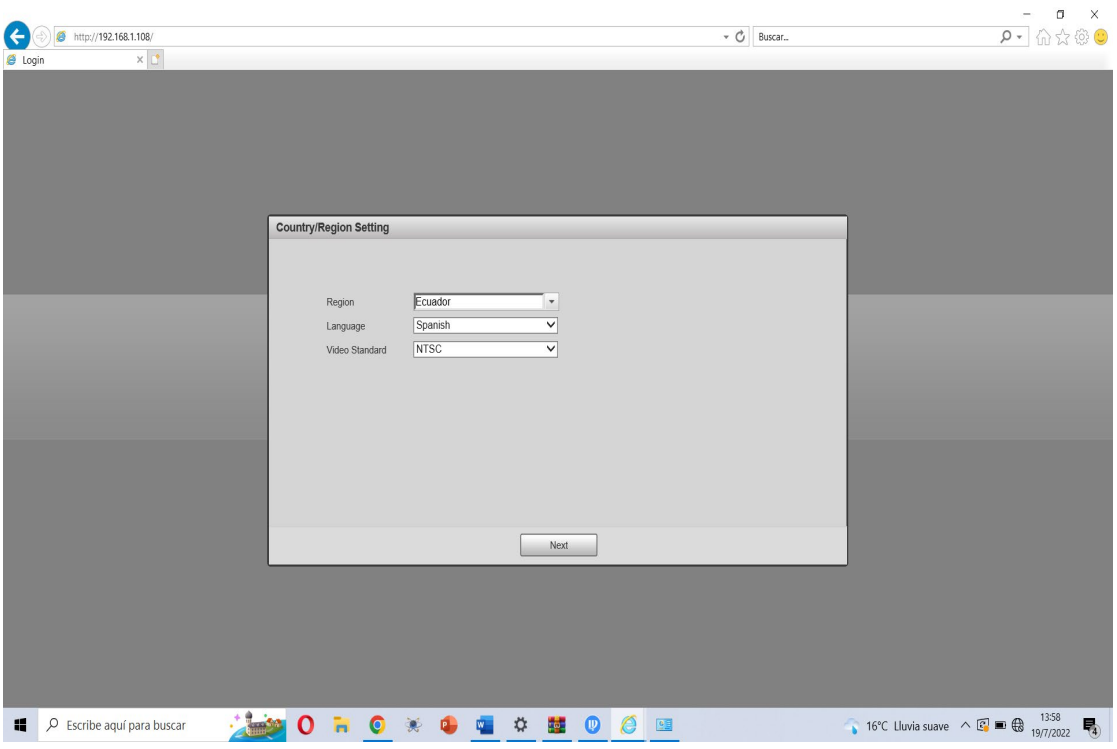
Concluido con los diseños de las zonas de cobertura tanto de las cámaras IP como del Access Point y finalizado con la instalación de las cámaras IP se realizó la configuración de cada uno de los equipos ubicados en los distintos puntos.

Empezamos alimentando la cámara y la conectaremos a la red local mediante un cable de red, accediendo por medio de un sitio web con la IP 192.168.1.108 ya que esta es la dirección IP por defecto del equipo, permitiéndonos con la inicialización del equipo. Si la red está en un rango distinto utilizaremos la herramienta ConfigTool para poder cambiar la configuración de red de la cámara.

A continuación, empezaremos eligiendo el país y la región en la que se encuentre.

Figura 64

Ajuste de país y región

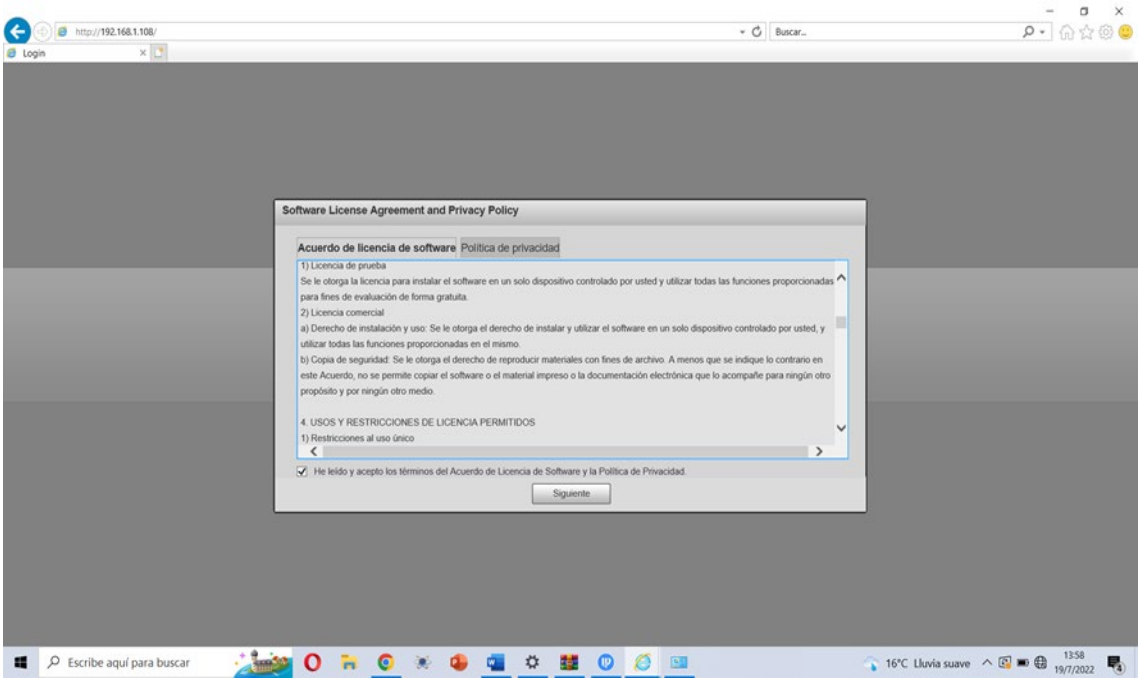


Nota. La figura muestra el país y la región en donde será configurada la cámara.

Luego se nos presenta los términos de licencia del software del equipo, aceptamos los términos del software y políticas de privacidad del equipo. Ya realizado eso se presiona next para continuar con la configuración.

Figura 65

Acuerdo de licencia de software y políticas de privacidad

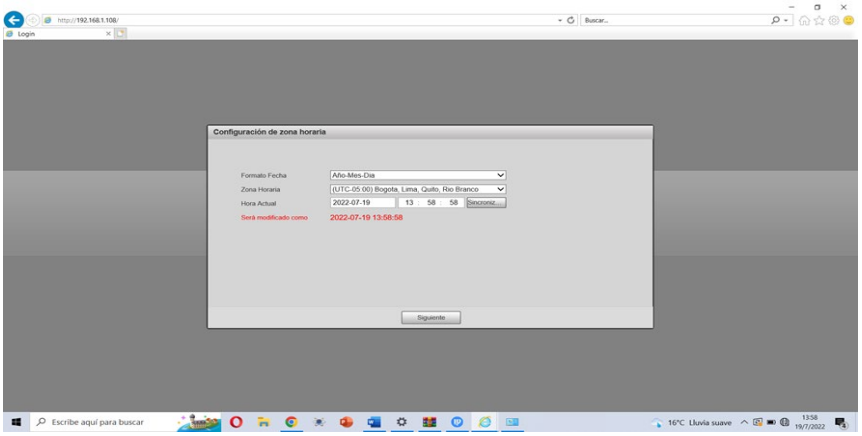


Nota. Aceptar el acuerdo de licencia de software y política de privacidad para poder continuar con la configuración.

Continuamos con la configuración de la zona horaria, elegimos un formato de fecha (Año-Mes-Día), seleccionamos la zona horaria correspondiente y finalmente presionamos sincronizar para obtener la hora actual, ya realizado estos pasos procedemos a presionar siguiente como se muestra en la figura.

Figura 66

Configuración de zona horaria

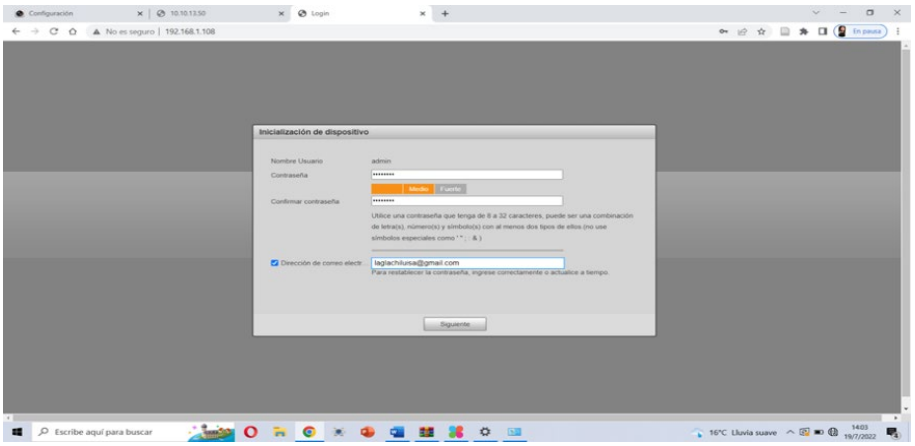


Nota. Configuración de la zona horaria de acuerdo al país en que se encuentra.

Continuamos con la parte de inicialización el cual nos solicita que creemos la contraseña del usuario admin, se procedió a generar una contraseña que debe constar de un mínimo de 8 caracteres, y tenemos que mezclar letras y números, al final se coloca un correo electrónico el cual nos ayudara a restablecer la contraseña en caso de que fuera olvidada ya realizado esto procedemos a la siguiente ventana.

Figura 67

Inicialización del dispositivo

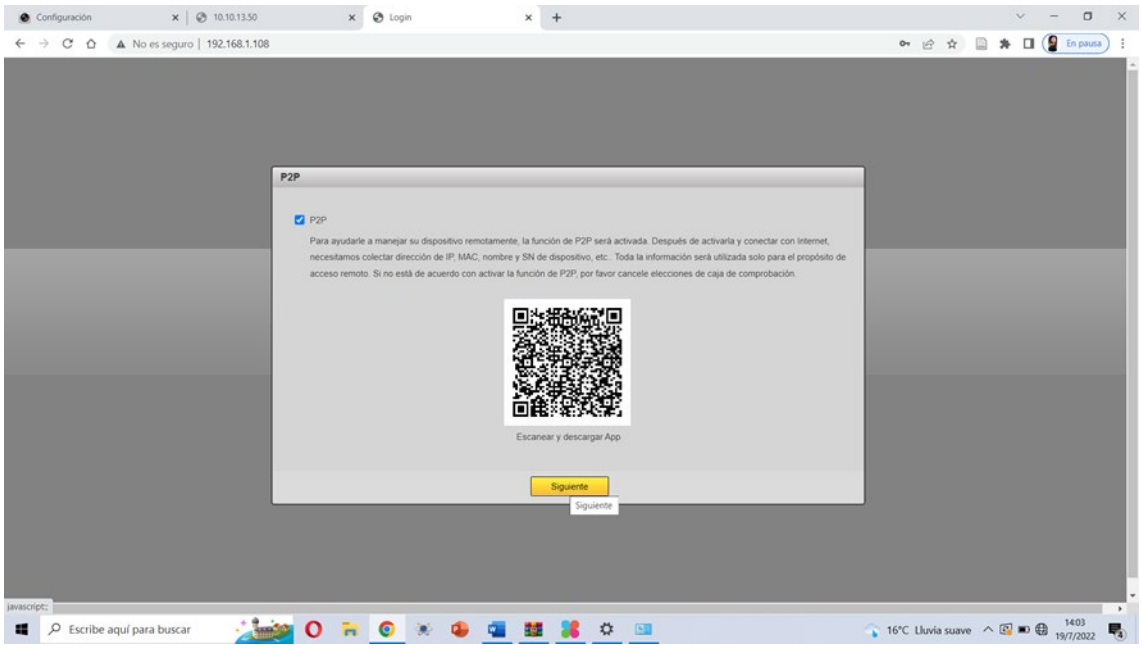


Nota. La figura muestra la inicialización de la cámara con una contraseña nueva y la colocación de un correo electrónico.

En esta ventana se nos genera un código QR el cual nos permitirá manejar el dispositivo remotamente ya que la función P2P será activada. Ya seleccionado la opción procedemos a presionar siguiente.

Figura 68

Código de escaneo P2P

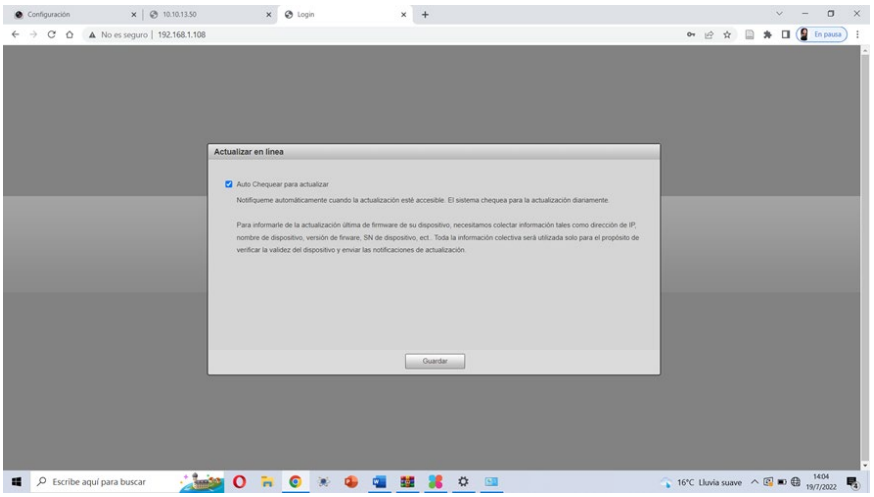


Nota. La figura muestra un código QR, esta opción debemos desactivarla debido a q se integrará a un NVR.

