Implementación de un sistema de video vigilancia con tecnología IP para áreas exteriores y un control de acceso mediante un servidor Radius para el área de docentes en el Colegio Particular “Israel” N°2

Erazo Quito, Rodney Alexander y Quispe Hernández, Esteban Paul

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

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

Msg. Viteri Arias, Santiago Christian

18 de agosto de 2023

Latacunga

Copyleaks

Plagiarism report

ERAZO-QUISHPE.pdf

Scan details

Scan time:
August 16th, 2023 at 17:48 UTC

Total Pages:
70

Total Words:
17273

Plagiarism Detection

3.5%

Types of plagiarism		Words
Identical	3.5%	598
Minor Changes	0%	0
Paraphrased	0%	0
Omitted Words	0%	0

AI Content Detection

N/A

Text coverage
- AI text
- Human text

Plagiarism Results: (49)

TESIS CAPITULOS TESIS V5.pdf — 0.4%

https://bibdigital.epn.edu.ec/bitstream/15000/17471/1/cd-79...

BBG03

ESCUELA POLITÉCNICA NACIONAL FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA ANÁLISIS DE DOS ALGORITMOS PARA DETECCIÓN DE ROSTR...

Router TP-link Gigabit Doble-Banda Inalámbrico - L... — 0.3%

https://www.laserprintsoluciones.com/producto/router-tp-lin...

Saltar al contenido ...

DISEÑO DE UN SISTEMA DE SEGURIDAD A TRAVÉS DE... — 0.3%

https://1library.co/document/zgxvx37q-diseno-sistema-segu...

...

Viteri Arias, Cristian Santiago
C.C: 050247691-4

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACION PARA LA EXCELENCIA

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Certificación

Certifico que el trabajo de integración curricular: "**Implementación de un sistema de video vigilancia con tecnología IP para áreas exteriores y un control de acceso mediante un servidor Radius para el área de docentes en el Colegio Particular "Israel" N°2**", fue realizado por los señores **Quishpe Hernández, Esteban Paul y Erazo Quito, Rodney Alexander,** 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, 18 de agosto de 2023

Viteri Arias Santiago Christian

C. C: 0502476914

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnologia Superior en Redes y Telecomunicaciones

Responsabilidad de Autoría

Nosotros, **Quishpe Hernández, Esteban Paul** con cédula de ciudadanía N° 1728080712 y **Erazo Quito, Rodney Alexander** con cédula de ciudadanía N° 1752963908, declaramos que el contenido, ideas y criterios del trabajo de integración curricular: **Implementación de un sistema de video vigilancia con tecnología IP para áreas exteriores y un control de acceso mediante un servidor Radius para el área de docentes en el Colegio Particular "Israel" N°2** 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, 18 de agosto de 2023

Quishpe Hernández, Esteban Paul

C.C.: 172808071-2

Erazo Quito, Rodney Alexander

C.C.: 175296390-8

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Autorización de publicación

Nosotros, **Quishpe Hernández, Esteban Paul** con cédula de ciudadanía **N° 1728080712 y Erazo Quito, Rodney Alexander** con cédula de ciudadanía **N° 1752963908**, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de integración curricular: **Implementación de un sistema de video vigilancia con tecnología IP para áreas exteriores y un control de acceso mediante un servidor Radius para el área de docentes en el Colegio Particular "Israel" N°2,** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi/nuestra responsabilidad.

Latacunga, 18 de agosto de 2023

Quishpe Hernández, Esteban Paul

C.C.: 172808071-2

Erazo Quito, Rodney Alexander

C.C.: 175296390-8

Dedicatoria

De manera especial y con mucho respeto, gratitud y amor, dedico este proyecto a mi madre, ya que, sin sus palabras de aliento, cariño y apoyo, fomentó dentro de mí una iniciativa para poder superarme. Espero que este sea el primero de muchos logros los cuales le quiero dar, porque se lo merece, gracias por apoyarme en todas mis decisiones.

A mi familia que siempre tuvo la confianza en mí, a pesar de la distancia y de diferencias, nunca me han dejado solo, razón por la cual tampoco he querido decepcionarlos y siempre los apoyaré como ellos lo hicieron y lo siguen haciendo.

Finalmente, a mi segunda familia, mis amigos, gracias por todas las risas, bromas, apoyo, enfados, me ayudaron a crecer como persona y a entender muchas cosas si hacerme sentir mal, siempre estaré agradecido con lo buenos amigos que son y decirles que todo se puede, nunca abandonen sus sueños.

RODNEY ALEXANDER ERAZO QUITO

Dedicatoria

En primera instancia deseo conceder esta tesis principalmente a mi papá y mi mamá Miguel y Blanca por ser el pilar importante en mi vida, a mi papá quien me enseñó a apreciar el resultado del trabajo duro, me di cuenta que el precio de una gota de sudor en mi frente, por ser un "amigo" y darme ánimos, papá mío, tienes un espacio bastante particular en mi corazón.

A mi madre que estuvo una y otra vez a mi lado brindándome su mano amiga dándome a cada instante una palabra de aliento, por haberme dado su apoyo incondicional a lo largo de todos los años para llegar a concluir mi profesión.

A mis hermanos Leonardo y Henry por su respeto, su cariño y su apoyo incondicional, me impulsan a seguir adelante, gracias por estar en los momentos más importantes de mi vida. Este logro también es de ustedes.

ESTEBAN PAUL QUISPE HERNANDEZ

Agradecimiento

Agradezco a mi madre, pilar fundamental para que yo pueda seguir adelante, a pesar de las adversidades, me ha enseñado a como levantarme de cada caída, gracias por todo el sacrificio realizado, para que yo pueda lograr esta meta, por las habladas que en todo momento siempre pudo escoger palabras sabias, siempre será mi ejemplo de persona.

También agradezco a la vida, por haberme dado dos hermanas a las cuales siempre cuidaré con mi vida, porque ellas siempre han estado ahí conmigo en mis momentos más difíciles, haciéndome reír y olvidar de los problemas, quiero que sean incluso mejores que yo en todo aspecto.

Agradezco a los docentes de la carrera que, con sus conocimientos y experiencia, pudieron hacer que nunca me diera por vencido, ya que siempre hay más oportunidades, siempre y cuando se intente con más fuerza de voluntad.

RODNEY ALEXANDER ERAZO QUITO

Agradecimiento

En primera instancia quiero agradecer a Dios, por darme la vida por darme una familia maravillosa que nunca me han dejado ni un momento solo, siempre estuvieron apoyándome, en cada reto que me propuse.

Agradezco a mis padres por su apoyo incondicional que nunca termina, que se han sacrificado más que mí, por lograr esta meta, gracias por su amor, dedicación y paciencia. A mi papá gracias porque ha sido un ejemplo de honestidad y trabajo irreductible. A mi mamá por acompañarme en cada noche agotadora por darme un ejemplo de esmero y firmeza en la vida.

También agradezco a mis hermanos Leonardo y Henry, por cada uno de sus consejos, por sus palabras de aliento, su animo a lo largo de la vida.

Gracias a todas las personas que jamás dejaron de creer en mí, fueron clave en mi vida, parientes, docentes y amigos, quienes me acompañaron en todo este proceso de cumplimiento de este desafío.

ESTEBAN PAUL QUISHPE HERNANDEZ

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Resumen

El objetivo de este proyecto es implementar un sistema de video vigilancia con tecnología IP para áreas exteriores y un control de acceso mediante un servidor Radius para el área de docentes en el Colegio Particular “Israel” N°2. El proyecto justifica como se realizó el diseño, el análisis realizado en el establecimiento, los requisitos necesarios para su implementación, y las respectivas pruebas de conectividad y funcionamiento. Esto estableció un sistema inalámbrico sin seguridad. Además, hay espacios donde no hay un sistema de videovigilancia y es necesario implementar el sistema de seguridad. Este proyecto aborda temas relacionados de los elementos que componen un sistema de videovigilancia entre software y hardware por igual en el servidor Radius, centrándose en el análisis de ubicación de cada una de las cámaras de vigilancia para cada uno de los espacios con el objetivo de controlar y supervisar por poder evitar los casos de inseguridad, agresión, etc. De la misma forma, el control de acceso mediante un servidor Radius nos permite un método de autenticación que limita el acceso a usuarios no autorizados en la red inalámbrica del colegio, permitiéndonos fortalecer y mejorar el rendimiento de la red. En definitiva, este plan podrá comprobar un sistema de videovigilancia eficaz y muy fiable que ofrece tranquilidad y seguridad al personal, ya que además podemos acceder a las grabaciones de las cámaras a través de Internet. Además, se pudo brindar una solución para acceder a la red inalámbrica, en la que se imprima el riesgo de perder información importante luego de autenticar al personal.

Palabras Clave: Tecnología IP, videovigilancia, conexión segura.

Abstract

The objective of this project is to implement a video surveillance system with IP technology for outdoor areas and access control through a Radius server for the teachers' area in the Colegio Particular “Israel” N°2. The project justifies how the design was carried out, the analysis made in the establishment, the necessary requirements for its implementation, and the respective connectivity and operation tests. This established a wireless system without security. In addition, there are spaces where there is no video surveillance system and it is necessary to implement the security system. This project addresses related issues of the elements that make up a video surveillance system between software and hardware alike in the Radius server, focusing on the analysis of location of each of the surveillance cameras for each of the spaces in order to control and monitor by being able to prevent cases of insecurity, aggression, etc. In the same way, the access control through a Radius server allows us an authentication method that limits access to unauthorized users in the school's wireless network, allowing us to strengthen and improve the performance of the network. In short, this plan will prove to be an effective and very reliable video surveillance system that offers peace of mind and security to the staff, since we can also access the camera recordings via the Internet. In addition, it was possible to provide a solution to access the wireless network, in which the risk of losing important information after authenticating the staff is printed.

Keywords: IP Technology, video surveillance, secure connection.

Capítulo I

Planteamiento del problema

Tema

Implementación de un sistema de video vigilancia con tecnología IP para áreas exteriores y un control de acceso mediante un servidor radius para el área de docentes en el Colegio Particular “Israel” N°2

Introducción

En los últimos años se ha podido evidenciar los avances de la tecnología IP y los estudios realizados en distintos sistemas de video vigilancia que en la actualidad se encuentra, sus funcionamientos, medios de conexión y los beneficios que nos ofrecen cada uno de ellos, cada vez siendo más accesibles a ataques en su seguridad, con el objetivo de plegarse de forma ilegal a la información privada, esto ha sido una muestra por la cual empresas, compañías y establecimientos se han visto obligados a adquirir estos equipos para mantener su seguridad física y lógica.

Se observa hoy en día como empresas, instituciones educativas, compañías o sectores públicos han recurrido de un sistema de video en red que puede disminuir hurtos, mejora de la seguridad de personal de la institución y así tener un progreso en la seguridad física de los mismos. El sistema permite la detección rápida de posibles percances.

Sin duda las preocupaciones que genera la situación de inseguridad que se vive en todos los sectores públicos como privados, lo que conlleva que el Colegio Particular Israel N.º 2 ubicado en la ciudad de Quito, cuente con un sistema de cámaras de video vigilancia en áreas

exteriores de las aulas de los estudiantes para ayudar a controlar y monitorear a los estudiantes y docentes que pertenecen a la comunidad educativa.

Técnicamente es posible implementar el sistema con equipamiento técnico e infraestructura de red que se pueda adaptar a las necesidades de la empresa, además de dotar al personal de una nueva red wifi en el área de docentes totalmente segura controlada por un control de acceso para ver o compartir información personal o institucional.

Antecedentes

Las instituciones educativas públicas y privadas exigen a sus autoridades garantizar la seguridad de los estudiantes, docentes y todas las personas que laboran en la entidad durante la jornada académica. Cabe mencionar que hoy en día existen dispositivos eléctricos o electrónicos que nos ayudan a motivar un nivel de seguridad un poco mayor.

En la actualidad, la seguridad se ha convertido en un tema muy importante para toda la sociedad en general, pues permite proteger la vida de las personas y mantener bajo control los bienes materiales, ya sea un negocio, empresa o institución, para que pueda mantener su continuidad. Esto ha llevado a las personas a tomar los temas de seguridad con mayor importancia.

El sistema de seguridad debe instalarse de manera segura y no dar falsas alarmas, de lo contrario puede ser ignorado. Antes de proceder con la implementación, debe estimar consideraciones tales como los objetos, equipos y personas a proteger, así como el presupuesto total del sistema de seguridad.

Con la realización e implementación de este proyecto se pretende dar solución a estos y otros problemas que puedan surgir durante su ejecución, previo al diseño e implementación se

darán a conocer los tipos de cámaras IP a utilizar, así como los diversos recursos e instrumentos para ser utilizados con sus respectivas características y funciones de ser apropiados.

Por lo determinado es fundamental que el Colegio Particular Israel N.º 2 deba contar con un sistema de video vigilancia mediante tecnología IP, ya que mediante este sistema se podrá controlar y vigilar casos de bullying, problemas, de igual manera se podrá vigilar la parte exterior de las aulas de la institución, al igual que una red inalámbrica segura para el área de docentes, ya que es donde más información existe sobre los estudiantes e institución, permitiendo así que la información no sea hurtada, manipulada o usada en contra de la institución, permitiendo así una mejoría al momento de compartir datos entre personal docente de la institución.

Planteamiento del Problema

Basados al tema de seguridad se analiza que en la actualidad el “Colegio Particular Israel N.º 2”, carece de un sistema de seguridad, debido que no cuenta con cámaras de video vigilancia o un cerco eléctrico, también de personal de guardianía con equipamiento seguro y tecnológico que se usa para realizar su respectiva ocupación, se observa que estos sistemas podrían mejorar la seguridad y la vigilancia de algunas dependencias y podrían ser implementados en la institución y que formen parte de la solución del problema. De no solucionarse se podrían presentar temas como la inseguridad para estudiantes y docentes en la institución.

Asimismo, debido a la falta de tecnología de última generación en los circuitos informáticos, se corre el riesgo de perder archivos, robar información confidencial o bloquear datos de diferentes equipos informáticos, que se utilizan en la institución.

La tecnología se desarrolla rápidamente, y paralelamente también surgen nuevos métodos de ruptura de redes, por lo que cada vez más instituciones públicas, empresas privadas, establecimientos educativos, hogares y otros son víctimas de la delincuencia; y se han visto en la necesidad de buscar alternativas de seguridad.

Por lo mencionado es necesario que el Colegio Particular Israel N.º 2 deba contar un sistema de seguridad con tecnología IP y un sistema el cual pueda controlar el acceso no permitido a la red, estos nos permitirán generar niveles de seguridad integral a los estudiantes, docentes y las diferentes entidades que trabajen en el mismo lugar que labora diariamente.

Justificación e importancia

Actualmente la situación de inseguridad en el país es alarmante, por lo cual hay que acoger medidas eficientes las cuales nos ayuden a controlar lo que sucede en nuestro alrededor.

Instituciones tanto públicas como privadas han optado por implementar sistemas de seguridad tecnológicas, razón por la cual la institución educativa Colegio Particular “Israel” N°2 para brindar una mejoría de seguridad en sus instalaciones ha optado por colocar un sistema de seguridad de video vigilancia para lugares exteriores del plantel, permitiendo detectar y responder rápidamente a actividades sospechosas hacia comunidad estudiantil y ante accidentes que estén ocurriendo en tiempo real, además para salvaguardar información y evitar delitos informáticos hacia la institución, se implementará un sistema de control de acceso de usuarios a la red mediante un servidor radius en el área de docentes, logrando así evitar que personas externas logren acceder a archivos, información, notas y/o registros estudiantiles.

Los sistemas a implementar en las instalaciones de la institución, contarán con equipos sumamente funcionales, mejorando así el control de la zona estudiantil y de información en

equipos tecnológicos, igualmente permitirá que a futuro se pueda agregar más equipos de seguridad en la institución, permitiendo que el proyecto sea viable y ejecutado.

Objetivos

Objetivo General

- Implementar un sistema de video vigilancia con tecnología IP para áreas exteriores y un control de acceso mediante un servidor radius para el área de docentes en el Colegio Particular “Israel” N°2.

Objetivos Específicos

- Establecer los requisitos teóricos prácticos para la selección del equipo necesario para la implementación del sistema de video vigilancia IP y verificar el estado de la infraestructura de la red.
- Implementar cámaras de video vigilancia y de los equipos necesarios.
- Configurar el control de acceso mediante el servidor radius en el área de docentes.

Alcance

El proyecto de sistema de videovigilancia con tecnología IP para áreas exteriores se lo desarrollará en el Colegio Particular “Israel” N°2, para lo cual se utilizará cámaras con la capacidad necesaria en pixeles que nos brindará una mejor visualización del sistema de video vigilancia en tiempo real mismas que se instalarán en puntos que la institución definió como estratégicos cubriendo así las zonas externas donde se logrará mantener el control dentro y fuera de la institución, las cámaras estarán conectadas a un nvr que soportará la capacidad de pixeles a usar, los videos captados por las cámaras se almacenarán en un disco duro el cual

estará implementado en el nvr lo que permitirá tener respaldos de todo lo que capte el sistema de video vigilancia. Adicionalmente, para que los docentes tengan una mejor seguridad en almacenar datos, se colocará un control de acceso mediante un servidor radius, este sistema nos ayudará a controlar los usuarios que tengan acceso a la red, mediante credenciales, lo ideal del sistema es que solo docentes tengan acceso a la red inalámbrica.

Capítulo II

Marco Teórico

Sistema de seguridad

Un sistema de seguridad es un conjunto de elementos instalados estratégicamente en sitios específicos y comunicantes que previenen, detectan o actúan contra intrusiones, robos y otros eventos que no posean acceso permitido. Es decir, es un conjunto de elementos en las instalaciones necesarios para proteger a las personas y los bienes materiales de ataques, robos, incendios, etc. (Novaseguridad, 2020)

Figura 1

Sistema electrónico de seguridad

Nota. Sistema de seguridad electrónico. Tomado de (LAGE, 2022)

Evolución del sistema de seguridad

Los sistemas de seguridad han avanzado mucho en los últimos años debido a la propia evolución de la tecnología. De esta forma, los dispositivos que se pueden encontrar en el mercado hoy en día se han perfeccionado y garantizan cada vez más opciones. Actualmente, estos pueden integrarse con otros dispositivos, lo que les permite no solo detectar posibles intentos de robo, sino también alertar en caso de incendio, fuga de gas, inundación u otro evento.

Las alarmas actuales también son más inteligentes. Esto quiere decir que están diseñados para ser controlados por los propietarios de la vivienda o negocio en cuestión y gestionados desde sus propios teléfonos móviles. (Galán, 2018)

Características de los sistemas de seguridad

Los sistemas y servicios de seguridad requieren de un conjunto de cualidades y características, que se pueden resumir en los cinco conceptos definidos a continuación:

Integridad: Son medidas asociadas a un sistema de seguridad para proteger contra daño, pérdida o modificación accidental, tanto de sus partes físicas como lógicas (hardware y software, equipos e información).

Confidencialidad: Los métodos, codificaciones e información que manejan los sistemas de seguridad se conservan secretos y con acceso limitado, los sistemas de seguridad utilizan la información que les permite reconocer intrusiones y enviar información encriptada.

Disponibilidad: este es el tiempo que un dispositivo o sistema está disponible para su uso, generalmente se expresa como un porcentaje que compara el tiempo de actividad, algunos sistemas de seguridad deben tener disponibilidad completa (24/7).

Confiabilidad: Es la capacidad de un producto o servicio para cumplir con la función propuesta. En el caso de los sistemas electrónicos, la confiabilidad se mide en el tiempo, comúnmente como MTBF (Medium Time Between Fails).

Control de acceso: Los dispositivos electrónicos (servidores, sistemas de almacenamiento) que permitan a usuarios restringidos obtener información, así como el control de ingreso y salida de personal hacia y desde áreas limitadas. (Montoya, 2014)

Ventajas y desventajas del Sistema de Seguridad

Tabla 1

Sistema de seguridad

Técnica	Ventajas	Desventajas
Reconocimiento de cara	Fácil, rápido y barato	La iluminación puede menorar la resolución de la autenticación.
Lectura de huella digital	Barato y muy seguro	Posibilidad de burla por medio de replicas, lastimaduras estas pueden alterar la autenticación.
Lectura de retina	Muy seguro	Intrusivo (molesto para usuarios)
Lectura de la palma de la mano	Necesidad baja de memoria de los patrones	Lento y no muy seguro
Reconocimiento de la firma	Barato	Puedes ser alterado por el estado emocional de la persona

Técnica	Ventajas	Desventajas
Reconocimiento de la voz	Barato, útil para accesos remotos	Lento, puede ser alterado por el estado emocional de la persona, fácilmente reproducible.

Nota. La siguiente tabla muestra las ventajas y desventajas de los sistemas de seguridad. Tomado de (Hernandez, 2016)

Componentes del sistema de seguridad

Baldo (2014) nos menciona que existen distintos tipos básicos en los sistemas de seguridad, el cual nos manifiesta en los siguiente:

Iluminación perimetral y en acceso

Las fachadas y los sistemas de seguridad de acceso deben estar iluminados, que pueden equiparse con sensores activados por movimiento y permiten ahorrar energía.

Sistema de monitoreo para la detección de intrusos

Según Baldo (2014) manifiesta que es importante contar con un sensor de movimiento (infrarrojos, microondas, combinado) que detecta el movimiento del cuerpo humano; detección perimetral (barrera de infrarrojos, cable de micrófono, microondas) que permite crear una valla invisible alrededor de la casa; sensores de apertura (magnéticos) de puertas, ventanas y portones para detectar su apertura, y sensores de rotura de cristales.

Altura

Las cámaras residenciales se utilizan para la vigilancia general de espacios y lo correcto es colocar las cámaras a una altura de 3-4 metros. Debe colocarse a una altura más baja en edificios corporativos debido al alto tráfico peatonal y la necesidad de ver los detalles.

Iluminación

Evitar la luz de fondo y minimizar los reflejos también es importante si la cámara se instala al aire libre. Agregar bombillas tanto en interiores como en exteriores es útil para priorizar las condiciones necesarias para capturar una imagen clara. También hay que tener en cuenta que, al aire libre, la luz solar varía a lo largo del día. Además, evite la luz directa sobre la cámara, ya que puede afectar el sensor de imagen. Idealmente, la cámara debe colocarse de modo que el sol brille desde atrás. La iluminación de fondo en la habitación se puede evitar con cortinas e iluminación frontal. (Baldo, 2014)

Funcionamiento del Sistema de Seguridad

Los sistemas de seguridad son cada vez más comunes en todo tipo de instalaciones y más conocidos por lo que consisten en un conjunto de cámaras y grabadoras digitales. Las cámaras de seguridad capturan imágenes de video y las grabadoras digitales almacenan estas imágenes durante varios días. Pero el manejo es similar, la cámara a través del CCD adquiere la imagen convertida y la envía por cable a la grabadora digital, y este DVR almacena la información para mostrarla en el monitor. Las imágenes se pueden ver en tiempo real o se pueden ver imágenes grabadas previamente. (Aresseguridad, 2018)

Beneficios del Sistema de Seguridad

En su estudio el autor (Admin, 2015) no indica que existen algunos beneficios que nos indica un sistema de seguridad:

- **Prevención de robo:** tener videovigilancia instalada en una empresa es una ventaja clave, ya que previene los robos. Los delincuentes y delincuentes tienen más miedo y se lo piensan dos veces antes de entrar a robar y ver las cámaras instaladas.
- **Registro legal de delincuencia:** una de las mejores cosas de un sistema de cámara de seguridad de video es la evidencia que puede proporcionar en caso de un delito, ya que estos sistemas también pueden grabar audio.
- **Capacidad de construir una red de cámaras de seguridad:** Si su empresa es muy grande, puede instalar varias cámaras conectadas a una red. La vista de cada cámara se puede transmitir a una sala de control central para la vigilancia por parte del control de seguridad.
- **Monitoreo conveniente desde cualquier lugar:** puede acceder a las cámaras de vigilancia de su empresa a través de Internet o videovigilancia. En algunos modelos, incluso puede ver su hogar o negocio con su teléfono inteligente.

Clasificación de los sistemas de seguridad

Existen cuatro grandes bloques clasificados como sistemas de seguridad, a saber:

- Robo y atraco: central de sensores y alarmas, defensa física, central de notificaciones receptores de alarma, avisadores de robo, dispositivos de acceso y circuitos cerrados televisión.
- Antirrobo: protección de la propiedad, escáner detector de rayos X, detectores explosivos, arco detector de metales.

- Incendio: extinción manual, equipos de bombeo, puertas cortafuego, alumbrado de emergencia, central receptora de alarma, bocas de incendio completo.
- Sistemas especiales: detectores de metales, sondas detectoras de nivel, sondas detector de humedad, detector de sustancias químicas, detector de presión, medicina y gasolina.