Finalmente, se nos presenta la ventana de la actualización del software del equipo, en este caso la opción de actualización viene marcado por defecto. Concluido esta sección presionamos en guardar como se muestra en la figura.

Figura 69

Actualización en línea

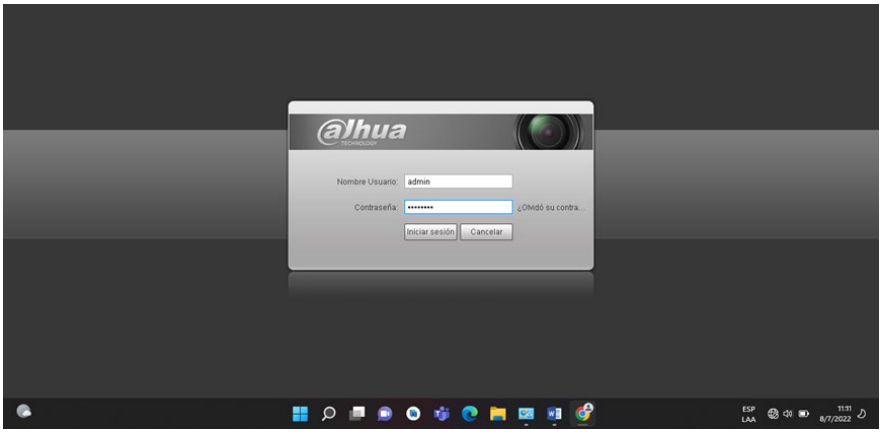


Nota. La figura nos presenta las actualizaciones que serán notificadas al usuario.

Nos aparecerá la página de login donde pondremos el usuario y la contraseña que hemos creado al principio el cual nos permitirá acceder a la parte de configuración de la cámara respectivamente.

Figura 70

Login de la cámara



Nota. La figura presenta el login para ingresar a la cámara.

Establecemos parámetros de red en el menú Network. En TCP/IP podremos configurar IP, máscara de subred, la puerta de enlace y servidores DNS según la Tabla., en la cual serán designadas a las diferentes cámaras.

Tabla 9

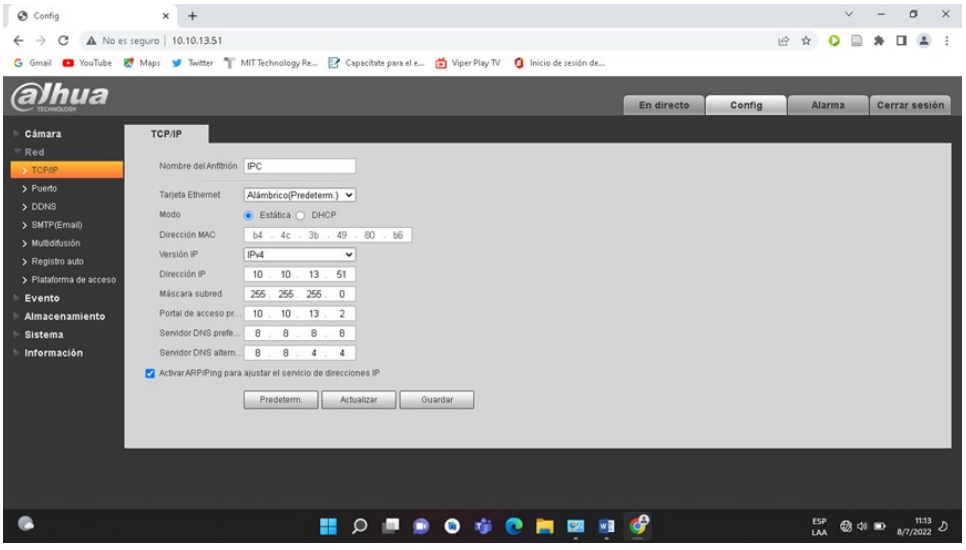
IP designada para cada cámara

Nombre (cámara)	IP	Máscara de Subred	Gateway
Entrada trasera 1er Piso	10.10.13.50	255.255.255.0	10.10.13.2
Pasillo 2do Piso	10.10.13.51	255.255.255.0	10.10.13.2
Salón de la ciudad 3er Piso	10.10.13.52	255.255.255.0	10.10.13.2
Pasillo principal 3er Piso	10.10.13.53	255.255.255.0	10.10.13.2

Nota. La tabla representa las direcciones IP que serán asignadas a cada uno de los equipos instalados.

Figura 71

Configuración direccionamiento IP de la cámara

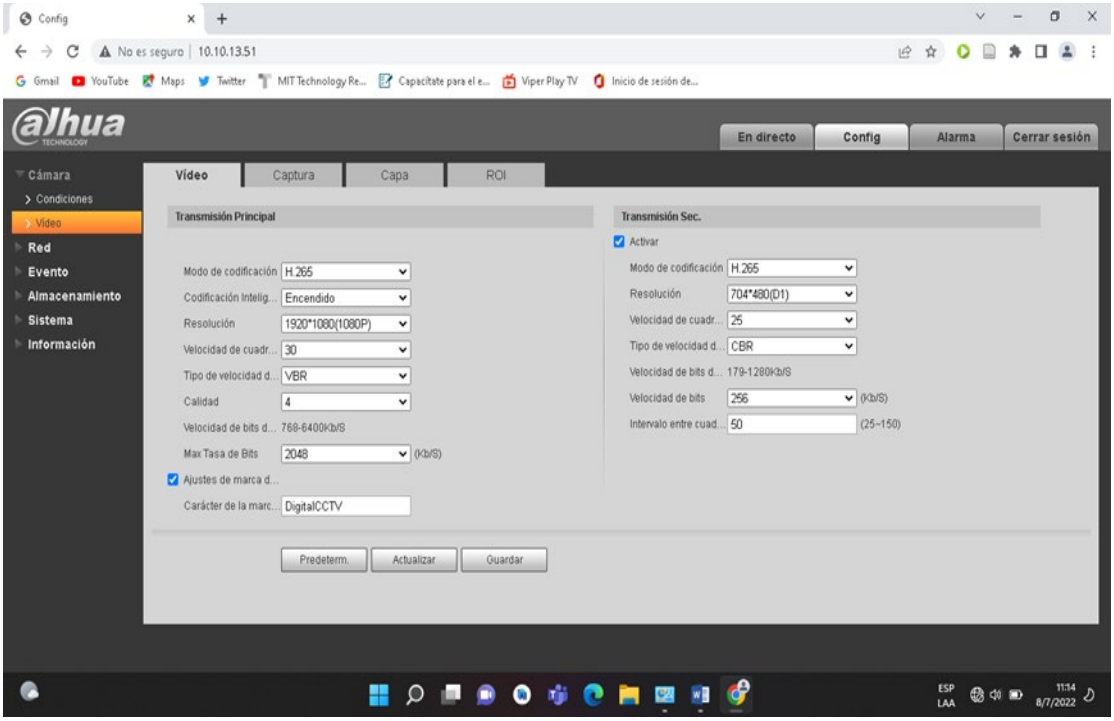


Nota. En la figura se muestra la configuración de IP según la tabla.

Configuramos la transmisión principal y secundaria como se muestra en la Figura. para poder visualizar con una mejor resolución la cámara el cual permitirá que las imágenes capotadas por la cámara tendrán mayor nitidez para la visualización.

Figura 72

Configuración de video de la cámara

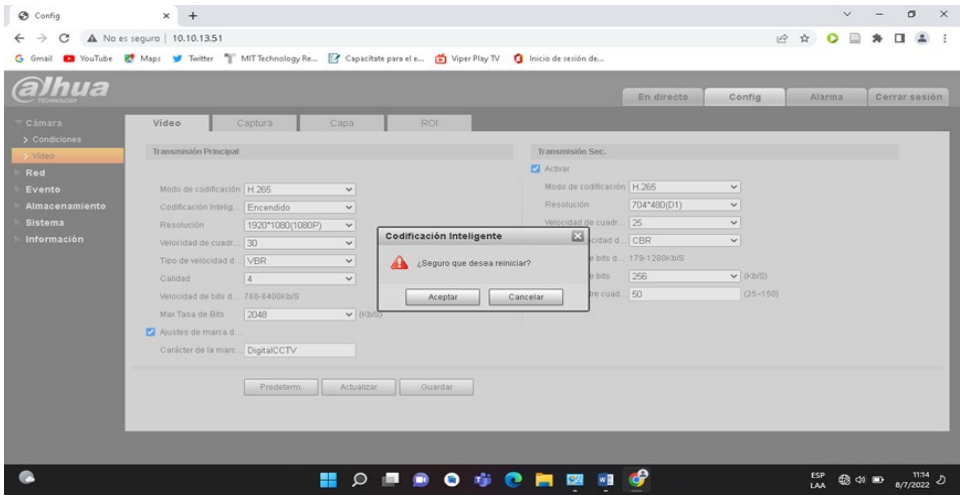


Nota. En la presente figura se muestra la configuración de video de la transmisión principal y secundaria de la cámara.

Una vez culminada con el paso anterior procedemos a guardar los cambios el cual tarda unos minutos hasta que el equipo inicialice nuevamente con los datos ingresados para el funcionamiento en la red que ya se encuentra en el municipio.

Figura 73

Guardar cambios



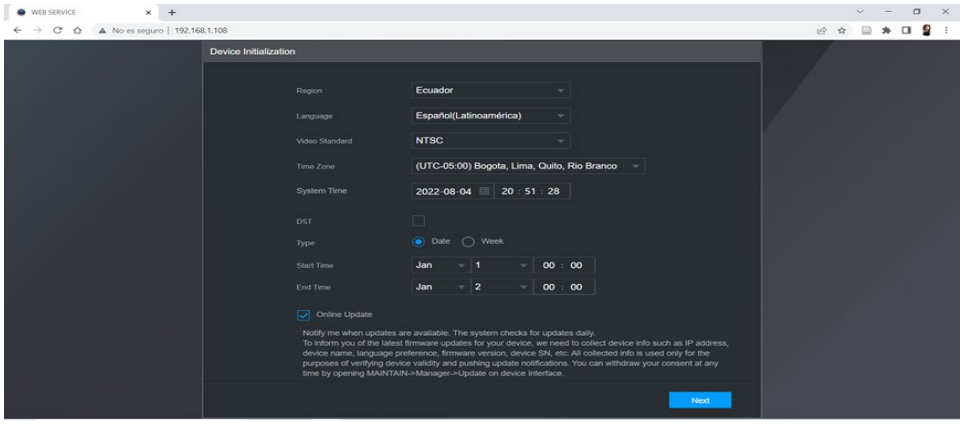
Nota. El dispositivo se reiniciará una vez guardado los cambios.

Configuración del NVR

Empezamos con la inicialización del equipo, estableciendo su zona horaria correctamente para garantizar una sincronización precisa. Cuando termine, haga clic en siguiente para continuar.

Figura 74

Inicialización del NVR

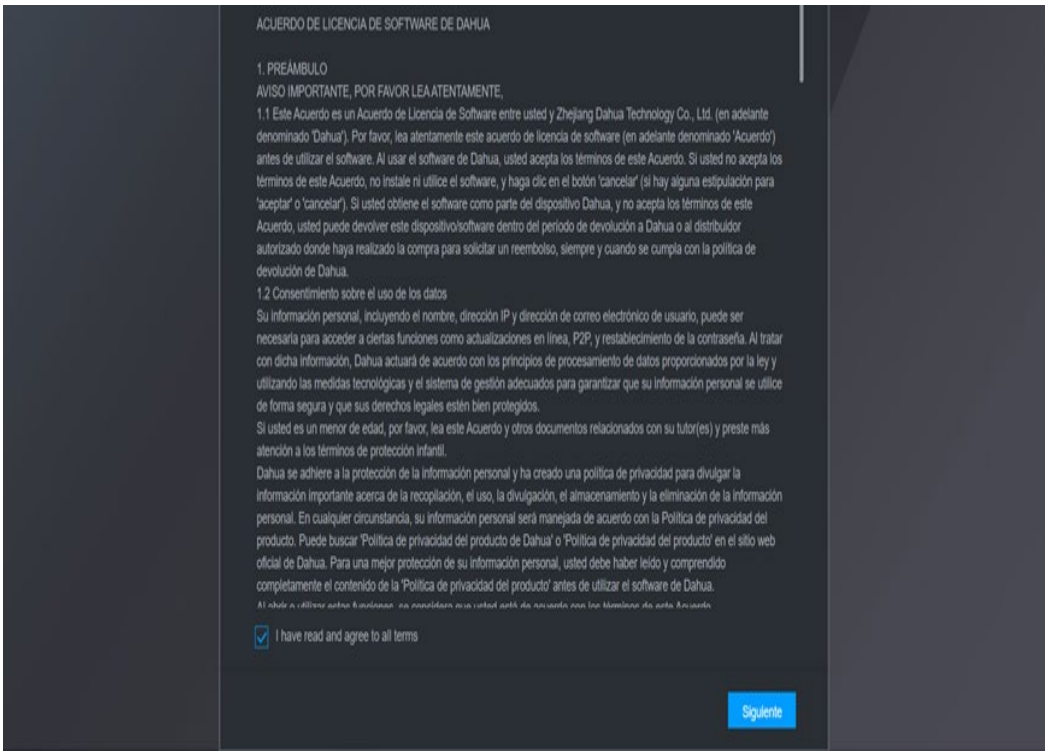


Nota. En la figura se indica el estándar de video y la zona horaria en la que se encuentra el equipo.

Seguidamente lea el acuerdo de licencia de usuario final marcamos la casilla aceptaremos del acuerdos y términos de licencia de software de Dahua para que se habilite la opción de siguiente.

Figura 75

Acuerdo de licencia de software de Dahua

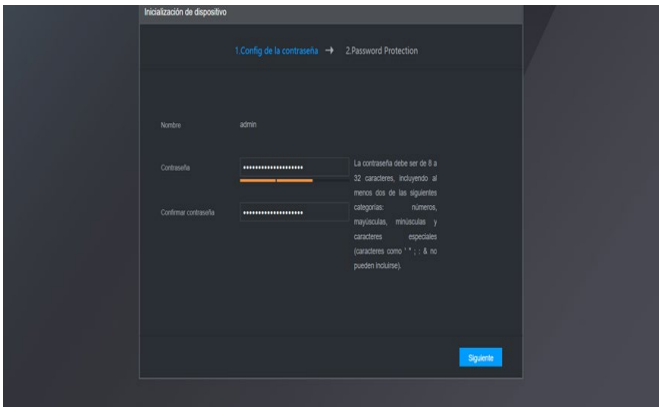


Nota. Es necesario leer los acuerdos y términos para su uso y consentimiento de los datos.

Establecemos una contraseña de inicio de sesión de admin para la seguridad del dispositivo asegúrese de que tenga al menos 8 caracteres y que contenga letras, números y símbolos. (Al menos dos de los tres tipos)

Figura 76

Creación de contraseña

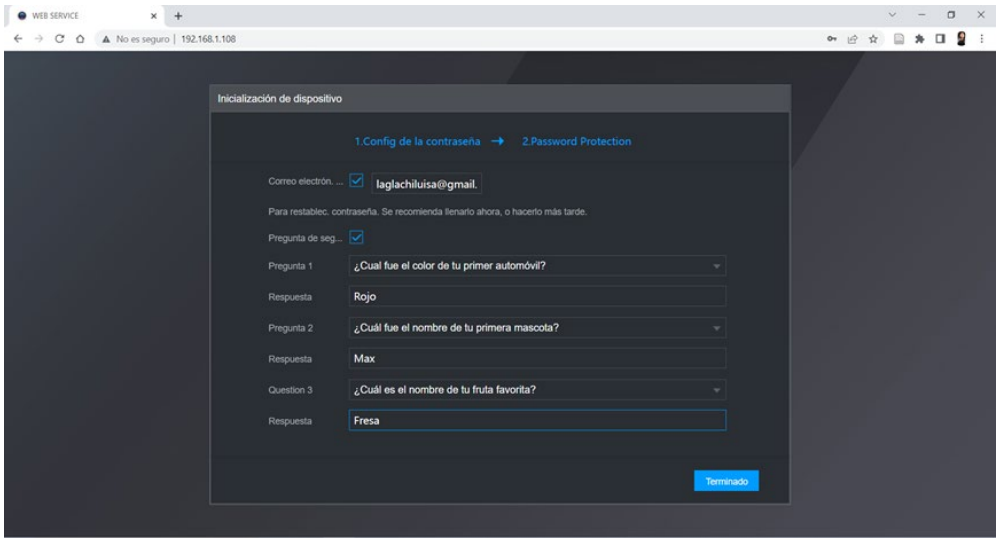


Nota. Para la seguridad del equipo es necesario cambiar con regularidad la contraseña de inicio de sesión del administrador.

Luego de establecer la contraseña, el equipo pasa a la siguiente interfaz en donde ingresaremos una dirección de correo electrónico, opcional responder las preguntas de seguridad para restablecer administración contraseña.

Figura 77

Ingreso de correo electrónico y respuestas de preguntas

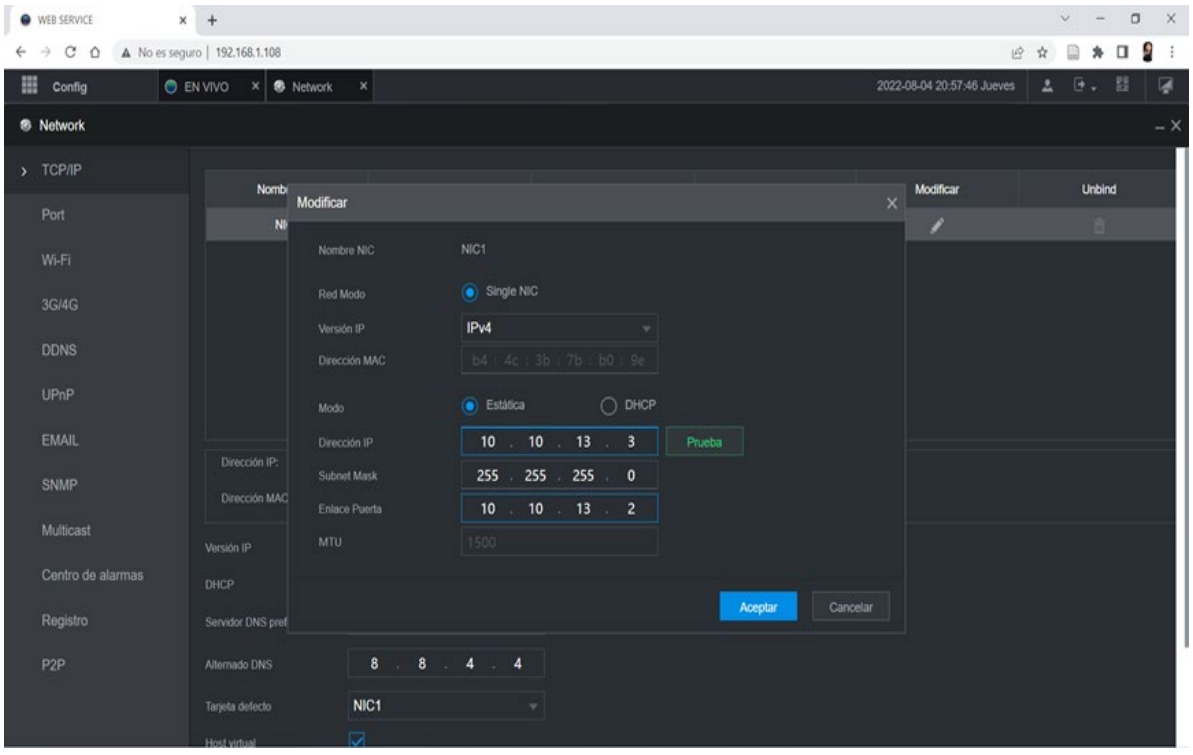


Nota. Es la única opción si olvida su contraseña y omite este paso.

Una vez inicializado el equipo deshabilitaremos el DHCP y procedemos a cambiar la dirección IP, mascara de subred y la puerta de enlace manualmente, en el mismo segmento en que se encuentra la red del GAD municipal del cantón Saquisili.

Figura 78

Asignación de dirección IP



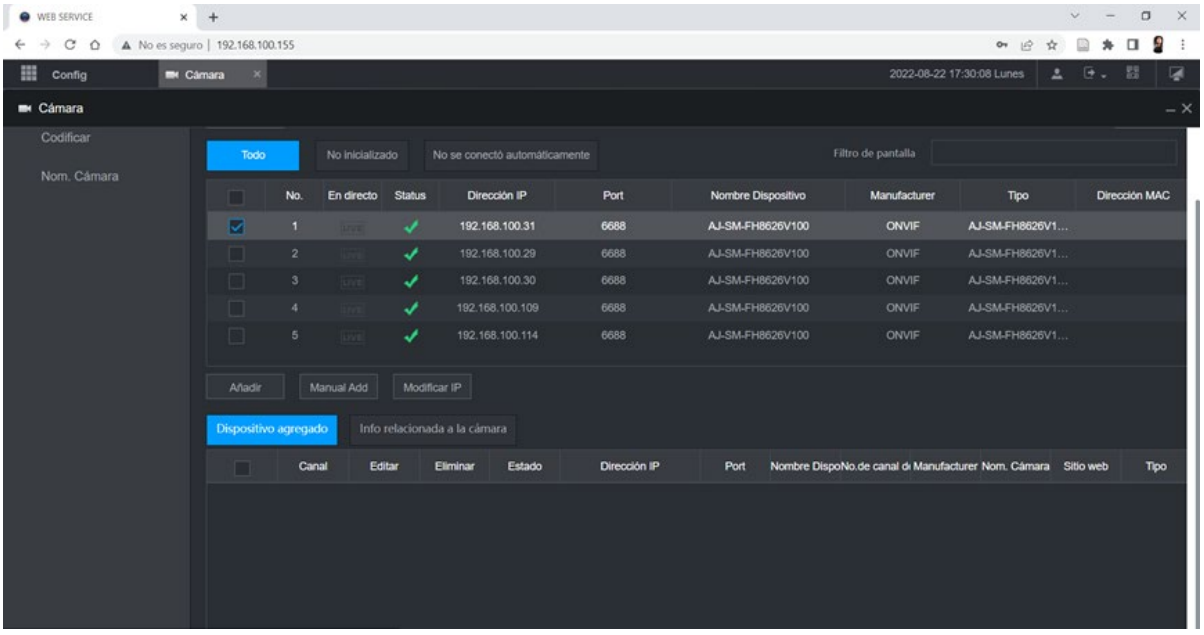
Nota. El NVR no sede mantener configurada en la misma dirección IP asignada a otro dispositivo en la red.

Empezaremos a buscar las cámaras que están en la red en este caso se observara las que fue colocada en las instalaciones del Gad Municipal de Saquisilí, cuando termine el

proceso de búsqueda se mostrara el nombre de la cámara, la dirección IP, tipo de cámara, el puerto.

Figura 79

Búsqueda de cámaras en la red

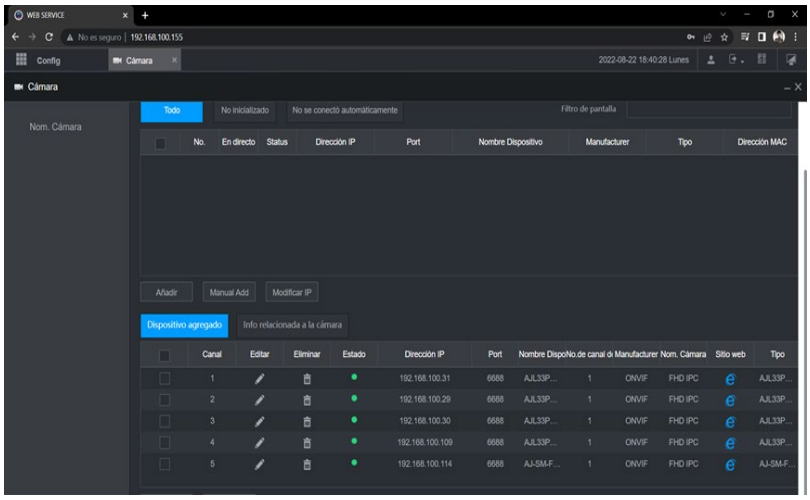


Nota. Al momento de añadir cada cámara debemos colocar la contraseña con la que se inicializo la cámara.

Finalmente debemos esperar a que la conexión se genere y el botón de estado se vuelva a color verde, una vez este color verde finalmente nos asigna un canal podemos visualizar el canal.

Figura 80

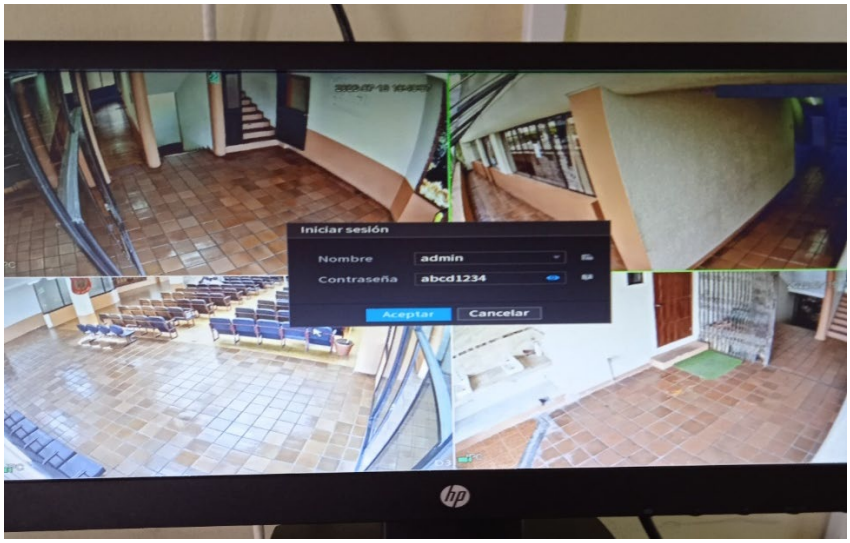
Cámaras en estado en funcionamiento



Nota. En la siguiente figura se visualiza el listado de las cámaras agregadas al NVR.