Cámaras de Videovigilancia

Una cámara de videovigilancia es un dispositivo electrónico que nos permite capturar imágenes de video en tiempo real para poder visualizarlas en un monitor o pantalla de manera local o remota; de igual forma, podemos almacenar esas imágenes en cualquier dispositivo habilitador, como una computadora, un videograbador o una simple tarjeta de memoria, lo cual es una tecnología aplicable a todo tipo de edificaciones tales como: comercios, industrias, plazas, casas, etc. Se utiliza para protección contra intrusos, control de acceso, monitoreo empresas, trabajadores y procesos, así como el control de personas y familiares en el ámbito doméstico. (Aimeseguridad, 2014)

Orígenes de las cámaras de videovigilancia

Según el autor Aimeseguridad (2014) nos señala que los orígenes de las cámaras de videovigilancia se remontan a la década de 1950, con la expansión que experimentó la tecnología en los años posteriores al final de la Segunda Guerra Mundial y sus aplicaciones se centraron en la gestión del tráfico, la banca y los grandes almacenes.

Actualidad de las cámaras de videovigilancia

Las cámaras de entonces no tienen mucho en común con las que tenemos hoy, la tecnología analógica ha dado paso a la digital, que puede ofrecer una resolución mucho mayor;

Sin embargo, debido a la facilidad de uso y al alto rendimiento que ofrecen las cámaras analógicas actuales, ambas tecnologías aún coexisten a día de hoy, lo cual es suficiente para muchos usuarios. (Aimeseguridad, 2014)

Importancia de las Cámaras de videovigilancia

Las cámaras de vigilancia están siendo apreciadas en el mundo actual, gracias al hecho de que pueden proteger su negocio y lo que más le importa. Además, aportan muchas ventajas como poder identificar a las personas en caso de acciones imprevistas o situaciones de peligro para sus dueños.

En otra de las importancias las cámaras de vigilancia no solo están relacionada con las acciones de vigilancia o seguimiento, también se pueden obtener pruebas legales para los casos en que exista un conflicto. (Diaridetarragona, 2019)

Características de las Cámaras de Videovigilancia

Según el autor Rogel (2016) nos indica algunas características de las cámaras de videovigilancia los cuales son:

- **Alimentación:** puede ser de 220VCA, 24 VCA y/o 12 VCC.
- **Tamaño del sensor:** la cámara de videovigilancia tiene un tamaño de sensor imagen como 1/2”, 1/3”, 1/2” 1/8”, 2/3”, 2/5”, 1” pulgada, para obtener calidad de imagen óptimo
- **Resolución:** este es el aspecto de calidad donde las cámaras estándar tienen 380 y las cámaras profesionales van desde 420 a 550 líneas de resolución (TVL), las cámaras en el rango de megapíxeles son especialmente útiles para aplicaciones de vigilancia donde los detalles son indispensables para poder realizar una identificación.

- **Audio:** Se consideran cámaras con micrófonos incorporados o se instalan micrófonos ocultos independiente de la cámara, pero conectado al sistema de CCTV y escuchar sonido medioambiente.
- **Sensibilidad:** entendida como la capacidad de capturar imágenes nítidas a velocidades bajas condiciones de luz, sensibilidad general de la cámara en blanco y negro sensibilidad de 1 y 0,05 lux y las cámaras a color tienen esa sensibilidad suelen oscilar entre 3 y 0,5 lux.

Ventajas de las cámaras de videovigilancia

Las ventajas de las cámaras de videovigilancia son muy simples y se pueden utilizar allí donde se requiera su montaje, además, su colocación es mucho más flexible, menos manipulable y se pueden encontrar daños.

Desventajas de las cámaras de videovigilancia

Su desventaja es que puede haber interferencia con otras señales porque a veces las señales cruzan entre sí, además el precio de las cámaras de videovigilancia inalámbricas es mucho más caro que el de las cámaras de videovigilancia con cable. (Ruiz, 2018)

Características de cámaras de videovigilancia

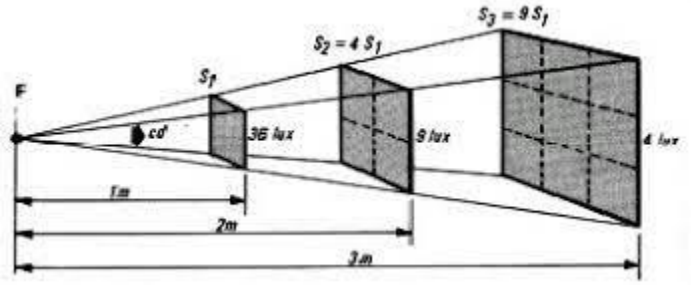
Para elegir una cámara IP, debe conocer los siguientes conceptos:

Sensibilidad

La intensidad de la luz que incide sobre la superficie. Cuanto mayor sea la sensibilidad, menor será el valor de lux, y su unidad de medida es lux.

Figura 2

Intensidad de luz



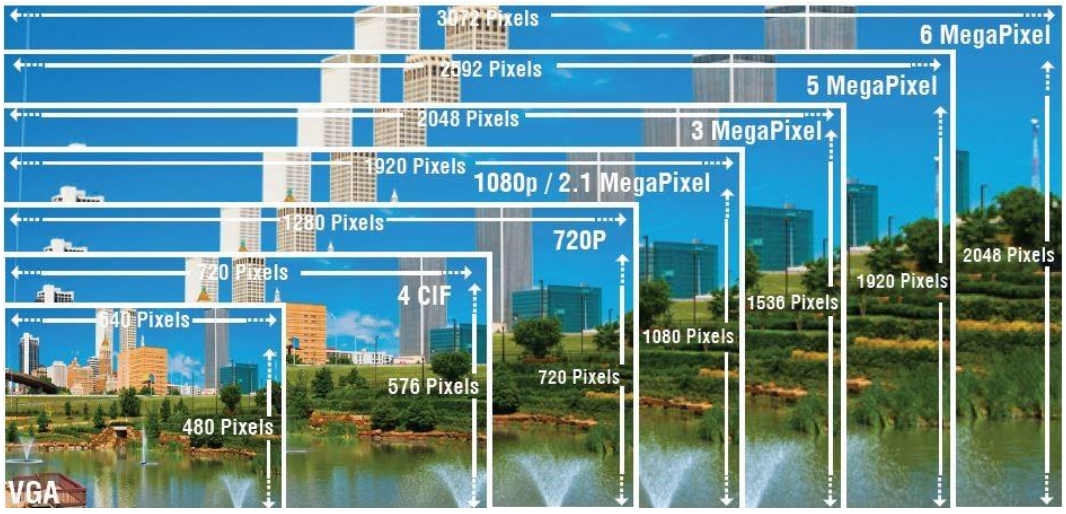
Nota. Intensidad de la luz sobre una superficie. Tomado de (Lancastergill, 2023)

Resolución

La resolución se mide en píxeles horizontales y verticales, más píxeles significa mayor resolución.

Figura 3

Resolución de cámara por pixeles



Nota. Resolución de imagen de cámara en megapíxeles. Tomado de (Garcia, 2017)

Conmutación

En el sistema de videovigilancia IP, la cámara día/noche tiene un sistema que funciona en color durante el día y cambia a funcionamiento en blanco y negro durante la noche o con poca luz para una mayor sensibilidad y resolución.

Compensación de contraluz (BLC)

Su función es evitar que las zonas de poca luz de la imagen queden demasiado oscuras y las zonas de mucha luz demasiado brillantes.

Ajuste blanco

Es muy necesario porque la cámara necesita tener una referencia de qué color blanco es para que el resto de colores tengan los tonos correctos en los ajustes de blanco que tenemos: AWC es automático, instalación y seguimiento automático ATW sucede cada vez.

Control de ganancia automática

Un circuito electrónico utilizado en cámaras que funcionan con poca luz que mantiene la señal de video a un nivel constante.

Shutter

Puede aumentar la sensibilidad de la cámara, presente en muchos sensores CCD en las cámaras.

Cámaras Full Color

Este tipo de tecnología hace referencia a la posibilidad de realizar videovigilancia en color de alta calidad las 2 horas del día con dos versiones de la solución, según el escenario:

sin operador, con operador. La versión Portless mejora la reproducción del color y reduce el ruido de la pantalla. En la versión equipada con luz, se utiliza luz un LED cálido de 3000 Kelvin. (Amortegui & Valencia, 2022)

Inteligencia artificial

Por otro lado, Scati (2022) señala que la AI para videovigilancia se centra en software o firmware cargado en ciertos dispositivos que analizan sonidos e imágenes de cámaras de videovigilancia para identificar personas, vehículos, objetos, eventos o comportamientos.

Beneficios de las soluciones de la IA

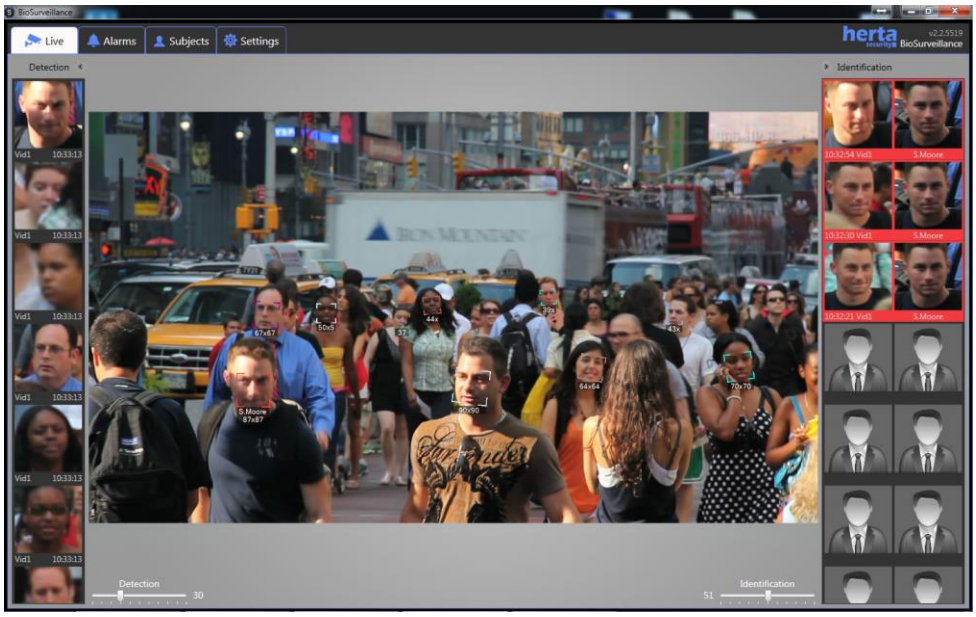
- Aumenta la satisfacción del cliente
- Ahorra esfuerzo
- Acelera las instalaciones
- Reduce complicaciones

Reconocimiento facial

Tecnología capaz de identificar o verificar a un sujeto por medio de una imagen, video o cualquier elemento audiovisual de su rostro. Generalmente, este identificador se utiliza para autorizar a una aplicación, sistema o servicio. Es una forma de identificación biométrica que utiliza medidas corporales, en este caso la cara y la cabeza, para comprobar la identidad de una persona a través de patrones biométricos y otros datos. La tecnología recopila un conjunto de información biométricos de cada persona asociados con su rostro y expresiones faciales para identificar, verificar y/o autenticar a una persona. (Electronicid, 2022)

Figura 4

Reconocimiento facial mediante cámara



Nota. Reconocimiento facial a personas mediante cámaras de videovigilancia. Tomado de (Videoanaliticas.com, 2016)

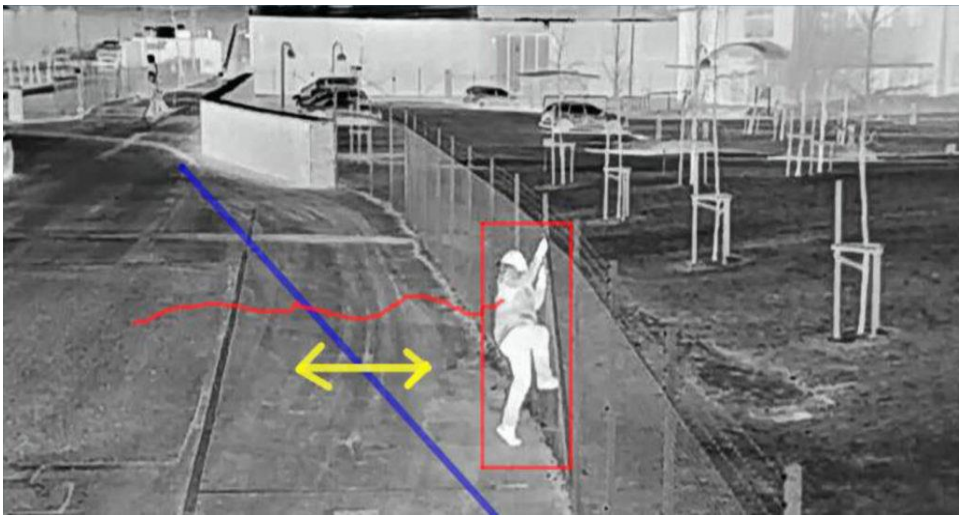
Seguridad Perimetral

La seguridad perimetral es la integración de elementos y sistemas de seguridad electrónicos y mecánicos para proteger áreas físicas. Diseñado para controlar el perímetro de su propiedad protegida, es muy útil como elemento disuasorio y para evitar el acceso no autorizado. La seguridad perimetral es la primera línea de defensa en cualquier sistema de seguridad.