Figura 81

Visualización de las cámaras en los puntos estratégicos



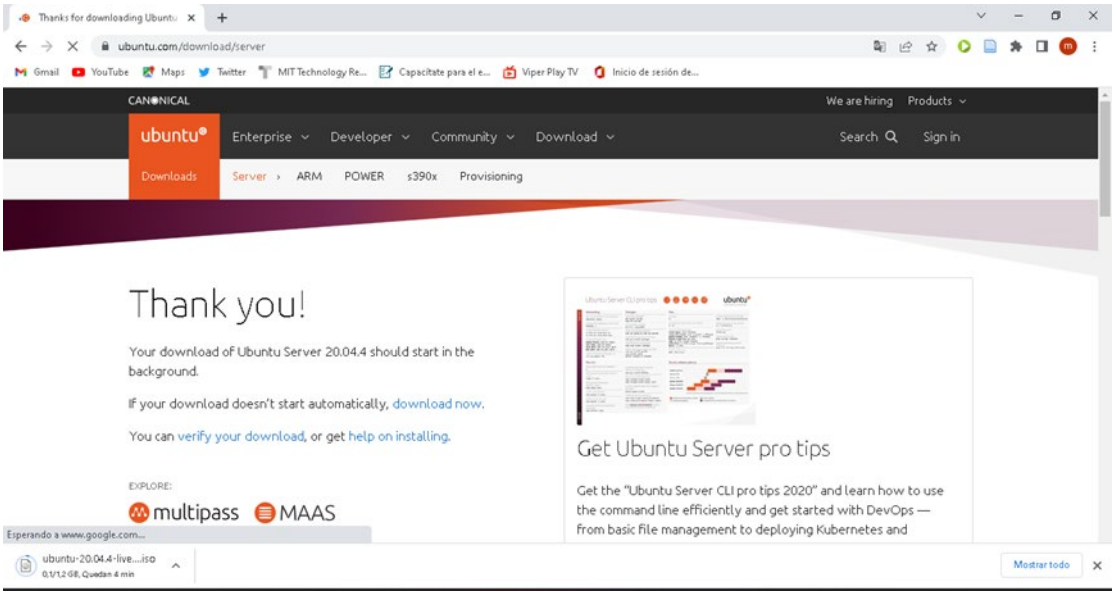
Nota. Visualización de las cámaras que se agregadas al NVR en la red del GAD municipal del cantón Saquisili.

Instalación del sistema operativo

Para la instalación del sistema operativo debemos tener en cuenta los requerimientos mínimos que necesita el sistema operativo para funcionar correctamente, para ello es necesario descargar la imagen ISO del sistema que se va a utilizar en este caso será Ubuntu server 20.04 LTS, el cual se encuentra en la siguiente página web https://ubuntu.com/download/server en donde podemos encontrar diferentes opciones, se selecciona la correcta y se procede a descargar.

Figura 82

Página web de descarga de la imagen ISO



Nota. Página para descargar Ubuntu server 20.04 LTS.

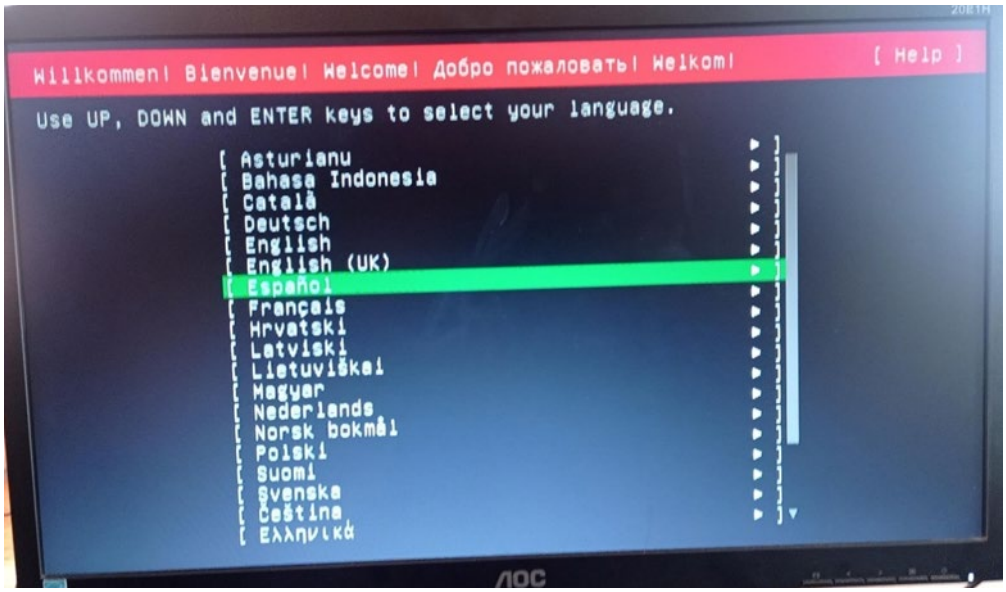
Primero deberemos instalar la imagen ISO descardada en una memoria USB con capacidad de 4 GB o superior. Una vez finalizado el grabado de la imagen ISO en la USB se procede a arrancar la BIOS de la máquina para poder configurar el orden de arranque, con la

finalidad que en el equipo arranque el sistema operativo almacenado. Ya culminado el paso se procede a reiniciar la máquina para poder continuar con la configuración del sistema operativo.

Ya arrancado el equipo nos aparece el asistente de configuración de Ubuntu Server. se nos presenta la primera ventana en el cual nos aparece las opciones de idiomas que podemos utilizar en el sistema operativo, esta ventana procedemos a seleccionar el idioma español para que el sistema se encuentre en este idioma.

Figura 83

Configuración de idioma

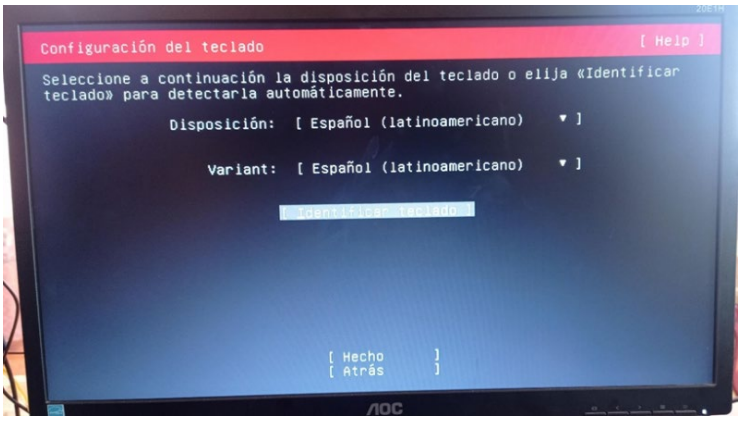


Nota. La figura representa la venta principal de configuración del sistema operativo.

Luego se procede a elegir que la configuración del teclado esté en español, este apartado es el más importante de tal forma que se va a utilizar para ejecutar los diferentes comandos. En la opción de Disposición presionamos enter y se elige la opción de español. Así mismo en la sección Variant deberemos escoger exactamente lo mismo.

Figura 84

Configuración del teclado



Nota. Ventana de disposición y variante del teclado

Se procede a las configuraciones de la red en esta sección lo dejamos de forma predeterminada el nombre red, en este caso es enp0s18, y la configuración predeterminada es la de cliente DHCP. De tal manera que se podrá modificar en todo momento la configuración de la red, tanto a nivel de IPv4 como de IPv6. De acuerdo a lo que se requiera para el servidor.

Figura 85

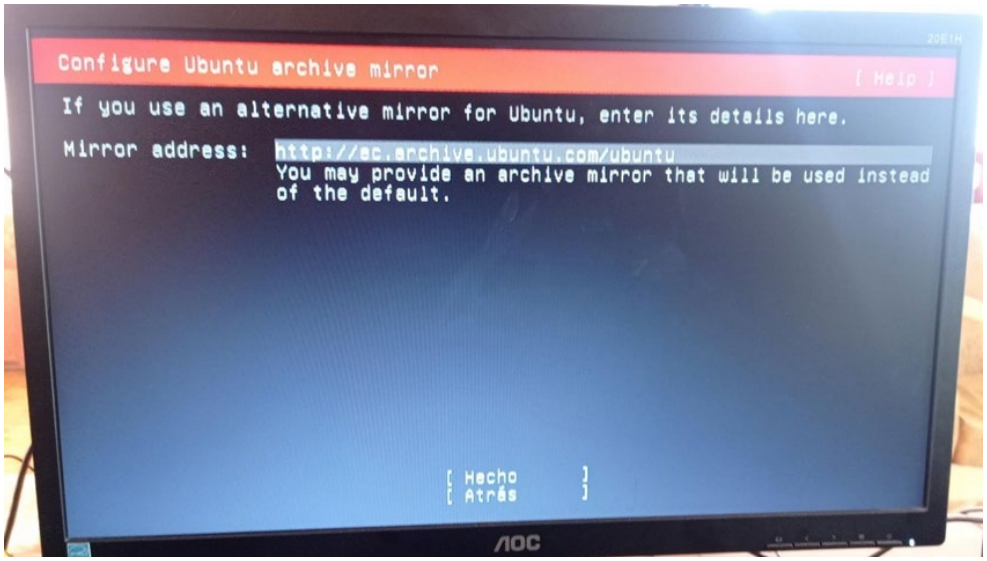
Configuración de la red del sistema operativo

Nota. En la figura se muestra la tarjeta de red y la IP designada al equipo

En la siguiente ventana nos presenta la configuración del archivo mirror en el cual se procede a dejar por defecto ya que el link del repositorio pertenece a ecuador de tal manera que podemos descargar las actualizaciones de este repositorio y procedemos a seleccionar en la opción de hecho.

Figura 86

Configuración archivo mirror

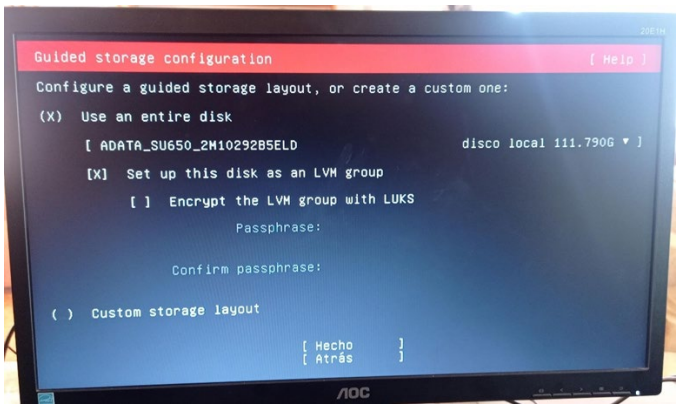


Nota. Configuración del archivo mirror de Ubuntu para la descarga de actualizaciones desde los repositorios.

Una de las partes más importantes es la configuración de la memoria. Le recomendamos que instale el sistema operativo en un disco específico. Esto es para tener varios discos para almacenamiento posterior para evitar cualquier interferencia que pueda afectar el dispositivo. Como regla general, instale el sistema operativo en una unidad SSD para que todo funcione lo más rápido posible. Esta ventana de configuración de Ubuntu Server le permite seleccionar el disco para instalar. También puede crear particiones de disco usted mismo de forma avanzada.

Figura 87

Guía de configuración de particiones



Nota. Configuración del almacenamiento para el funcionamiento del SO.

Una vez configurado, nos genera un resumen del sistema de archivos, el arranque y todo lo que hemos configurado previamente para el funcionamiento del servidor. Una vez que hayamos revisado todo, presionamos en la opción hecho para continuar.

Figura 88

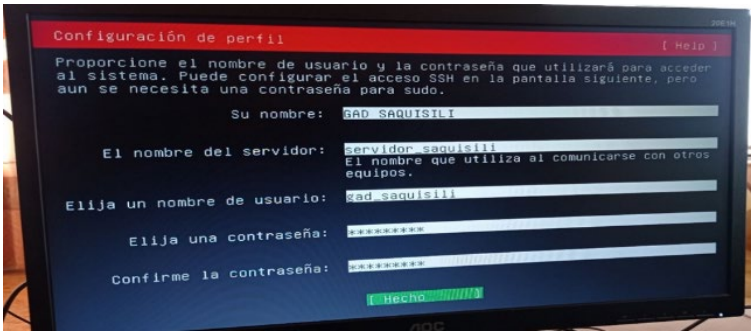
Resumen del sistema de archivos

Nota. Ventana de resumen de la partición de discos del servidor para el funcionamiento correcto.

Ya finalizado con la configuración del almacenamiento tenemos que generar un nombre, el nombre al servidor, nombre del usuario y su contraseña de acceso. Una vez que hayamos hecho toda la configuración respectiva, procedemos a seleccionar la opción hecho y pulsamos y presionamos enter para proceder con la instalación sistema operativo.

Figura 89

Configuración del perfil



Nota. Configuración de los nombres y sus respectivas contraseñas para el servidor.