La protección de marcos es un desafío constante para los sistemas de seguridad. Se deben considerar varias características al prevenir edificios industriales. Algunos de estos son distancias defendibles, condiciones climáticas, morfología del terreno, etc. (Covertsecurit, 2022)

Figura 5

Toma nocturna de una cámara



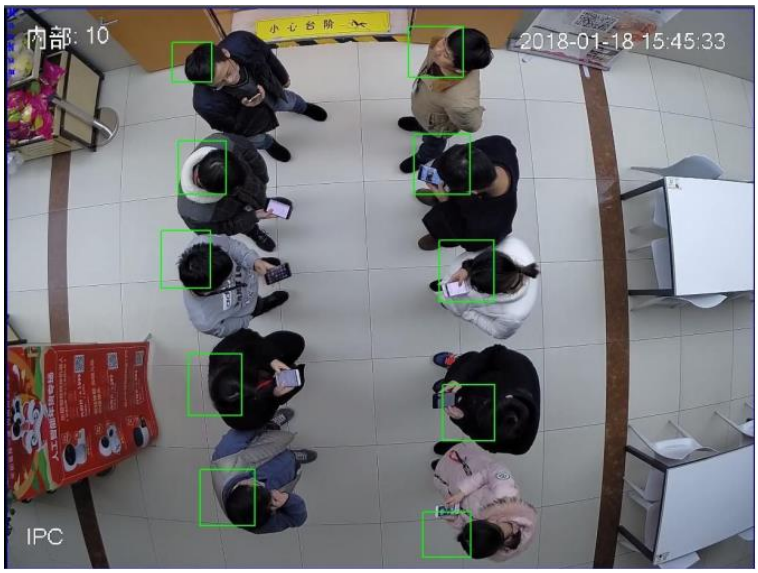
Nota. Toma nocturna de una cámara. Tomado de (cartronicgroup, 2023)

Conteo de personas

Las cámaras IP de conteo de personas con grabación y alimentación PoE son especialmente útiles para empresas y locales comerciales porque te permite controlar el número de personas en sus instalaciones, obtener informes diarios, mensuales o anuales sobre la capacidad y saber cuántas personas están pasando para un área específica en su lugar.

Figura 6

Conteo de personas mediante cámara



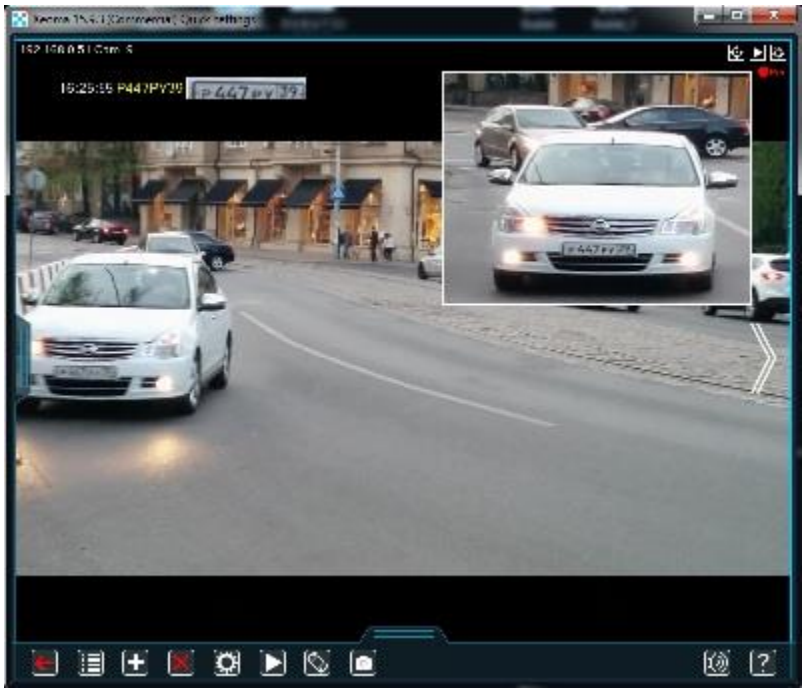
Nota. Conteo de personas mediante cámaras. Tomado de (Tecalsa, s.f.)

ANPR

Las cámaras ANPR, diseñadas solo para leer matrículas, pueden capturar imágenes perfectas de vehículos en movimiento (incluso aquellos que se mueven a alta velocidad) gracias a su excelente velocidad de obturación: este tipo de dispositivo es común con una velocidad de obturación de 1/10,000 (es decir, al tomar una foto). en apenas una décima de milésima de segundo). (Merino, 2019)

Figura 7

Funcionamiento de cámara ANPR



Nota. Funcionamiento de cámara ANPR captando una matrícula vehicular. Tomado de (Grupo Meyah, 2023)

Video IP

El video IP, a menudo conocido como vigilancia IP para aplicaciones específicas en el campo de la vigilancia de seguridad y la vigilancia remota, es un sistema que permite a los usuarios controlar y grabar video a través de una red IP (LAN, /WAN/Internet). Los sistemas de video analógico, video IP, utilizan la red como un concentrador central para transferir información sin necesidad de cables punto a punto dedicados. El término video IP se refiere a las fuentes de video y audio disponibles a través del sistema. (Tecnoseguro, 2018)

Elementos de un sistema de videovigilancia IP

- **Cámaras:** Pueden ser analógicas o digitales.
- **Monitores:** Pantallas que muestran lo que está viendo la cámara.
- **Dispositivo de control:** Conmutadores y matrices de video.
- **Estaciones de monitorización:** Permite reflejar los videos almacenados en tiempo real.
- **Transmisión:** Recibe la señal del video, puede ser por coaxial o línea telefónica.

Ventajas de sistema de videovigilancia IP

Las ventajas pueden variar desde reforzar la productividad hasta proteger los activos de su empresa y proteger a los empleados de malas llamadas con evidencia de video irrefutable. (Bdrinformatica, 2022)

Reduce el riesgo de robo y fraude por parte de los empleados.

El robo corporativo es mayor que el robo de identidad y el fraude en línea en los negocios, y el 75 % de los empleados han sido asaltados por su empresa al menos una vez. El fraude de los empleados sigue siendo una cuestión importante. (Bdrinformatica, 2022)

Mejora las operaciones y la productividad

La baja productividad y los procedimientos disfuncionales pueden impedir que se logre este objetivo, esto no es ninguna novedad. Es común que los empleados chateen durante las horas de trabajo, lo que conduce a una baja productividad.

Reducir el riesgo de vandalismo

Las cámaras colocadas en lugares visibles acortan drásticamente la amenaza de violencia y vandalismo en las empresas. (Bdrinformatica, 2022)

Conectividad

Cuando una cámara IP está en línea, los datos que produce están disponibles desde casi cualquier lugar que utilice la infraestructura de red de datos global sin cableado adicional. (Sigmixv, 2021)

Ahorro de cableado

Las cámaras de vigilancia IP pueden utilizar la tecnología PoE (Power Over Ethernet). Esto permite que el mismo cable (UTP) transporte tanto video como energía.

Escalabilidad y flexibilidad del almacenamiento

Esto permite que el almacén de información esté perfectamente distribuido a una o más computadoras con acceso a la red de datos del sistema. (Sigmixv, 2021)

Integración con otras aplicaciones

El formato de transmisión digital permite una fácil integración de datos de video en otros sistemas de seguridad electrónica. Esta característica permite una transmisión de video rápida, competente y segura a través de múltiples plataformas seguras.

Configuración y ajuste remotos

La capacidad de comunicación bidireccional de las cámaras IP de videovigilancia permite el restablecimiento remoto de los parámetros internos del dispositivo. (Sigmixv, 2021)

Mejorar la calidad del video

Esta resolución es superada con creces por las cámaras IP más baratas del mercado, que rondan los 1,2 megapíxeles. Por lo tanto, una cámara con tecnología de transmisión IP proporciona más información, una mayor resolución y, por lo tanto, una mayor calidad de video.

Inmunidad al ruido

Las cámaras CCTV analógicas convencionales transmiten una imagen de video en forma de una señal eléctrica analógica. Este tipo de señal es muy sensible a la distorsión de señales eléctricas externas. (Sigmixv, 2021)

Cámaras Analógicas

Cámaras de video vigilancia que transmiten sus videos e imágenes a través de cable coaxial. Ofrecen buena calidad de imagen y video, pero tiene limitaciones como su resolución, no puede transmitir lo que captura por una red de internet, tiende a tener interferencia en su señal de transmisión. (PCREDCOM, 2021)

Figura 8

Cámara analógica de exterior

Nota. Cámara analógica para exteriores. Tomado de (PCREDCOM, 2021)

Especificaciones de cámaras analógicas

- Tiene cascaras de aluminio los cuales otorgan protección a efectos externos.
- Soporta diferentes tipos de climas, temperaturas.
- Efecto de contraluz y balance de blancos para que sus imágenes no pierdan calidad.
- Pueden usarse en exteriores como en interiores.
- Tienen un audio bueno ya que cuenta con reducción de ruido.

Características de las cámaras analógicas

Instalación

Para poder instalarlas se necesita cable coaxial el cual transmitirá los datos obtenidos por la cámara imagen o video mandándolas al centro de mando. (PCREDCOM, 2021)

Resolución

Se toma en cuenta las líneas existentes entre verticales y horizontales, solo así se podrá obtener la correcta resolución de la imagen. (PCREDCOM, 2021)

Forma de señal de transmisión

Se usa los dispositivos llamados balum, los cuales son los encargados de tener imágenes o videos de forma directa para que sea correcta la transmisión. (PCREDCOM, 2021)

Cámaras IP

Dispositivos de video vigilancia conectados a una red de computadoras, transmiten video e imágenes en tiempo real a través de internet. Se puede ver y controlar desde cualquier lugar con una conexión a internet.

Ofrecen una variedad de características avanzadas como la resolución en alta definición, detección de movimiento, almacenamiento de video tanto en nvr como en la nube y tiene enfoque automático. Estas características mejorarán la seguridad en vigilancia y facilitarán la detección de incidentes.

Como afirma (Cantalapiedra, 2017) “Las cámaras IP son una solución eficaz y eficiente en términos económicos. Sin embargo, es importante tener en cuenta que la seguridad de la cámara IP depende de la configuración y el uso adecuado de las mismas”

Figura 9

Cámara IP de visión nocturna

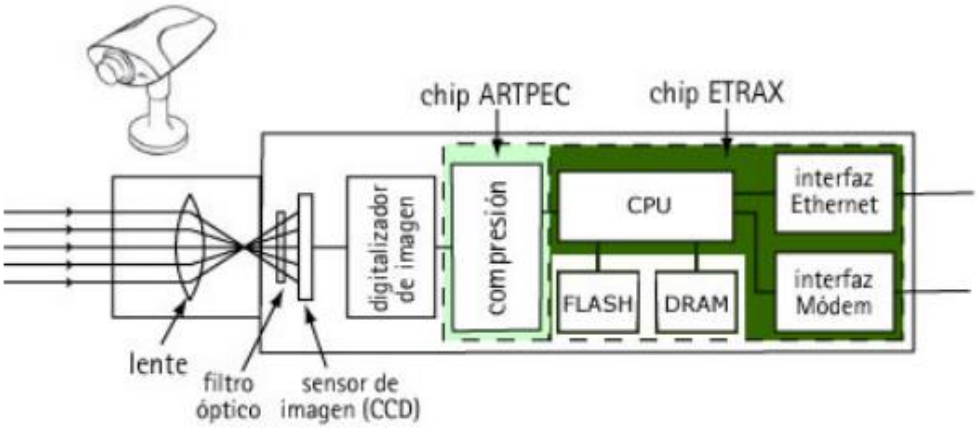
Nota. Cámara IP de visión nocturna para exteriores e interiores. Tomado de (Zoom Informatica, 2016)

Parte interna de una cámara IP

Las cámaras IP poseen un lente que enfoca la imagen en el sensor de imágenes. Antes de llegar al sensor, la imagen pasa a través de un filtro óptico, que elimina cualquier luz infrarroja, para que los colores mostrados sean “correctos”. El sensor de imagen convierte la imagen compuesta por información lumínica en señales eléctricas. Estas señales eléctricas digitales están ya en un formato que puede comprimirse y enviarse a través de la red. (López, 2007)

Figura 10

Arquitectura interna de cámara IP



Nota. Arquitectura interna de una cámara IP. Tomada de (López, 2007)

Lente

Componente encargado de capturar luz para enfocarla sobre el sensor de imagen, está compuesta de varios elementos ópticos como cristales, que funcionan conjuntamente para la precisión de la luz en el enfoque.