Finalmente comienza el proceso de instalación y en unos minutos lo tendremos instalado. Al no contar con una interfaz gráfica de usuario la instalación es realmente rápida, cuando la instalación haya culminado el equipo solicitara que reiniciemos el sistema.

Figura 90

Instalación del sistema

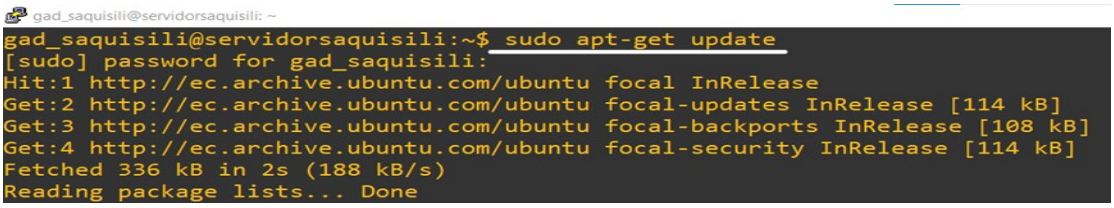
Nota. La figura representa la instalación del sistema operativo una vez culminada las configuraciones del servidor.

Instalación y configuración del servidor Freeradius

Culminado con la instalación de sistema operativo y revisado su funcionamiento correctamente se procede a la instalación del servidor donde se procedió a ingresar el comando sudo **apt-get update**, mediante este comando se empezará a descargarse todas las actualizaciones requeridas por el sistema operativo.

Figura 91

Actualización de paquetes disponibles y sus versiones

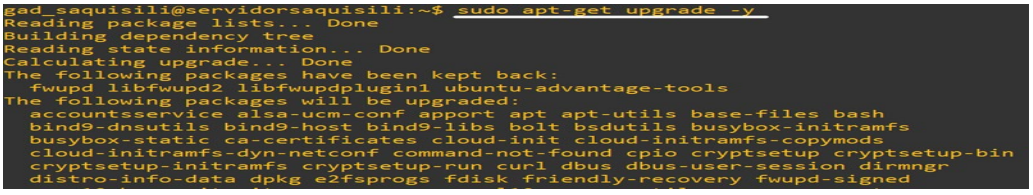


Nota. El siguiente comando ayuda a descargar todas las actualizaciones correspondientes para el sistema operativo.

Finalizado las descargas de las actualizaciones del sistema operativo procedemos a ingresar el siguiente comando **sudo apt-get upgrade -y**, este comando nos ayudara a subir a la última versión del sistema instalado.

Figura 92

Actualización de paquetes y programas que tenemos instalados

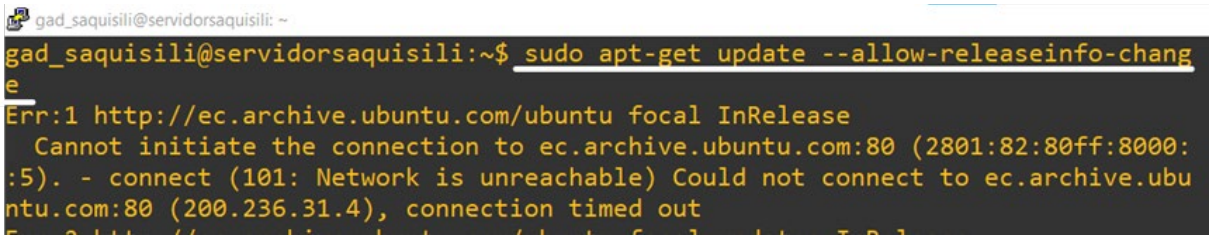


Nota. El siguiente comando ayuda a subir la última versión del sistema que se encuentra instalado.

Finalizado la actualización de la última versión se procede a ingresar el siguiente comando **sudo apt-get update--allow-releaseinfo-change**, este comando nos ayudara que la actualización continúe descargándose de un repositorio que cambio su información de la versión contenida en el repositorio anterior.

Figura 93

Actualización de repositorios

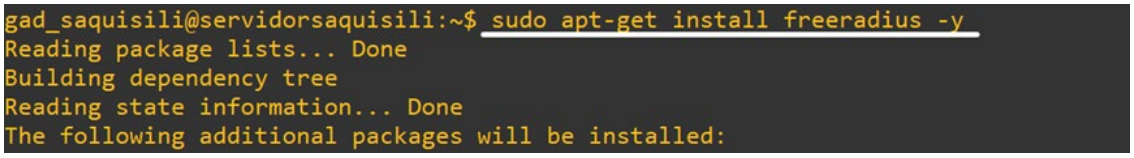


Nota. Este comando representa la descarga de actualizaciones recientes desde un directorio con información actualizada.

Culminada las descargas de los repositorios procedemos a la instalación del servidor freeradius por medio del comando **sudo apt-get install freeradius –y,** en este paso debemos esperar a que se instalen todos los paquetes correspondientes del servidor freeradius.

Figura 94

Instalación servidor freeradius

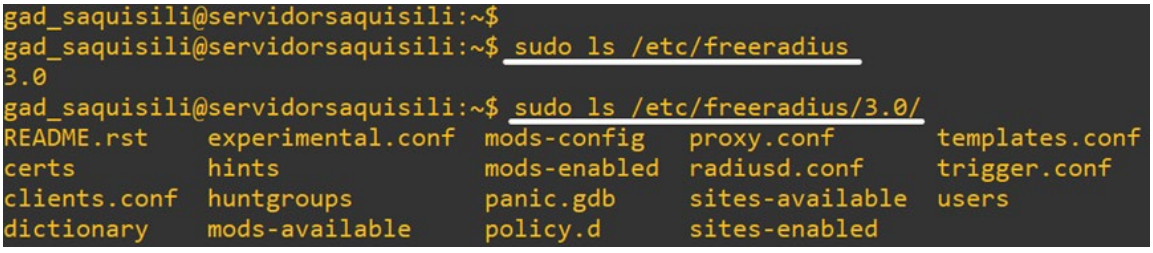


Nota. La siguiente figura representa el comando de instalación del servidor freeradius.

Procedemos a la configuración donde empezamos ingresado el siguiente comando **sudo ls /etc/freeradius** este comando nos ayuda a verificar la versión que tiene el servidor freeradius, luego de haber verificado la versión se procede a ingresar el siguiente comando **sudo ls /etc/freeradius/3.0/** , por medio de este comando podemos visualizar los directorios que contiene el servidor en este caso los directorios a configurar son los de users y los de clients.conf para poder crear cada uno de los usuarios respectivamente.

Figura 95

Verificación de la versión y los directorios

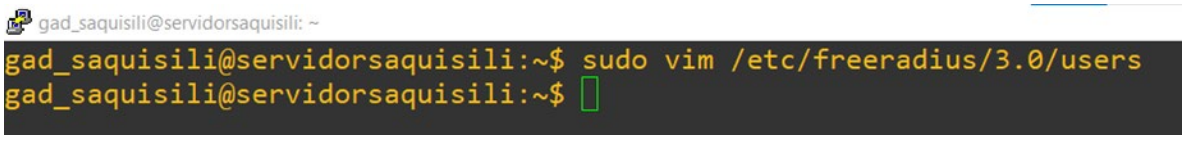


Nota. Mediante estos comandos podemos verificar la versión del servidor freeradius y los directorios que podemos configurar respectivamente de acuerdo al requerimiento.

Luego de haber revisado todos los directorios que tenemos procedemos a ingresar el comando **sudo vim /etc/freeradius/3.0/users**, este comando nos permitirá acceder al directorio de usuarios, es esta sección podemos crear los usuarios que van hacer la utilización de esta red wifi segura tal como se muestra en las siguientes figuras.

Figura 96

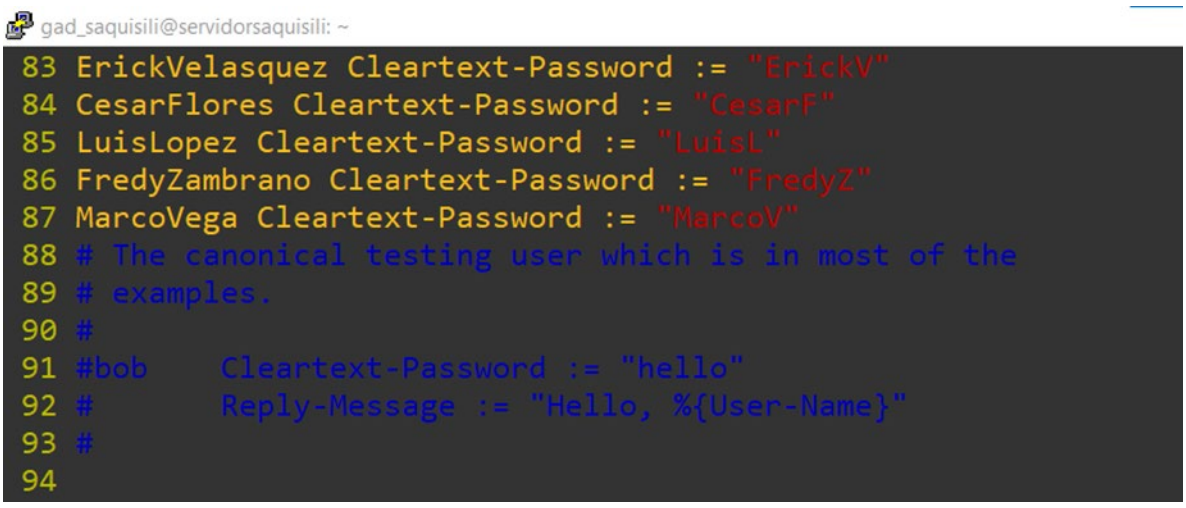
Acceso al directorio de los usuarios



Nota. La figura representa el comando que se debe ingresar para poder acceder al archivo donde nos permita crear los respectivos usuarios.

Figura 97

Creación de usuarios



Nota. la figura representa los usuarios generados en este archivo para la utilización de la red.

Culminado con la creación de usuarios procedemos al ingreso en el archivo clients. conf dentro del directorio /etc/freeradius/3.0 para el cual ingresamos el comando **sudo vim /etc/freeradius/3.0/clients.conf**, en esta sección creamos la autenticación con el servidor donde debemos colocar la dirección IP, una contraseña y el nombre del Access point, una vez realizado procedemos a guardar y salir del archivo.

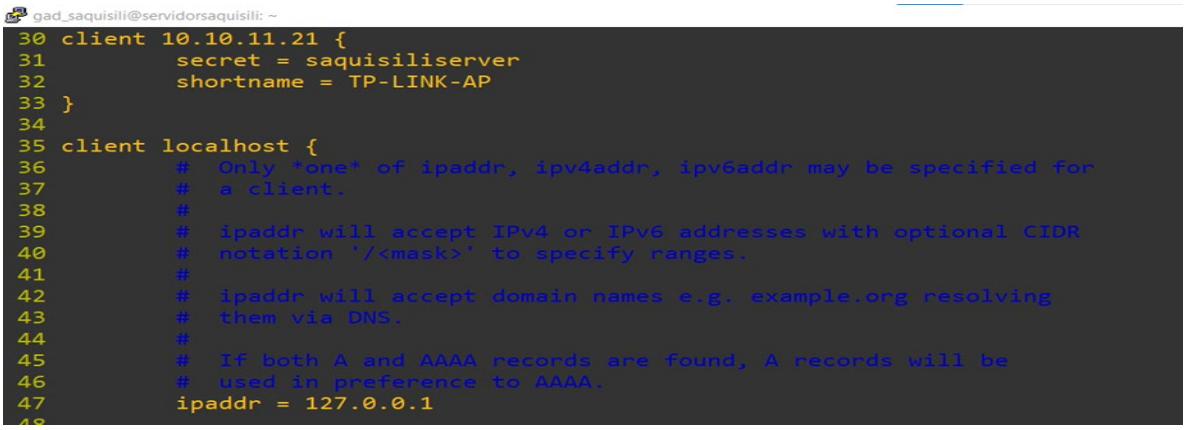
Figura 98

Inicialización al archivo clients.conf

Nota. La siguiente figura muestra el comando que se debe ingresar para crear la autenticación del servidor con Access point.

Figura 99

Configuración de client

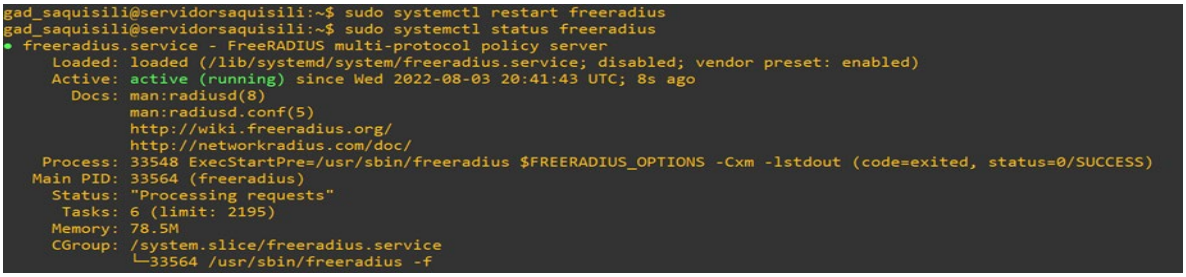


Nota. La figura representa la información creada para la autenticación del servidor con el AP.

Culminado con la configuración de autenticación del AP con el servidor, por medio del siguiente comando **sudo systemctl restart freeradius**, restablecemos el servicio del servidor para que actualice los datos ingresados en los archivos de configuración, luego de eso ingresamos el comando **sudo systemctl status freeradius**, este comando nos indicara si el servidor ya se encuentra activo y corriendo como se muestra en la figura.

Figura 100

Servidor activo



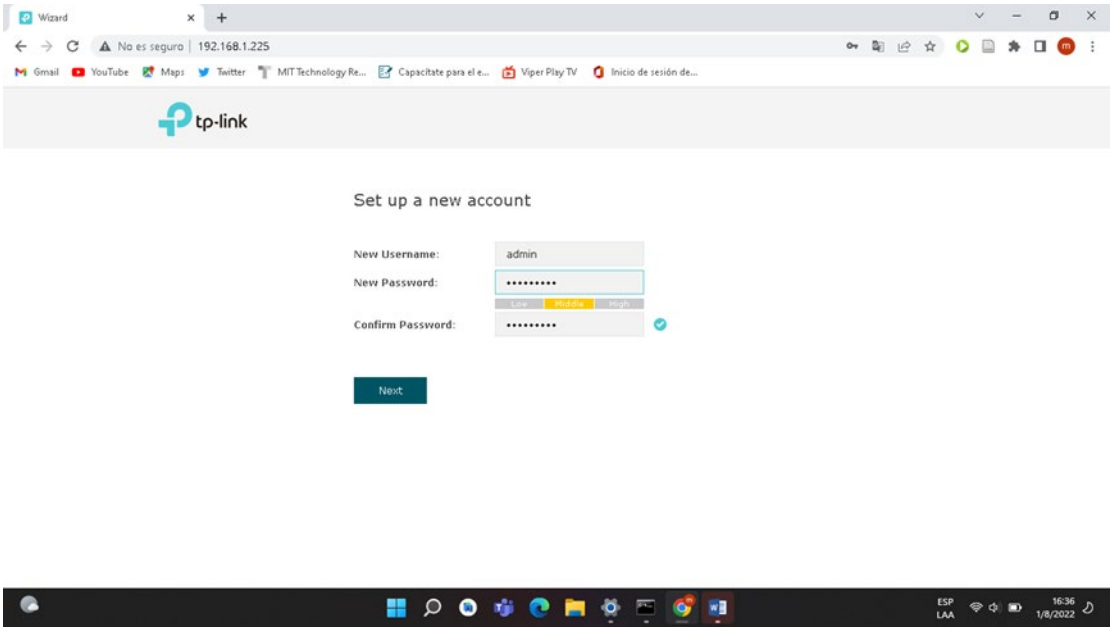
Nota. Esta figura muestra los comandos ingresados para restablecer el servicio y para verificar el estado del servidor para su respectiva utilización.

Configuración del Access Point

Para poder configurar al equipo primero procedemos a ingresar al navegador don ponemos la dirección IP del equipo para poder inicializar el Access Point colocando una contraseña de administrador.

Figura 101

Inicialización Access Point



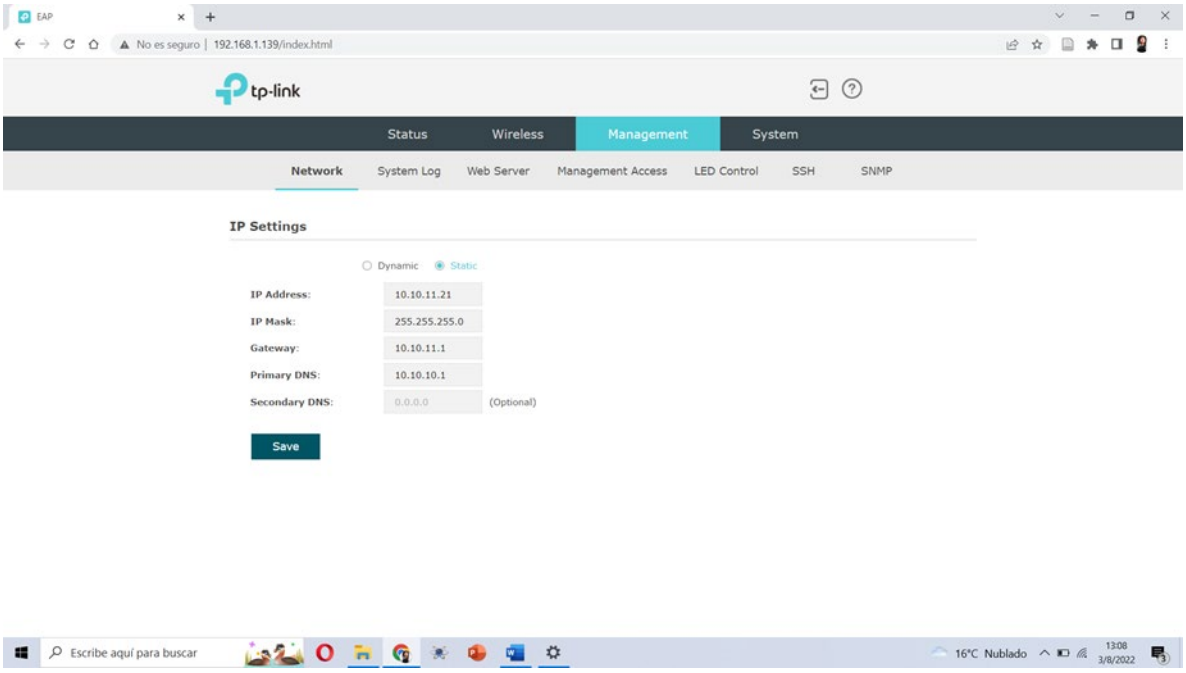
Nota. La figura representa la creación de parámetros para tener restringido el acceso al equipo.

Con respecto a las configuraciones del Access Point primero procedimos a cambiar la dirección IP de equipo para que este se encuentre en el mismo segmento de red con el servidor y permita tener comunicación entre los dos equipos. En este caso la dirección IP era la

10.10.11.21/24 su máscara 255.255.255.0 el Gateway 10.10.11.1 y su DNS 10.10.10.1 ya colocado estas direcciones respectivamente procedemos a guardar los cambios.

Figura 102

Configuración de IP

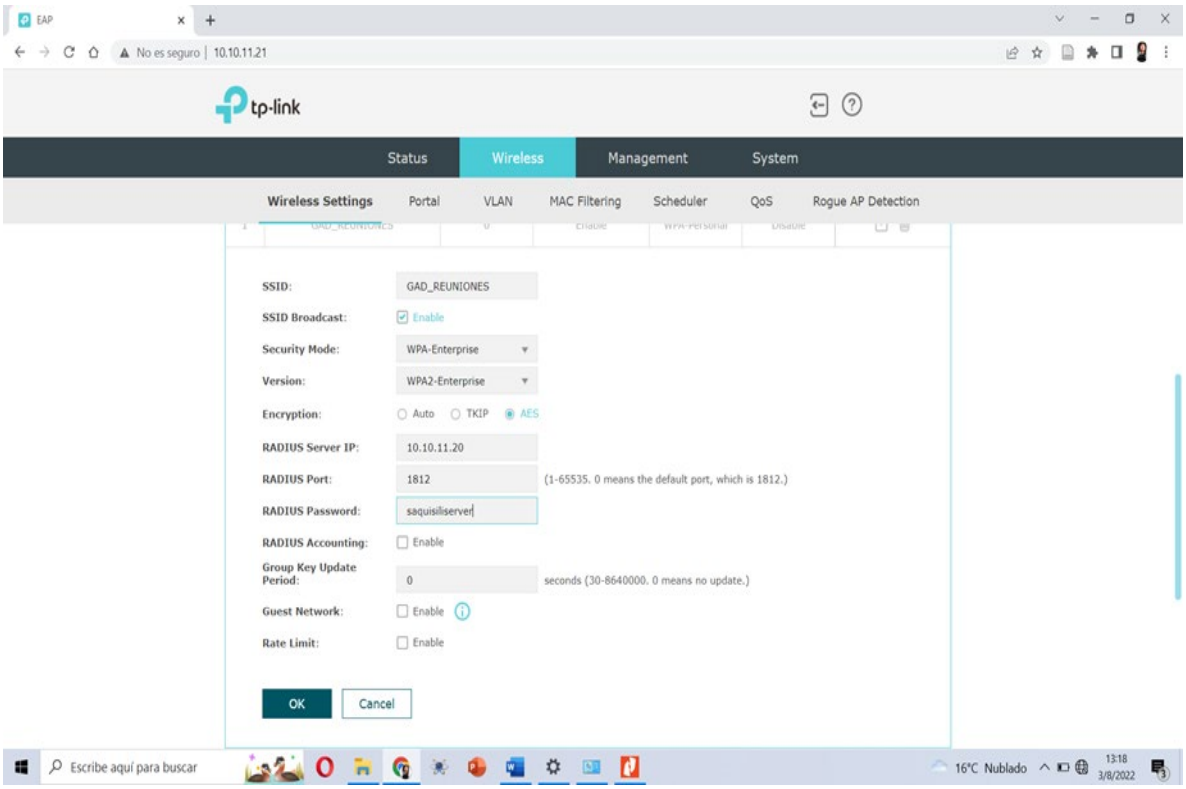


Nota. En la siguiente figura podemos visualizar la dirección asignada al Access point en el mismo segmento de red con el servidor.

Luego de haberle asignado una IP al Access Point procedemos a realizar la configuración de la seguridad WPA2 Enterprise con el servidor donde en el modo de seguridad seleccionamos la opción WPA-Enterprise, en la versión seleccionamos la opción WPA2-Enterprise, en el modo de encriptación seleccionamos la opción AES, también nos pide la dirección IP del servidor radius el tiempo de espera de autentificación, puerto del servidor radius, la contraseña del servidor. Finalmente guardamos las configuraciones realizadas en el AP.

Figura 103

Configuración de seguridad WPA2 Enterprise



Nota. La figura representa las configuraciones realizadas de seguridad con la opción de WPA2 Enterprise para la red segura.

Infraestructura de la red del proyecto

Es de gran importancia segmentar la red para la colocación de las respectivas direcciones IP que posteriormente deberán ser asignadas a los equipos para el funcionamiento, gracias a la segmentación podemos mejorar el rendimiento de la red y sobre todo la seguridad, permitiendo que el administrador de la red pueda dar una mejor gestión de los servicios a través de cada uno de los segmentos específicos en la entidad.

Tabla 10

Segmentación de red

Subred	Mascara	Gateway	DNS
10.10.11.0	255.255.255.0	10.10.11.1	10.10.10.1

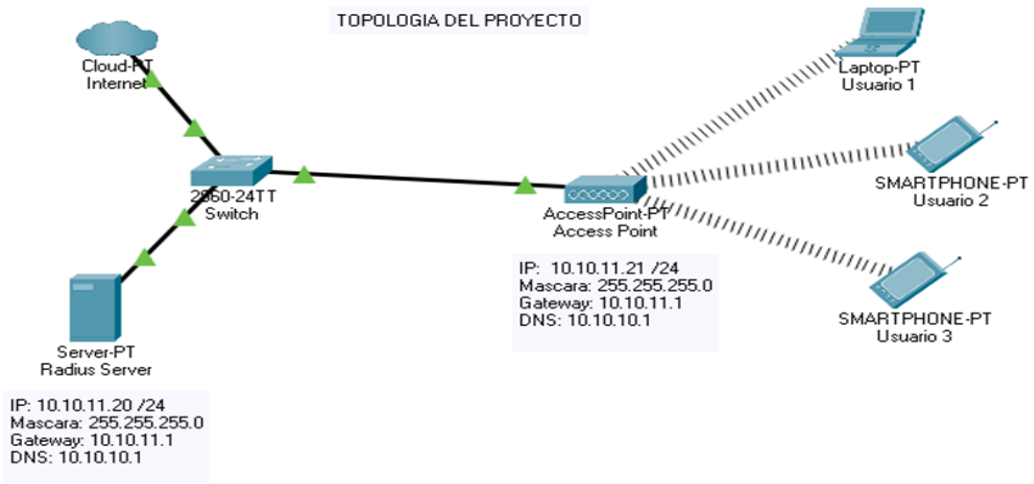
Nota. Esta tabla representa la limitación del segmento de red para las direcciones IP correspondientes.

Una vez establecida la red para la infraestructura del proyecto se realiza las respectivas designaciones de direcciones IP en los equipos correspondientes en este caso en el servidor y el Access Point que se van a utilizar en el GAD Municipal del cantón Saquisili.