Tiene una apertura la cual funciona como controladora de ingreso de luz, esta apertura es medida en f-stop.

Adicionalmente tiene una distancia focal, medida en milímetros, cuya función es tener el control del alcance de la imagen capturada, mientras más distancia focal se tenga permitirá capturar imágenes con alcance más amplios. (Casarino, 2015)

Sensor de imagen

Componente el cual captura la imagen para poderla convertir en una señal eléctrica, está compuesto de foto sitos los cuales corresponden elementalmente a la imagen, conocidos como píxeles. Los sensores de imagen que son más usados son:

- CCD

Proporcionan imágenes de mayor calidad, son altos en costo y consumen más energía.

- CMOS

Tienen mayor eficiencia en el consumo de energía, son de bajo costo y puede que su imagen no sea de tan buena calidad.

Procesador de imagen

Es el hardware o software que se encarga de procesar y analizar la imagen capturada por el sensor de imagen, para poderla trasmitir con facilidad mediante la red, entre características primordiales tenemos la detección de movimiento, mejoramiento de imagen, seguimiento de objetos en movimiento y comprensión de datos para una determinada calidad o resolución de imagen. (aula Clic, 2020)

Sistema de chip (SoC)

Sirve para ahorrar espacio y concentrar funciones de la cámara, como el sensor de imagen, procesador de imagen, memoria y moduladores de comunicación en un solo chip, también cuenta con un microcontrolador el cual configura y controla diferentes componentes

del sistema. Permite almacenar video y detectar movimiento, logrando que se realice el grabado solo cuando lo amerite. (Romero, 2021)

Chip Ethernet

Así como lo afirma (Martí, 2013) “El chip ethernet en cámaras IP ofrece conectividad de red para poder transmitir las imágenes captadas a través de la red IP”

Permite a la cámara conectarse a una red mediante un cable de red ethernet o por una red inalámbrica, lo cual logrará la comunicación entre las cámaras que estén en red y el nvr, permitiendo acceder a las cámaras desde cualquier lugar.

Tipos de cámaras IP

Cámara Box

Su diseño es en forma de caja, teniendo la capacidad de conectarse a la red mediante un chip ethernet o mediante red Wi-Fi.

Tiene implementado un sensor de alta calidad para la imagen, otorgando una resolución de alta calidad tanto en imágenes como en videos, transmitiéndolos de la misma calidad en tiempo real. Usada para exteriores e interiores ya que permite cubrir un gran ángulo de visión del área. (Martí, 2013)

Figura 11

Cámara IP tipo Box

Nota. Cámara IP tipo Box modelo IP8155HP. Tomado de (VIVOTEK, s.f.)

Cámara de red PTZ (pant tlit zoom)

Llamadas también como domo móvil es una cámara con la capacidad de movimiento en direcciones diferentes, permitiendo ser controlada por los usuarios logrando posicionarla en la dirección que sea desde una ubicación remota, brindando una cobertura y flexibilidad de vigilancia de mejor calidad. (Martí, 2013)

Figura 12

Cámara Domo PTZ

Nota. Cámara IP PTZ modelo PTZ-N42151-DE. Tomado de (SistemSeguridad, s.f.)

Cámara Bullet

Cámaras para exteriores. Tienen diseño aerodinámico y compacto, similar a una forma de bala, contienen un lente fija, gran resolución y un ángulo de visión lo suficientemente amplio. Adicionalmente y mejorando su rendimiento físico, son resistentes al agua y se adaptan a condiciones climáticas extremas. (Martí, 2013)

Figura 13

Cámara Bullet Alhua

Nota. Cámara Bullet Alhua modelo DH-HAC-HFW2501TUN-Z-A-27135-S2. Tomado de (ZCmayoristas, 2023)

Cámara mini domo

Son una versión compacta de las cámaras domo tradicionales, son ideales para exteriores como para interiores en cualquier tipo de infraestructura, ventajosamente etas cámaras son discretas gracias a su tamaño compacto, así mismo tienen resistencia al agua y a condiciones climáticas extremas.

Tienen reconocimiento facial, detección de movimiento y alertas en caso de accidentes. (Martí, 2013)

Figura 14

Cámara Mini Domo HikVision

Nota. Cámara mini domo HikVision modelo Fisheye 360A IR. Tomado de (TST Ecuador, 2023)

Medios de Transmisión

Cable UTP

Cable usado para conectar dispositivos en red, transmite variedad de información por lo cual es usado en áreas de red local, el cable es simple de instalar y configurar, resistente a interferencias electromagnéticas. (Irving, 2021)

Categorías del cable UTP

Tabla 2

Categorías de cable UTP

CATEGORIA	VELOCIDAD	FRECUENCIA	DISTANCIA	USOS
5	100 Mbps	100 MHz	100 m	Señales de video, telefonía
5e	1 Gbps	100 MHz	100 m	Para uso interior y exterior de edificios, comerciales, escuelas, colegios u oficinas.
6	10 Gbps	250 MHz	55 m	Infraestructura de telecomunicaciones genérica, redes de áreas amplias.
6a	10 Gbps	500 MHz	100 m	En entornos con alta interferencia electromagnética y aplicaciones de alto rendimiento.

Nota. Tabla indicadora de especificaciones de cada categoría del cable UTP. Tomado de (Irving, 2021)

Normas de cable UTP

Formado por ocho hilos de cobre, formando cuatro pares de colores los cuales son:

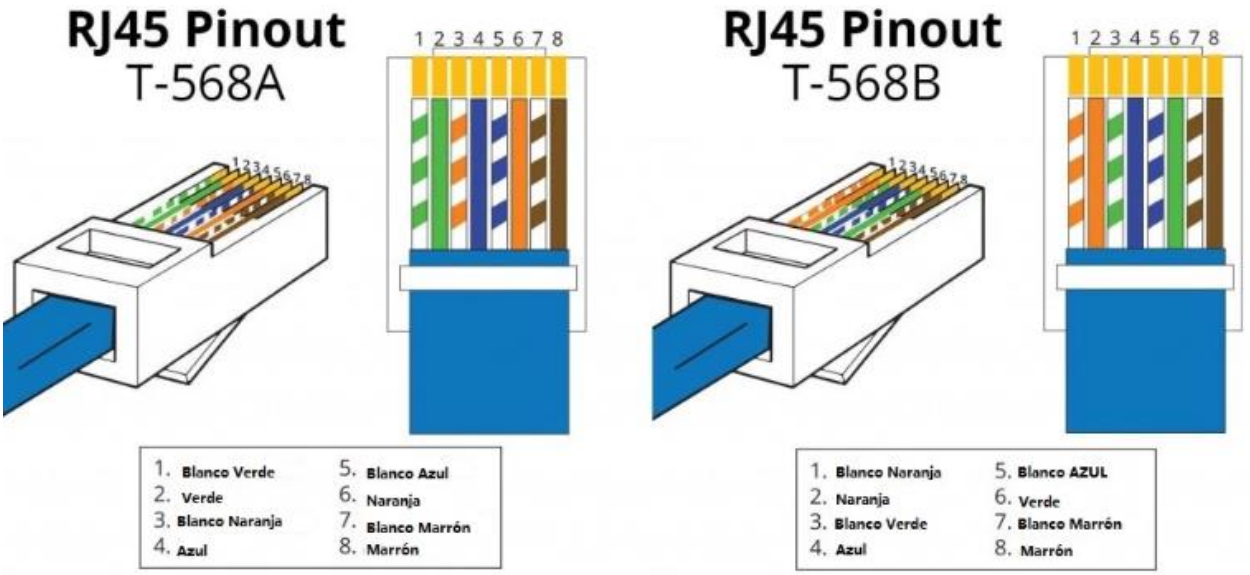
- Blanco con naranja, naranja
- Blanco con verde, verde
- Blanco con azul, azul
- Blanco con café, café

Existen normas para poder colocar el cable utp, respetando un debido orden, las normas que se deben seguir son las EIA/TIA-568A y EIA/TIA-568B.

Norma de colores EIA/TIA-568 A y EIA/TIA-568 B

Figura 15

Código de colores en 568A y 568B



Nota. Código de colores basados en las normas T-568 A y T-568 B. Tomado de (Worton, 2021)

Ventajas y desventajas del cable UTP

Tabla 3

Ventajas y desventajas del cable UTP

Ventajas	Desventajas
El cable de red es más compatible y se encuentra con facilidad en el comercio.	Es probable que tenga interferencia electromagnética y de radio frecuencia.
La velocidad en transmisión de datos es más fluida que con cable de cobre.	Tiene un alcance de señal más corto comparado a cable coaxial o fibra óptica.
Bajo costo de adquisición.	Alto costo de equipos que requieren el tipo de cable UTP.
Puede ser ubicado sea en exteriores como interiores de infraestructuras.	Su ancho de banda es limitado.

Nota. Ventajas y desventajas del cable UTP. Tomado de (Rico, 2017)

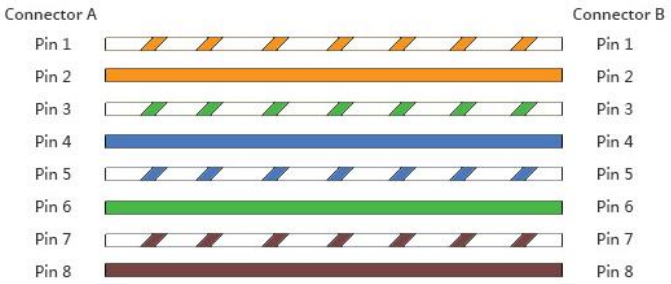
Segmentos por cable UTP

Cable Directo (Pin a Pin)

Cuya dirección no varía, ambos extremos del cable utilizan el mismo estándar ya sea T-568 A o T-568 B, dando, así como resultado que ambos extremos del cable tengan el mismo orden de colores. Son utilizados en conexiones de ordenadores a switches, enrutadores o concentradores. (Walton, 2021)

Figura 16

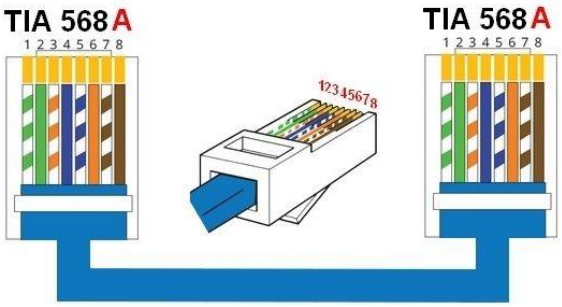
Conexión de cable directo



Nota. Conexión directa de cable UTP, basado en la norma T-568B. Tomado de (Worton, FS Community, 2021)

Figura 17

Conexión cable directo



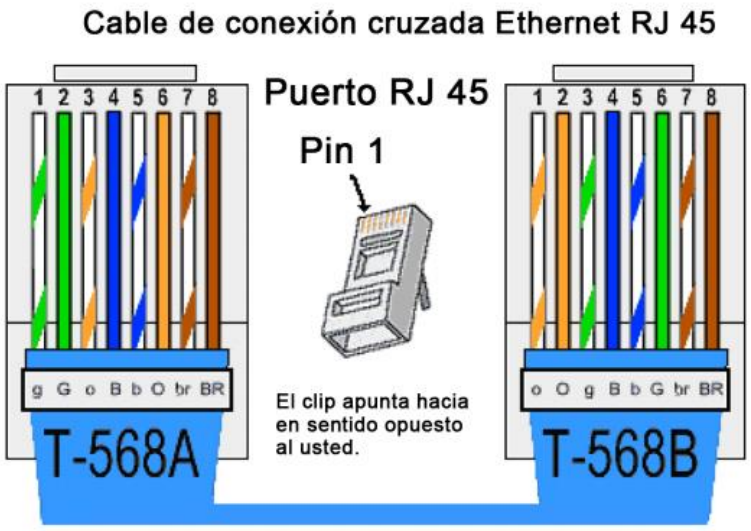
Nota. Conexión directa de cable UTP, basado en la norma T-568B. Tomado de (Walton, 2021)

Cable Cruzado

Su dirección varia de un extremo con el otro, usando así los dos tipos de estándares un extremo usará el T-568 A y el otro extremo el T-568 B, obteniendo así que un extremo tenga dos pares de transmisión y dos pares de recepción. Se lo puede implementar de switch a switch, router a router o de host a host. (Walton, 2021)

Figura 18

Conexión cable cruzado UTP



Nota. Conexión cruzada de cable UTP, ocupando normas T-568 A Y T-568B. Tomado de (Abraham, s.f.)

Fibra Óptica

Medio de transmisión de datos por medio de un hilo de vidrio y plástico. Transmite señales de luz a larga distancia por medio de laser o led, la fibra óptica tiene mínima pérdida y más resistencia a interferencias electromagnéticas. Usada para transmitir datos en redes, conexiones de audio de calidad alta y en fuentes de iluminación de espacios reducidos. (Castillo, 2019)

Cable de fibra óptica

- Núcleo

  Hilo de vidrio formado de dióxido de silicio, conductor de luz, su diámetro es de 8 a 62,5 micrómetros (μm). (Coimbra, 2011)

- Revestimiento

  Tubo de vidrio formado de dióxido de silicio, su objetivo es guiar la luz hacia el núcleo y evitar que salga de él. Su diámetro es de 125 micrómetros (μm). (Coimbra, 2011)

- Drenaje de humedad

  Se lo utiliza para que la humedad existente pueda salir, este elemento va enrollado al núcleo, dando así una buena funcionalidad de la fibra y evitando daños. (Castillo, 2019)

- Hilos de fibra

  Funcionan como conductores de luz y de datos en redes, formado por un cristal de silicio, permitiendo que la luz pueda reflejarse y reflectarse hasta llegar a su punto de destino. (Castillo, 2019)

- Buffer y Cladding

  Gel que impide que los rayos de la luz no escapen de la fibra cubriendo los hilos de la fibra. (Castillo, 2019)

- Cinta Mylar y capas aislantes

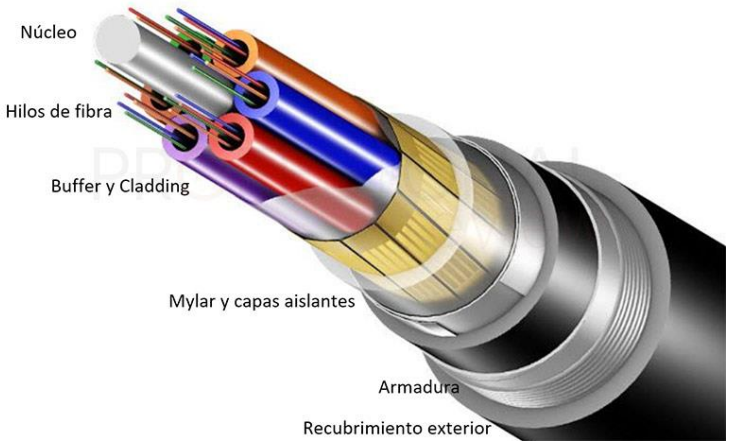
  Sirven para proteger daños físicos a la fibra en el momento de realizar instalaciones y en su uso, evitan que la fibra tenga interferencias eléctricas obteniendo una mejor calidad de señal. (Castillo, 2019)

- Recubrimiento Exterior

Brinda protección a la superficie exterior de la fibra protegiéndolo de factores climáticos y mecánicos, puede estar recubierto por tubo pvc, polietileno o fluoruro de polietileno. (Castillo, 2019)

Figura 19

Partes del cable de fibra óptica



Nota. Partes del cable de fibra óptica. Tomado de (Castillo, 2019)

Tipos de fibra óptica

Monomodo

Emite un solo modo de luz, esto se debe a que su diámetro es corto, tiene menos probabilidad de tener atenuación o dispersión de señal, lo cual lo vuelve eficiente en sistemas de larga distancia y alta velocidad. (Coimbra, 2011)

Multimodo

Se puede llegar a transmitir varias señales de luz, su costo es inferior al de la fibra monomodo, es aplicado en sistemas de corta distancia y es probable que tenga atenuaciones debido a la dispersión modal. (Castillo, 2019)

Ventajas y Desventajas de la fibra óptica

Tabla 4

Ventajas y Desventajas de la fibra óptica

VENTAJAS	DESVENTAJAS
Transmisión de gran cantidad de datos a alta velocidad.	Su instalación es limitada en zonas rurales y de difícil acceso.
Contienen inmunidad a interferencias electromagnéticas o ruido.	Es demasiado frágil, puede tener daños si el personal no está debidamente capacitado para poder implementarla.
Su tiempo de durabilidad es mejor a la de otras transmisiones de datos, lo cual es apropiado para aplicarlas en proyectos de largo plazo.	El mantenimiento es más costoso comparado con otros medios de transmisión.

Nota. Ventajas y desventajas de transmisión por fibra óptica. Tomado de (Castillo, 2019)

Red inalámbrica

Las redes inalámbricas permiten que los dispositivos permanezcan conectados a una red sin necesidad de cables. El punto de acceso mejora su señal Wi-Fi para que sus dispositivos puedan permanecer conectados a la red incluso cuando está lejos del enrutador. Cuando se conecta a un punto de acceso WiFi en una cafetería, hotel, sala de aeropuerto u otro lugar público, está conectado a la red inalámbrica de esa empresa. (Cisco, 2015)

Beneficios de una red inalámbrica

Como señala Cisco (2015) “Las empresas pueden obtener varias ventajas de una red inalámbrica de Cisco”, incluidas las siguientes:

- **Comodidad:** acceda a los recursos de la red desde cualquier lugar dentro de la cobertura de su red inalámbrica o desde cualquier punto de acceso Wi-Fi.
- **Movilidad:** No se ata a su escritorio como una conexión por cable
- **Productividad:** el acceso inalámbrico a Internet y las aplicaciones y los recursos empresariales clave ayuda a los empleados a realizar su trabajo y facilita la colaboración.
- **Escalabilidad:** las redes inalámbricas se pueden expandir fácilmente utilizando el equipo existente, pero las redes cableadas pueden requerir cables adicionales.
- **Seguridad:** Los avances en las redes inalámbricas ofrecen una sólida protección de seguridad.
- **Costos reducidos:** las redes inalámbricas eliminan o eliminan los costos de cableado, lo que resulta en costos operativos más bajos que las redes cableadas.

Tipos de redes inalámbricas

Redes WLAN

Esta red permite a los usuarios establecer conexiones inalámbricas dentro del área de cobertura. En una WLAN de infraestructura, las estaciones inalámbricas (dispositivos con NIC de radio o módems externos) se conectan a puntos de acceso inalámbricos que actúan como puentes entre las estaciones y la red troncal existente.

Una WLAN punto a punto permite múltiples usuarios dentro de un área limitada. La tecnología utilizada en esta red es Wi-Fi. Como red inalámbrica para el hogar y la empresa, Wi-Fi se ha convertido en el estándar para el acceso a Internet y el uso compartido de recursos. (Coñapes, 2015)

Redes WPAN

Esta red permite la comunicación inalámbrica para dispositivos como teléfonos móviles y ordenadores portátiles utilizados en quirófanos privados (POS). POS es el espacio que rodea a una persona, hasta una distancia aproximada de 10 metros. El objetivo de esta red es comunicar cualquier dispositivo personal (ordenador, terminal móvil, PDA, etc.) con sus periféricos, así como permitir la comunicación directa de corto alcance entre estos dispositivos.

En la actualidad las dos principales tecnologías que utiliza en red son Bluetooth y la luz infrarroja.

- **Bluetooth:** una tecnología de cable alternativa que utiliza ondas de radio para transmitir datos en un rango de 1 a 100 metros (generalmente unos 10 metros).
- **ZigBee:** utilizado principalmente en entornos industriales o comerciales y aplicaciones de seguridad. Es económico, tiene un consumo muy bajo y es bastante inviolable, pero no está diseñado para altas velocidades de

transferencia. Esto está en el rango de 20-250 kbps, mucho más bajo que Bluetooth.

- **Infrarrojos:** Las redes inalámbricas de infrarrojos no funcionan en objetos sólidos como paredes. Su rango normal es más estrecho que el de Bluetooth o ZigBee, y el transmisor y el receptor deben poder verse entre sí para que la transmisión funcione. (Coñapes, 2015)

Redes WMAN

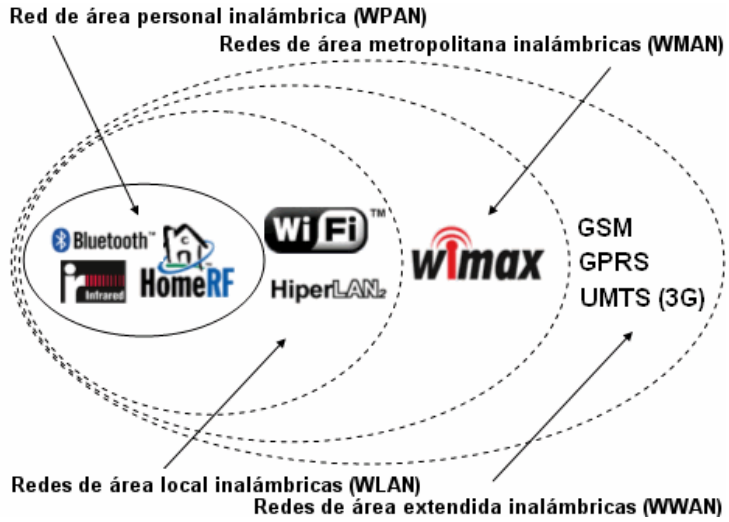
La red WMAN permite que los usuarios puedan crear conexiones inalámbricas entre múltiples ubicaciones dentro de un área, como entre múltiples edificios de oficinas dentro de una ciudad o en un campus universitario. No hay necesidad de costosos cables de fibra óptica o cobre ni de alquiler de líneas. La WMAN utiliza ondas de radio o infrarrojos para transmitir datos. Tienen un radio de operación mayor que WLAN. Es del orden de decenas de kilómetros. suficiente para cubrir a toda la población. Las WMAN pueden interconectar WLAN. (Coñapes, 2015)

Redes WWAN

El autor corporativo Sony (2018) señala que la tecnología WWAN (Wireless Wide Área Network), también conocida como banda ancha móvil, permite el acceso a Internet mediante redes celulares. Además de los beneficios de la movilidad inalámbrica, puede aprovechar la banda ancha regular como ADSL y cable.

Figura 20

Red WWAN



Nota. Funcionamiento de una red WWAN. Tomado de (Coñapes, 2015)

Estándares y Normativas

Los estándares y normativas son elementos fundamentales que se centran en reglas que deben cumplirse para realizar una determinada actividad, esto tiene la finalidad que los procesos trabajen de manera globalizada.

Estándar IEEE 802.11

El estándar 802.11 es un conjunto parámetros desarrollado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Define parámetros tales como:

- Señales RF
- Modulación
- Codificación
- Bandas

- Canales
- Velocidades de transmisión

Figura 21

Estándares IEEE 802.11

Nota. Estándares Wi-fi IEEE 802.11. Tomado de (Redesinalambricas, 2019)

Estándar IEEE 802.11a:

Es el estándar más antiguo y opera en la banda de frecuencia de 5 GHz (gigahercios) con 12 canales a una velocidad teórica de 54 Mbit/s (megabits por segundo).

Estándar IEEE 802.11b

Se trata de una revisión del estándar original (el anterior), operando en la banda de frecuencia de 2,4 GHz con una velocidad máxima de 11 Mbit/s.