Diagrama de la topología de proyecto

Figura 104

Topología del proyecto



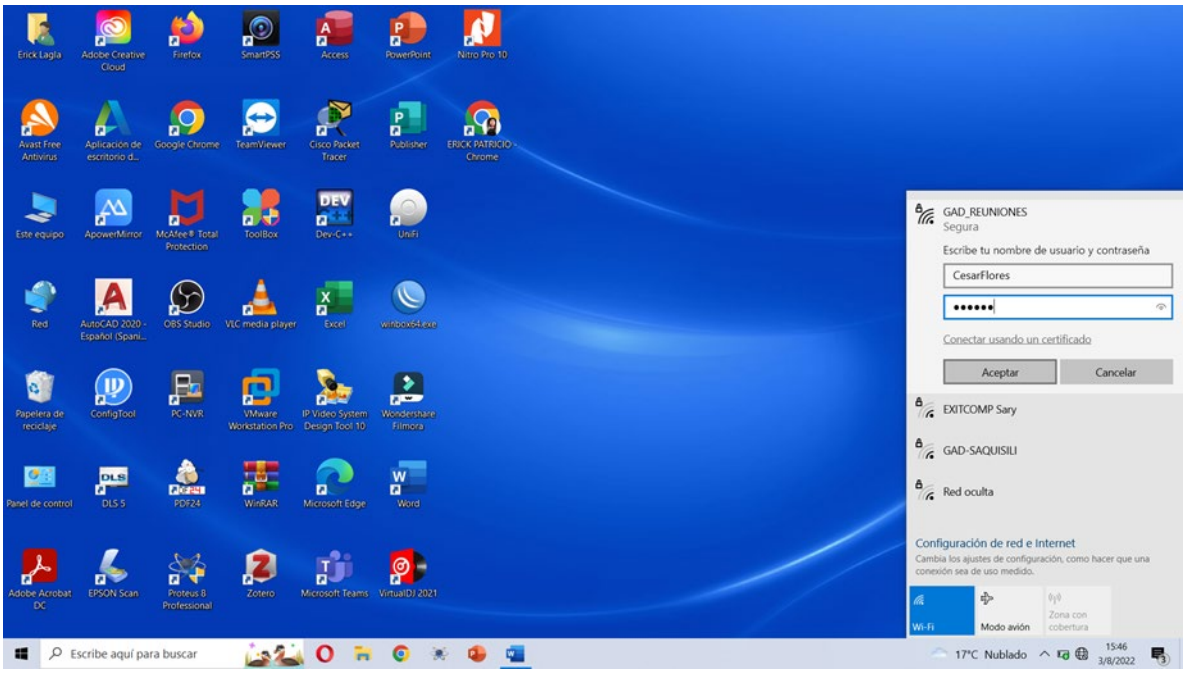
Nota. El diagrama muestra la conexión física realizada en el GAD Municipal del cantón Saquisili.

Pruebas de funcionamiento

Finalizado con la configuración de la red segura procedemos a ingresar la información correspondiente para poder conectarse a la red de GAD_REUNIONES es este caso nos pide el usuario y contraseña, en este caso el usuario es el que fue generado en el servidor freeradius respectivamente, ya ingresado esta información presionamos en aceptar.

Figura 105

Usuario y contraseña

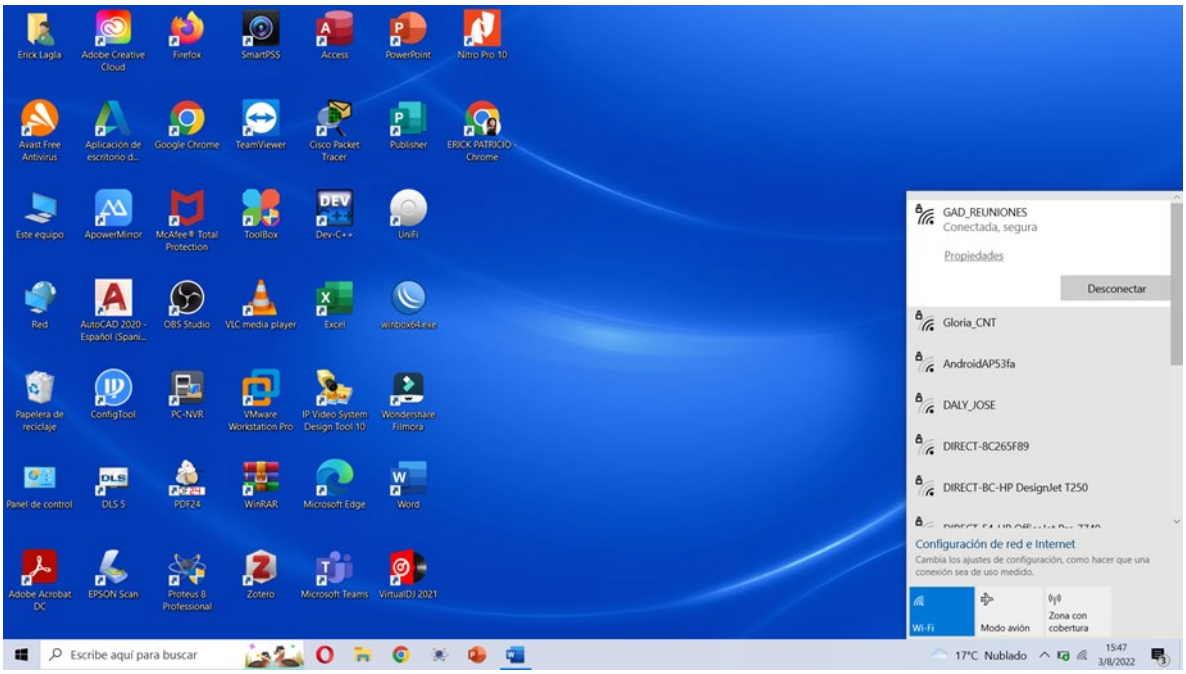


Nota. La figura representa el ingreso del usuario y contraseña del mismo para acceder a la red GAD_REUNIONES.

Ya terminado con el proceso de ingreso de datos del usuario en la siguiente figura podemos observar que el usuario ya se encuentra conectado a la red y puede hacer uso de la misma para sus respectivas actividades en el GAD municipal del cantón Saquisili.

Figura 106

Autenticación del usuario con éxito



Nota. En la figura podemos observar que la autenticación del servidor freeradius con el Access Point fue con éxito ya que permito al usuario acceder a la red GAD_REUNIONES.

Capitulo IV

Conclusiones

- Se obtuvo información específica acerca de los sistemas a implementar, tanto para la parte de video vigilancia IP como para el sistema de seguridad wifi WPA2 Enterprise y la configuración del servidor radius; logrando determinar mediante un análisis y selección, los equipos más adecuados para el funcionamiento de nuestros sistemas cumpliendo de esta manera con los estándares de calidad y servicios de las redes de telecomunicaciones.
- Se completa la instalación y configuración adecuada de los equipos del sistema de video vigilancia IP, cubriendo las zonas vulnerables previamente analizadas, como son la sala de reuniones, la bodega, el pasillo a las oficinas de la segunda planta y Tics, aportando de esta forma una mayor seguridad en la municipalidad.
- Se realiza la instalación y configuración del punto de acceso, así como también la configuración en el servidor de autentificación AAA freeradius, el cual permitirá controlar el acceso a la red de manera segura y que, además, al limitar el acceso a esta red por medio del servidor, se logra tener una mejor estabilidad en términos de conexión para los usuarios.
- Se ejecutan las pruebas de funcionamiento en la primera sección como es en el sistema de cámaras, logrando verificar que cada equipo funciona y capta las imágenes de manera eficiente y con mayor resolución, así también se realiza las pruebas de conexión de los usuarios al Access point, ubicado en la sala de reuniones por lo que podemos decir que este protocolo utiliza el esquema cliente-servidor, es decir que el usuario requiere de su contraseña para el acceso a la red inalámbrica segura que se implementó en el GAD Municipal de Saquisili.

Recomendaciones

- Se recomienda que los equipos que componen el sistema de videovigilancia IP y el sistema de seguridad wifi WPA2 Enterprise sean sometidos a un mantenimiento preventivo periódico cada cuatro meses para evitar averías y fallos del sistema permitiendo prolongar más la utilidad de los equipos tanto en el sistema de video vigilancia IP como en el sistema de seguridad wifi.
- Para mantener la integridad de los datos, se recomienda implementar una política de seguridad para el acceso a los datos protegidos y que sea accesible solo para quienes son responsables de monitorear estos sistemas de seguridad.
- Se recomienda que tanto el servidor Freeradius como el sistema operativo instalado en la PC se actualicen con una versión nueva y estable de este software en los próximos años, mejorando así el rendimiento de los dispositivos, y mejorando los sistemas de seguridad del mismo.

Glosario

IP: Protocolo de Internet

NVR: Network Video Recorder (Grabador de Video de Red)

CCTV: Closed Circuit Television (Circuito Cerrado de Televisión)

ANPR: Automatic number plate recognition (Reconocimiento Automático de Matrículas)

Autentificación: Es el proceso o conjunto de actividades que se deben desarrollar para confirmar que algo es lo que se dice.

Usuario: Es aquel individuo que se necesita acceder o utilizar un servicio.

Servidor: Equipo o conjunto de equipos capaces de brindar un servicio y atender las peticiones solicitadas por un usuario.

Access Point o WAP: Wireless Access Point (Punto de Acceso Inalámbrico)

WIFI: Wireless Fidelity (Fidelidad Inalámbrica)

Radius: Es un protocolo de autenticación AAA, usado para controlar y monitorear el acceso a una red wifi.

WPA2 ENTERPRISE: Es un tipo de cifrado de seguridad usado en redes inalámbricas, que permite vincular un servidor radius para la autentificación de usuarios

EAP: Extensible Authentication Protocol (protocolo de autenticación extensible)

WPA: Wi-Fi Protected Access (acceso Wi-Fi protegido)

WEP: Wired Equivalent Privacy (privacidad equivalente a cableado)

UTP: Cable de par trenzado sin blindaje

STP: Par trenzado apantallado

FTP: Cable de par trenzado apantallado

SFTP: Par trenzado apantallado totalmente blindado

DHCP: Protocolo de configuración dinámica de host

PoE: Alimentación a través de ethernet

WLAN: Wireless Local Area Network (Red de Area Local inalambrica)

LAN: Local Area Network (Red de Área Local)

MAN: Metropolitan Area Network (Red de área metropolitana)

WAN: Wide Area Network (Red de área amplia)

PC: Computadora personal

LINUX: Sistemas operativos, en su mayoría con licencia libre

Gateway: Puerta de enlace

CPU: Unidad de procesamiento central

RAM: Memoria de acceso aleatorio

Bibliografía

Acosta, S. (9 de Octubre de 2015). *TecnoSeguro*. Recuperado el 24 de Junio de 2022, de https://www.tecnoseguro.com/noticias/cctv/conteo-personas-colombia

ACRYLICSuite. (12 de junio de 2020). *ACRYLICSuite*. Recuperado el 25 de junio de 2022, de ACRYLICSuite: https://www.acrylicwifi.com/blog/es-segura-red-wifi-wpa-wpa2/

ALFATELECOM. (19 de septiembre de 2019). *ALFA*. Recuperado el 25 de junio de 2022, de ALFA: https://www.alfatelecom.mx/punto-a-multipunto/

Arango, A. (14 de Agosto de 2021). *Sigma Electrónica LTDA*. Recuperado el 24 de junio de 2022, de Sigma Electrónica LTDA: https://www.sigmaelectronica.net/producto/cable-utp/

ARGSEGURIDAD. (22 de Marzo de 2017). *BLOG ARGSEGURIDAD*. Recuperado el 16 de Junio de 2022, de https://site.argseguridad.com/blog/resolucion-camaras-megapixel/

Austerberry, D. (2019). *STREAMING DE VIDEO Y AUDIO.* España: Editorial: Elsevier.

Axis Communications. (15 de agosto de 2019). *Axis Communications*. Recuperado el 24 de junio de 2022, de Axis Communications: https://www.axis.com/es-es/products/video-encoders

Baltazar, M. (2019). *INTRODUCCIÓN A LA INGENIERIA DE FIBRA ÓPTICA.* Buenos Aires: Editorial Addison.