Estándar IEEE 802.11g

Utiliza la misma banda, pero a una velocidad equivalente a la de IEEE 802.11a, es decir 54 Mbit/s Es el estándar más utilizado por los usuarios particulares desde su aparición en el mercado con la etapa de mayor expansión de este tipo de tecnología, por lo que existen muchos dispositivos que cuentan con este estándar en los hogares. (Redesinalambricas, 2019)

Estándar IEEE 802.11g

Esta es una pequeña variante de IEEE 802.11g que permite velocidades de hasta 108 MB/s, pero solo en circunstancias muy especiales.

Estándar IEEE 802.11n

Utiliza las bandas de frecuencia de 2,4 GHz y 5 GHz simultáneamente y es compatible con todos los estándares anteriores. Es el estándar que ofrecen actualmente la mayoría de los fabricantes. Tiene una tasa de transferencia teórica (velocidad) de 300Mbps.

Estándar IEEE 802.11ac

Este es el último estándar aprobado por este estándar. Funciona en la banda de 5 GHz y amplía el ancho de banda hasta los 160 MHz. Mejora la tasa de transferencia (velocidad) y llega a 1 GHz (1 gigabit por segundo = 1.000 Mbit/s). (Redesinalambricas, 2019)

Estándar IEEE 802.11i

IEEE 802.11i es un estándar de la industria para asegurar redes inalámbricas. La versión de Wi-Fi Alliance se llama WPA2. Tanto 802.11i como WPA2 utilizan el estándar de cifrado avanzado (AES). AES se considera actualmente el protocolo de cifrado más seguro.

Las redes inalámbricas modernas siempre deben usar el estándar 802.11i/WPA2. WPA2 es la versión Wi-Fi de 802.11i, por lo que los términos WPA2 y 802.11i suelen usarse indistintamente. Desde 2006, todos los dispositivos con el logotipo Wi-Fi Certified cuentan con la certificación WPA2. (Sapalomera, 2006)

EIA/TIA 586A

El estándar de cableado estructurado TIA/EIA define cómo deben diseñarse, construirse y administrarse los sistemas de cableado estructurado. Esto significa que el sistema está diseñado con bloques que tienen características de desempeño muy específicas. Los bloques están integrados jerárquicamente para crear un sistema de comunicaciones unificado. Además, los extremos de los cables UTP, ya sean de Categoría 5 o Categoría 6, tienen conectores RJ45 en el orden de color especificado por el estándar de izquierda a derecha: blanco-verde-blanco-blanco naranja azul-blanco azul-naranja-blanco marrón-marrón. (Elcapored, 2020)

EIA/TIA 586B

Esto se debe a las revisiones de EIA/TIA 568A. TIA/EIA-568-B intenta definir un estándar que permitirá el diseño y la implementación de sistemas de cableado estructurado entre edificios en edificios comerciales y entornos de campus.

Se dividen en:

- **ANSI/TIA/EIA-568-B1:** Cables de telecomunicaciones comunes en edificios comerciales. (Requisitos y recomendaciones para la construcción, composición, interfaz, instalación, parámetros de desempeño y verificación).
- **TIA/EIA 568-B2:** Requisitos generales para componentes de par trenzado balanceado.
- **TIA/EIA 568-B3:** Componentes de cable, fibra óptica (Cables, conectores, hardware de conexión, cables, puentes, equipo de prueba). (Elcapored, 2020)

WI-FI (Wireless Fidelity)

Wi-Fi es el nombre de una popular tecnología de red de área local inalámbrica que utiliza ondas de radio para proporcionar Internet inalámbrico de alta velocidad y conectividad de

red, según el estándar IEEE 802.11. Wi-Fi es una marca comercial registrada de Wi-Fi Alliance, que limita el uso del término Wi-Fi Certified a productos que hayan superado las pruebas de certificación de interoperabilidad. Wireless Fidelity es un término general que hace referencia al estándar de comunicación IEEE 802.11 para redes WLAN. (MexicoNewark, 2018)

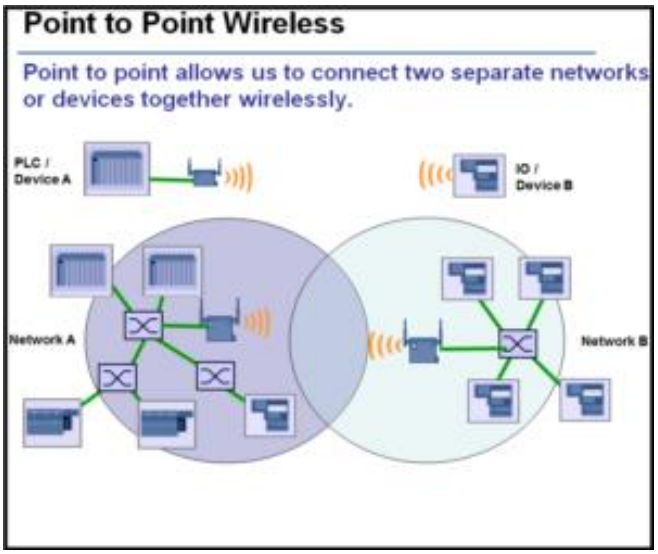
Arquitecturas inalámbricas

Red punto a punto (P2P) o ad-hoc

La conectividad P2P se puede lograr mediante tecnología Bluetooth o WiFi. Las arquitecturas P2P suelen tener una conexión inalámbrica dedicada entre dos dispositivos, dos AP (puntos de acceso) o entre un dispositivo y un AP. Estos dispositivos son, por ejemplo, controladores PROFINET y dispositivos IO. En algunos casos, un dispositivo puede tener capacidades inalámbricas integradas, lo que elimina la necesidad de un AP separado. La principal ventaja de los enlaces P2P es tener un canal dedicado para la comunicación. Los canales no se comparten, por lo que hay más ancho de banda disponible en el enlace inalámbrico. Tenga en cuenta que la mayoría de las aplicaciones Bluetooth utilizan conexiones P2P como método de comunicación principal. (Profinetuniversity, 2019)

Figura 22

Red Punto a Punto



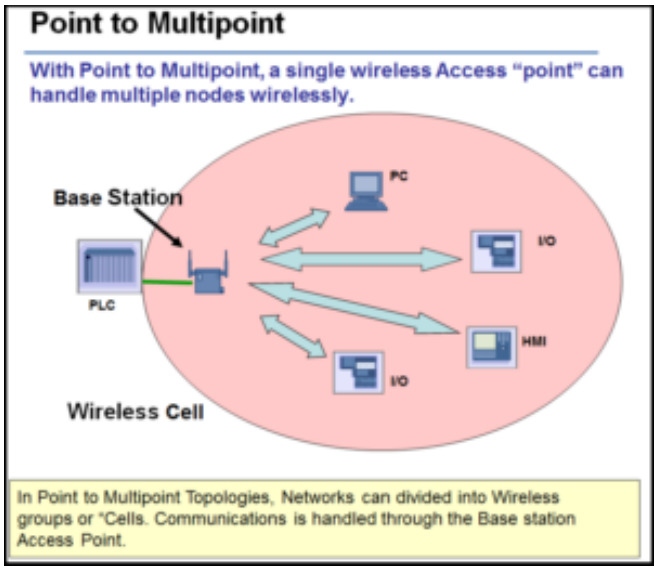
Nota. Estructura de una red punto a punto. Tomado de (Tic.portal, 2022)

Red punto a multipunto (P2M/Infraestructura)

La arquitectura P2M se realiza principalmente a través de WiFi, pero Bluetooth también es una opción. P2M permite a los usuarios vincular múltiples estaciones inalámbricas (clientes) a un controlador u otro dispositivo (PC/SCADA) a través de un solo AP (punto de acceso). La mayoría de las redes inalámbricas utilizan la infraestructura inalámbrica (P2M) como modo inalámbrico principal. Por ejemplo, supongamos que tiene una red PROFINET que consta de computadoras portátiles, HMI y varios dispositivos accesibles a través de conexiones inalámbricas. (Profinetuniversity, 2019)

Figura 23

Red punto a multipunto



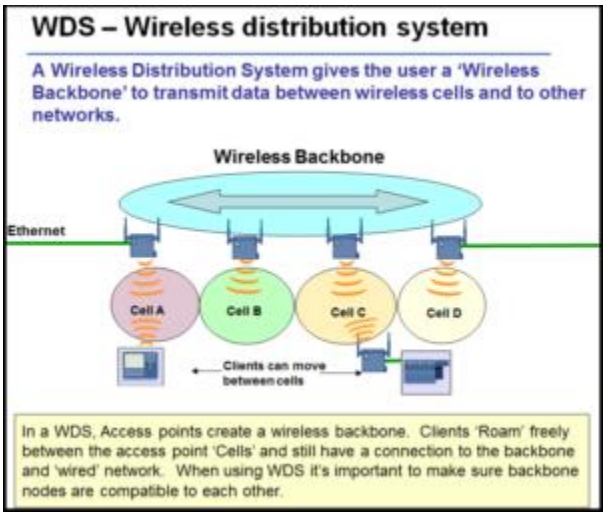
Nota. Estructura de funcionamiento de una red punto a multipunto. Tomado de (Solutech, 2022)

Red sistema distribuido inalámbrico (WDS)

WDS (Sistema Distribuido Inalámbrico o Sistema Distribuido Inalámbrico) permite el uso de una red troncal inalámbrica entre múltiples AP. En este caso, el cliente puede "viajar de ida y vuelta" de una celda a otra y continuar con la comunicación sin inconvenientes. Es adecuado para vehículos guiados automatizados y otros componentes inalámbricos móviles. (Profinetuniversity, 2019)

Figura 24

Red WDS



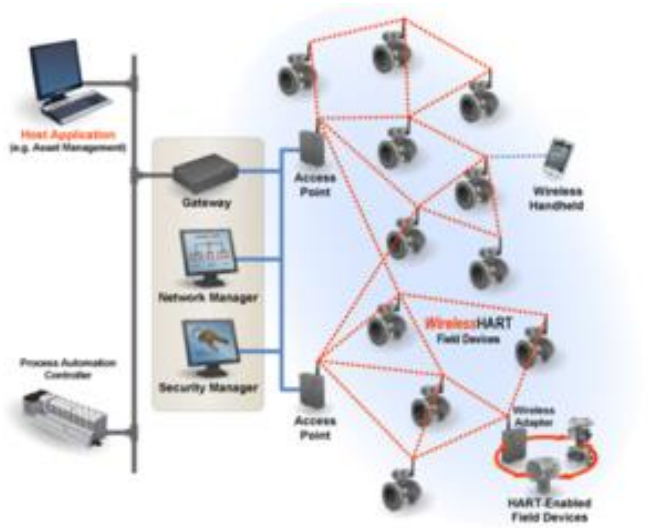
Nota. Estructura de funcionamiento de una red WDS. Tomado de (U.S. Robotics, 2023)

Red Mesh

Las redes inalámbricas de tipo malla son bastante nuevas en la industria, pero importantes para dispositivos de bajo consumo en redes de sensores y procesos. Estas aplicaciones envían datos muy lentamente (segundos). El dispositivo entra en un estado de "reposo" hasta que un cambio de proceso lo despierta.

Figura 25

Red Mesh



Nota. Estructura de funcionamiento de una red Mesh. Tomado de (win, 2020)

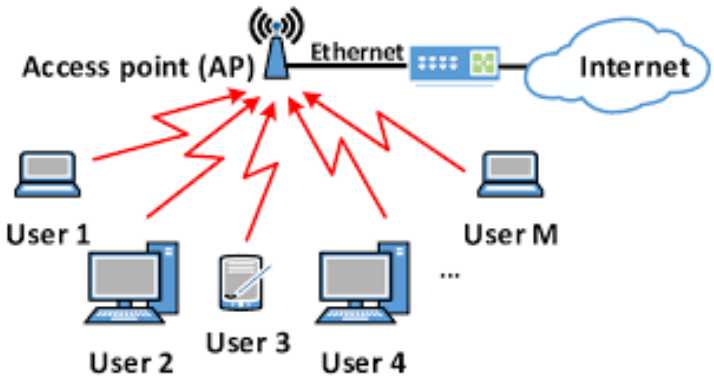
Equipos de telecomunicaciones usados en redes inalámbricas

Punto de acceso o Access point

Un dispositivo que realiza la función de un amplificador de señal y permite la conexión de dispositivos inalámbricos. Funciona de manera similar a un concentrador cableado, manejando un ancho de banda reducido por dispositivo a medida que más dispositivos se comunican a través de él. (Sities Google, 2017)

Figura 26

Uso de Acces Point



Nota. Funcionamiento de un access point. Tomado de (Martinez, 2023)

Router inalámbrico

Son dispositivos utilizados en hogares y pequeñas oficinas para conectarse a Internet y redes corporativas. Los dispositivos más inteligentes no solo actúan como puntos de acceso (con funciones de concentración, impulso y repetición), sino que su función principal es permitir que los dispositivos cableados e inalámbricos de una red accedan a otra red.