Blogger. (15 de octubre de 2020). *Blogger*. Recuperado el 25 de junio de 2022, de Blogger: https://itgeeknotes.blogspot.com/2020/10/macbook-air-recovery-ask-wpa2.html

Blogodisea. (2 de octubre de 2018). *Blogodisea*. Recuperado el 26 de junio de 2022, de Blogodisea: https://www.blogodisea.com/cuales-tipos-servidores-web-como-trabajan.html

Brown, P. (3 de enero de 2020). *Mundo Digital*. Recuperado el 26 de junio de 2022, de Mundo Digital: https://www.mundodigital.net/258/

Campoy, C. G. (9 de agosto de 2016). *Xerinfor*. Recuperado el 25 de junio de 2022, de Xerinfor: https://xerinfor.com/smartblog/8_Qu%C3%A9-es-y-c%C3%B3mo-funciona-un-router-inal%C3%A1mbrico.html

Cando Salme, M., & Llumitasig Galarza, M. E. (2016). *implementación de un sistema de autenticación para controlar la seguridad de la red inalámbrica de la brigada de fuerzas especiales No. 9 Patria.* Latacunga, Ecuador: UNIVERSIDAD TÉCNICA DE COTOPAXI. Recuperado el 26 de junio de 2022, de http://repositorio.utc.edu.ec/bitstream/27000/438/1/T-UTC-1017.pdf

Castellón Arenas, A. (2014). *cableado estructurado norma EIA TIA 568.* FUNDACIÓN TECNOLÓGICA ANTONIO DE ARÉVALO - TECNAR. Recuperado el 25 de junio de 2022, de https://mtlsasturiasnoe.files.wordpress.com/2015/10/cableado-estructurado_norma-eia-tia-568.pdf

Castillo, J. A. (26 de enero de 2019). *PROFESIONALREVIEW*. Recuperado el 24 de junio de 2022, de PROFESIONALREVIEW: https://www.profesionalreview.com/2019/01/26/cables-utp-cables-stp-cables-ftp/

Chan García, A. E. (2020). *fibra óptica evolucion,estandares y aplicaciones.* México: UNIVERSIDAD DE QUINTANA ROO. Recuperado el 25 de junio de 2022, de http://risisbi.uqroo.mx/bitstream/handle/20.500.12249/2610/TA1800.2020-2610.pdf?sequence=1

Colaboradores de Docusing. (19 de noviembre de 2021). *Docusing*. Recuperado el 26 de junio de 2022, de Docusing: https://www.docusign.mx/blog/tipos-de-servidores

Colobran. (2 de junio de 2022). *Solución de vigilancia*. Obtenido de https://www.synology.com/es-mx/vms/solution/surveillance_small_business?utm_medium=cpc&utm_source=google&utm_campaign=sac-latam-google-surveillance-0601202

CTA. (18 de Marzo de 2021). *Centro de Ciencia y Tecnología de Antioquia - CTA*. Recuperado el 23 de Junio de 2022, de https://cta.org.co/que-es-la-inteligencia-artificial-y-por-que-es-tan-importante/

D. M. (7 de octubre de 2015). *Geektopia*. Recuperado el 25 de junio de 2022, de Geektopia: https://www.geektopia.es/es/technology/2015/10/07/articulos/antenas-conoce-como-funcionan-aprende-colocar-tu-router-repetidor-senal-wi-fi.html

Dahua Technology. (12 de Enero de 2021). *Dahua Technology*. Recuperado el 24 de Junio de 2022, de https://www.dahuasecurity.com/es/products/keyTechnologies/352

De León, A. (27 de agosto de 2019). *Penso*. Recuperado el 26 de junio de 2022, de Penso: https://www.penso.com.br/o-que-e-um-servidor-de-e-mail/

DMS. (12 de noviembre de 2016). *DMS*. Recuperado el 25 de junio de 2022, de DMS: https://dms.com.pe/redes-mesh/

ELPA. (12 de agosto de 2019). *ELPA*. Recuperado el 24 de junio de 2022, de ELPA: https://elpa.cl/categorias-de-cables-utp/

España, J. C. (1 de JUNIO de 2022). *Soluciones integrales de gestión de vídeo para una seguridad por vídeo optimizada*. Obtenido de https://www.johnsoncontrols.com/es_es/seguridad/videovigilancia/video-management-sistemas

Espinosa, O. (19 de abril de 2022). *redeszone*. Recuperado el 26 de junio de 2022, de redeszone: https://www.redeszone.net/tutoriales/internet/mejores-servidores-dns-sin-registros-logs/

Etecé. (11 de Julio de 2021). *Concepto*. Recuperado el 24 de Junio de 2022, de Concepto: https://concepto.de/cable-coaxial/

Explorer, A. I. (1 de junio de 2022). *Access Point*. Obtenido de https://www.ymant.com/blog/que-es-un-ap-access-point-y-que-usos-y-modos-tiene/

Fernández, Y. (31 de mayo de 2017). *Qué es un proxy*. Recuperado el 26 de junio de 2022, de Qué es un proxy: https://www.xataka.com/basics/que-es-un-proxy-y-como-puedes-utilizarlo-para-navegar-de-forma-mas-anonima

FERNÁNDEZ, Y. (1 de junio de 2022). *Direcciones IP dinámicas y fijas*. Obtenido de https://www.xataka.com/basics/direcciones-ip-dinamicas-fijas-que-que-ventajas-tiene-cada

Fuentes, C. A. (2020). Implementación de un prototipo de red inalámbrica . EL SALVADOR,: UNIVERSIDAD TECNOLÓGICA EL SALVADOR.

García, F. J. (2019). *VIDEOVIGILANCIA: CCTV USANDO VIDEOS IP.* España: Vértice.

Gaybor, C. L. (2018). *Diseño de un sistema de transmisión de caparas IP.* sin fuente.

Gerlysu. (26 de noviembre de 2012). *Gerlysu*. Recuperado el 25 de junio de 2022, de Gerlysu: https://gerlygirl.wordpress.com/2012/11/26/red-de-punto-a-punto/

grupo universal. (23 de febrero de 2020). *grupo universal*. Recuperado el 26 de junio de 2022, de grupo universal: https://grupouniversal.com/servidor-cloud-para-empresas/

Huidobro, J. M. (2013). Antenas de telecomunicaciones. *ACTA, II*(5), 18. Recuperado el 25 de junio de 2022, de https://www.acta.es/medios/articulos/ciencias_y_tecnologia/020001.pdf

ICO INTERNACIONAL S.A. (17 de Marzo de 2020). *ICO INTERNACIONAL S.A.* Recuperado el 25 de Junio de 2022, de https://ico-ecuador.com/sistema-de-proteccion-perimetral/

ICO INTERNACIONAL S.A. (14 de Mayo de 2020). *ICO INTERNACIONAL S.A.* Recuperado el 24 de Junio de 2022, de https://ico-ecuador.com/reconocimiento-facial/

Juan, A. (2018). *Camaras IP.*

Londoño., P. V. (2020). *Diseño de un Sistema Seguridad ciudadana mediante Cámaras IP para elIlustre Municipio Del Cantón Pelileo.* Pelileo: UTA.

López Jurado, C. (17 de febrero de 2021). *CCM*. Recuperado el 25 de junio de 2022, de CCM: https://es.ccm.net/contents/788-802-11i-wpa2

Lugo, M. (12 de julio de 2019). *conectemos*. Recuperado el 26 de junio de 2022, de conectemos: https://conectemos.com/principal-funcion-servidor-web/

Marchionni, E. A. (2011). *administrador de servidores* (Vol. I). Gradi S.A. Recuperado el 26 de junio de 2022, de https://books.google.com.ec/books?id=CfhGJ7yylRgC&printsec=frontcover&dq=inauthor:%22Enzo+Augusto+Marchionni%22&hl=es&sa=X&redir_esc=y#v=onepage&q&f=false

Mareco, D. (18 de junio de 2020). *securedge*. Recuperado el 25 de junio de 2022, de securedge: https://www.securedgenetworks.com/blog/access-point-placement-mistakes

Martí, S. (2013). *Diseño de un sistema de televigilancia.* UNIVERSIDAD POLITECNICA DE VALENCIA. Recuperado el 11 de junio de 2022, de https://riunet.upv.es/bitstream/handle/10251/34082/memoria.pdf

Mata, F. J. (12 de enero de 2019). *Videovigilamcia: CCTV usando video IP.* Recuperado el 11 de junio de 2022, de https://www.editorialelearning.com/catalogo/media/iverve/uploadpdf/1526035761_0327_demo.pdf

Medina, T. L. (2019). *RED DE VIDEO VIGILANCIA UTILIZANDO CÁMARAS IP PARA .* Ambato: UTA.

Nosteal. (1 de junio de 2022). *LA IMPORTANCIA DE LA CÁMARAS IP EN LA ACTUALIDAD*. Obtenido de https://nosteal.cl/la-importancia-de-la-camaras-ip-en-la-actualidad/

Olenski, J. (7 de noviembre de 2016). *GlobalSing*. Recuperado el 26 de junio de 2022, de GlobalSing: https://www.globalsign.com/es/blog/wpa2-personal-or-enterprise

Ordoñes, A. (29 de agosto de 2015). *cominicación digital y virtual*. Recuperado el 25 de junio de 2022, de comunicación digital y virtual: https://adrianordonhes.wordpress.com/2015/08/29/fibra-optica/

Parlamento Europeo. (8 de Septiembre de 2020). *Noticias Parlamento Europeo.* Recuperado el 23 de Junio de 2022, de https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa

Pérez Vega, C. (19 de enero de 2019). *unican*. Recuperado el 24 de junio de 2022, de unican: https://personales.unican.es/perezvr/pdf/Compresion%20de%20video.pdf

Redatel S.A.S. (11 de marzo de 2016). Cámara IP. pág. 1. Recuperado el 12 de Junio de 2022, de https://www.redatel.net/html/camara-ip-conceptos-basicos.html#:~:text=Una%20c%C3%A1mara%20IP%20consiste%20principalmente,red%20para%20transmisi%C3%B3n%20de%20datos.

REDES. (20 de marzo de 2018). *Telnet*. Recuperado el 5 de agosto de 2022, de Telnet: http://dcsmibloggrd.blogspot.com/

redesinalambricas. (13 de junio de 2017). *redesinalambricas*. Recuperado el 26 de junio de 2022, de redesinalambricas: https://www.redesinalambricas.es/conexiones-inalambricas/

RedesInalambricas. (16 de octubre de 2020). *RedesInalambricas*. Recuperado el 25 de junio de 2022, de RedesInalambricas: https://www.redesinalambricas.es/estandares-wifi/

RNDS. (2021). Cable de par trenzado. *RNDS*, 4. Recuperado el 24 de junio de 2022, de http://www.rnds.com.ar/articulos/052/rnds_136w.pdf

Ros, I. (21 de marzo de 2021). *MC noticias*. Recuperado el 25 de junio de 2022, de MC noticias: https://www.muycomputer.com/2021/03/21/estandares-wi-fi-mas-utilizados/

Salazar, J. (5 de mayo de 2016). redes inalámbricas. *Techpadia*, 40. Recuperado el 24 de junio de 2022, de https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf

Sanchez, C. (8 de Septiembre de 2022). *Tecnosinergia*. Recuperado el 18 de Junio de 2022, de https://tecnosinergia.zendesk.com/hc/es/articles/360002472751--Para-que-sirve-la-funci%C3%B3n-Compensaci%C3%B3n-de-Luz-de-Fondo-BLC-en-c%C3%A1maras-

SANTANA HERNANDEZ, C. D. (12 de Agosto de 2021). *Educaplay*. Recuperado el 24 de Junio de 2022, de Educaplay: https://es.educaplay.com/juegoimprimible/3610429-tipos_de_conexion_a_internet.html

SAQUIRAY, E. (19 de Abril de 2018). *Hardtech.pe.* Recuperado el 17 de Junio de 2022, de https://hardtech.pe/web/companies/new/articulos/9/que-es-una-camara-ptz

Sarabia Buñay, B. W. (2018). *DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD.* Riobamba, Ecuador: ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO. Recuperado el 15 de Junio de 2022, de http://dspace.espoch.edu.ec/bitstream/123456789/9153/3/98T00206.pdf

Sistemas., H. (31 de MAYO de 2022). *camaras IP*. Obtenido de <http://www.hommaxsistemas.com/es/>

Souza, I. (23 de noviembre de 2019). *rockcontent blog*. Recuperado el 26 de junio de 2022, de rockcontent blog: https://rockcontent.com/es/blog/software-libre/

Suárez Gutiérrez, M. (1 de mayo de 2012). *Mecanismos de seguridad en redes inalambricas.* México: Universidad Veracruzana. Recuperado el 26 de junio de 2022, de https://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf

Suquillo, E. (2020). *Diseño e Implementación de una red LAN inalámbrica y el sistema.* Quito: Universidad SEK.

TECNIT. (15 de enero de 2017). *TECNIT*. Recuperado el 25 de junio de 2022, de TECNIT: https://tecnit.com.ec/producto/access-point-wireless-n-tp-link-eap115-2-4ghz-dos-antenas-int-300mbps-soporta-poe-de-techo/

Tecnología Informática. (18 de octubre de 2021). *Tecnología Informática*. Recuperado el 25 de junio de 2022, de Tecnología Informática: https://www.tecnologia-informatica.com/que-es-red-inalambrica-seguridad-wifi/

Telectronika. (22 de junio de 2018). *Telectronika*. Recuperado el 24 de junio de 2022, de Telectronika: https://www.telectronika.com/articulos/ti/categoria-8/

Terabyte. (13 de septiembre de 2020). *terabyte.* Recuperado el 24 de junio de 2022, de terabyte: http://www.solucionesterabyte.com/nvrs.html#:~:text=que%20es%20un%20Nvr&text=Un%20NVR%20se%20incorpora%20generalmente,particular%20de%20c%C3%A1maras%20de%20red.

TRENDnet. (1 de enero de 2021). *TRENDnet.* Obtenido de https://www.trendnet.com/products/4MP-ip-cameras/TV-IP345PI

Ubuntu. (6 de enero de 2019). *Viva Ubuntu*. Recuperado el 26 de junio de 2022, de Viva Ubuntu: https://vivaubuntu.com/instalar-ubuntu-20-04-desde-usb-pendrive/

usecim. (7 de noviembre de 2022). *usecim*. Recuperado el 25 de junio de 2022, de usecim: https://usecim.net/2019/02/19/un-mejorado-software-de-gestion-de-video-para-los-negocios/

Vásquez, S. G. (2015). *Elementos de sistemas de telecomunicaciones.* Madrid: Paraninfo S.A. Recuperado el 24 de junio de 2022, de https://edoc.pub/elementos-de-sistemas-de-telecomunicaciones-2-pdf-free.html

WISPCONTROL. (11 de abril de 2020). *WISPCONTROL*. Recuperado el 25 de junio de 2022, de WISPCONTROL: https://wispcontrol.com/que-es-radius/

Anexos