A diferencia de un punto de acceso, un enrutador inalámbrico permite las siguientes funciones, que incluyen:

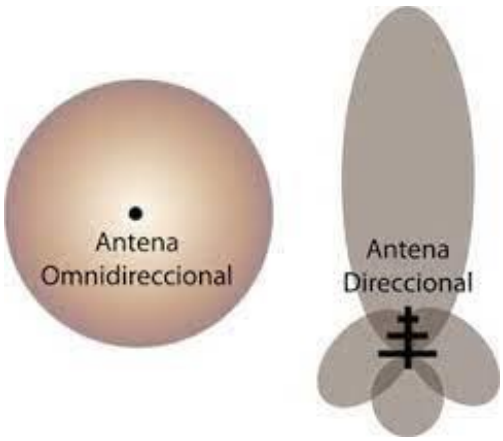
- Permitir o denegar la conexión de dispositivos de usuario final a la red.
- Facilita la conexión de red a dispositivos inalámbricos y cableados.
- Asigna direcciones de red (IP) a los dispositivos que las necesitan.
- Ofrecer funciones de calidad de servicio para mejorar la comunicación.

Antenas

El autor Wifisafe (2019)señala que las antenas son elementos pasivos que no aportan energía a la señal. Una antena redirige la energía recibida del transmisor. Redirigir esta energía tiene el efecto de suministrar más energía en una dirección y menos energía en todas las demás direcciones.

Figura 27

Antenas



Nota. Modelo de antena omnidireccional y antena direccional. Tomado de (Todo sobre redes, 2014)

Seguridad en redes inalámbricas

La seguridad de la red inalámbrica incluye controles de seguridad de capa de red tradicionales aplicados a redes inalámbricas (o WiFi). La seguridad de la red inalámbrica es un tema clave en los escenarios de teletrabajo de hoy. Los administradores enfrentan la necesidad de proteger los recursos corporativos críticos de los ataques. Cuando los empleados acceden a los datos privados de la empresa a través de la red inalámbrica, las personas no autorizadas

pueden comprometer la seguridad si el usuario no asegura la conexión (por ejemplo, al usar una contraseña para obtener acceso).

Mediante el uso de un dispositivo VPN SSL para proteger la capa de acceso de la red inalámbrica, los administradores pueden proteger todo el tráfico de los usuarios en las redes cableadas e inalámbricas, lo que permite el uso de otras alternativas como WEP (Privacidad equivalente por cable). mecanismos. (F5 Glossary, 2019)

Figura 28

Seguridad inalámbrica

Nota. Seguridad inalámbrica. Tomado de (Martinez T. , 2012)

Control de acceso a red inalámbrica

El control de acceso a la red es un concepto de computación en red, un conjunto de protocolos utilizados para definir cómo se protegen los nodos de la red antes de que obtengan acceso a la red.

Control/Filtrado de MACs en WiFi

Una cosa que puede hacer para controlar mejor el acceso a su red WiFi es el filtrado de direcciones MAC. Esta medida no es eficaz para protegerse contra intrusos expertos en redes, pero sigue siendo eficaz en determinados entornos pequeños.

Una dirección MAC es un identificador único asignado a una tarjeta de red (alámbrica o inalámbrica) y consta de seis bloques hexadecimales como 0A:0B: 0C:0D: 0E:0F. Este identificador se puede utilizar para restringir parcial o completamente el acceso a la red inalámbrica, según el punto de acceso o el enrutador. (Redes, 2017)

Autenticación con 802.1X

Otra alternativa al control o filtrado de usuarios es la autenticación en un servidor RADIUS (como NPS para Windows Server) mediante la tecnología de autenticación 802.1X. En este caso, el AP o enrutador debe admitir estas tecnologías.

Esta instalación le permite aprobar o denegar el acceso por pertenencia a un grupo de seguridad, o nombre de usuario y contraseña, en lugar de por dispositivo. También puede establecer si las IP se asignan de acuerdo con un conjunto de reglas, establecer restricciones de acceso por fecha y hora y desconectarse después de un cierto período de tiempo. (Redes, 2017)

Portal Cautivo

También podrá utilizar portales cautivos, sin que ello impida necesariamente el uso de alguna de las medidas anteriores. Un Portal cautivo es una modalidad de instalación de WiFi inalámbrico que permite compartir Internet controlando y regulando fácilmente lo que los usuarios pueden y no pueden hacer y por cuánto tiempo. Este tipo de instalación es muy común en cines, centros comerciales o comedores. (Redes, 2017)

EAP

El Protocolo de autenticación extensible (EAP) es un protocolo de autenticación flexible utilizado por el estándar de control de acceso IEEE 802.1X en LAN. Este protocolo proporciona un entorno en el que las redes inalámbricas pueden elegir un método de autenticación particular.

Existen diferentes variantes de EAP:

- **EAP-MD5:** esta es una versión menos segura del protocolo EAP que usa un nombre de usuario y una contraseña para la autenticación, usando un hash MD5 de la contraseña para la autenticación. Debido a que no verifica la identidad del servidor, es vulnerable a los ataques de intermediarios.
- **EAP-LEAP:** Este es el sistema EAP propietario de Cisco. Al igual que la versión MD5, utiliza un nombre de usuario y una contraseña para la autenticación. Utiliza un servidor RADIUS (explicado en una sección posterior) como servidor de autenticación. Utiliza la autenticación mutua para evitar ataques de persona a persona en primera instancia.
- **EAP-TLS:** utiliza certificados X.509 para usuarios y servidores para la autenticación mutua y el cifrado de las comunicaciones. Este sistema permite la autenticación con un nivel de seguridad muy alto, pero requiere que todos los usuarios generen certificados, lo que puede ser un inconveniente para las organizaciones pequeñas.
- **EAP-TTLS/PEAP:** En estas versiones, el usuario ya no necesita el certificado requerido para la versión TTLS. El servidor se identifica mediante su certificado y el usuario se identifica mediante el servidor RADIUS mediante un nombre de usuario y una contraseña. (De Alfonso, Caballer, & Hernandez, 2005)

Kerberos

Kerberos es un protocolo de seguridad desarrollado en el Instituto Tecnológico de Massachusetts (MIT) para autenticar usuarios y clientes en una red y distribuir claves de cifrado de forma segura. Permite que los dispositivos que se comunican en la red demuestren su identidad sin permitir que se suplanten. También proporciona funciones de integridad de datos (detección de modificaciones) y seguridad de datos (para evitar lecturas no autorizadas) utilizando sistemas de encriptación como DES. Kerberos funciona proporcionando a los actores (usuarios o servicios) "boletos" digitales que pueden usar para identificarse en la red y sirven como claves de cifrado para una comunicación segura. (De Alfonso, Caballer, & Hernandez, 2005)

Firewall

Un cortafuegos o cortafuegos es un dispositivo de hardware o software que actúa como barrera entre redes, permitiendo o denegando la transmisión de una red a otra dependiendo del tipo de conexión que se realice y de las políticas de seguridad vigentes. Estos tipos de dispositivos le permiten configurar los tipos de dispositivos que pueden conectarse a dispositivos en la red que protegen, los protocolos de comunicación que pueden usar para hacerlo, etc. En cambio, se usan para restringir el acceso externo a las computadoras en la red que protegen. En ambos casos, se define un conjunto de reglas que representa la política de seguridad de la red.

Tipos de seguridad en redes inalámbricas

WEP

Wired Equivalent Privacy (WEP) es una tecnología de encriptación de datos responsable de encriptar cada paquete de datos 802.11 antes de enviarlo usando el algoritmo de encriptación RC4. El algoritmo puede utilizar claves de entre 40 y 128 bits, lo que aumenta la seguridad con claves más grandes. WEP no proporciona un mecanismo de control de claves. Todos los cambios deben realizarse manualmente en cada dispositivo inalámbrico. Se ha descubierto que la tecnología tiene varias vulnerabilidades que permiten descubrir dichas claves. Por ello, se han desarrollado nuevas tecnologías (WPA, WPA2) basadas en WEP para solucionar sus problemas de seguridad. WEP es una forma fácil de evitar el acceso no autorizado a nuestra red inalámbrica, pero no es suficiente cuando se necesitan medidas de seguridad mínimas. (De Alfonso, Caballer, & Hernandez, 2005)

WPA

El acceso protegido Wi-Fi (WPA) parece superar las limitaciones de seguridad de WEP, lo que garantiza la compatibilidad con los equipos existentes. WPA es un subconjunto de la especificación IEEE 802.11i, un estándar de seguridad para redes Wi-Fi que apareció como una medida provisional antes de que el estándar 802.11i estuviera listo (WPA apareció en abril de 2003, mientras que el estándar 802.11i completo se aprobó en junio de 2003, 2004).

Las funciones principales son:

- Utilice el Protocolo de integridad de clave temporal (TKIP) para evitar la reutilización de claves (una de las vulnerabilidades de WEP)
- Comprobar la integridad de los paquetes de datos transmitidos (Message Integrity Check o MIC) para evitar errores de transmisión o manipulación de datos.

Viene en dos versiones: una versión personal que controla el acceso mediante una contraseña llamada clave precompartida (PSK) y una versión empresarial que brinda un mayor nivel de seguridad mediante claves de sesión dinámicas y autenticación de usuario mediante el protocolo 802.1X EAP. Al igual que su predecesor, WEP utiliza el algoritmo de encriptación RC4 con una clave de 128 bits. (De Alfonso, Caballer, & Hernandez, 2005)

WPA2

Basado en su antecesor WPA, con la misma funcionalidad, pero con una capa adicional de seguridad, implementa completamente la especificación IEEE 802.11i. Una de las mejoras más importantes es cambiar el algoritmo de cifrado utilizado por WEP y WPA (RC4) a un algoritmo de cifrado de mayor nivel conocido como Estándar de cifrado avanzado (AES). Al igual que su predecesor, WPA viene en dos versiones: una versión personal que utiliza una contraseña denominada clave precompartida (PSK) para controlar el acceso y una versión comercial que utiliza el protocolo 802.1X EAP para la autenticación de usuarios. red privada virtual. (De Alfonso, Caballer, & Hernandez, 2005)

VPN

Una red privada virtual (VPN) es una extensión de una red privada al compartir un enlace a través de una red pública, como Internet o una red inalámbrica. Una VPN permite enviar datos entre dos puntos de una red compartida o pública, simulando una conexión punto a punto. Para simular un enlace privado, los datos transmitidos se cifrarán para evitar que se lean los paquetes potencialmente interceptados. La parte de la conexión a través de la cual fluyen los datos encapsulados se denomina túnel. (De Alfonso, Caballer, & Hernandez, 2005)

NVR

Dispositivo de grabación de video digital que es utilizado conjunto con cámaras IP permitiendo así, grabar y almacenar videos e imágenes, es instalado en una computadora.

Es el encargado de recibir las señales de video de las cámaras IP que están conectadas a la misma red, para poder comprimirlas y almacenarlas en el disco duro.

La diferencia entre nvr con dvr la explica (Sosio, 2022) señalando que “Un NVR es muy similar a un DVR, la diferencia es que el DVR digitaliza, graba y administra imágenes enviadas desde cámaras de seguridad analógicas, en cambio un NVR, graba y administra imágenes ya digitales las cuales son enviadas desde las cámaras IP a través de una red.”

Figura 29

NVR HikVision DS-7608NI-K1/8P

Nota. NVR HikVision DS-7608NI-K1/8P. Tomado de (Tecnit, 2019)

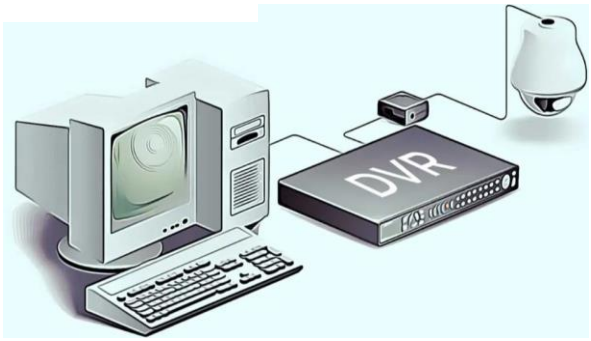
DVR

Dispositivo de grabación de video digital registrando imágenes y video, tiene grabación en tiempo real y grabación por detección de movimiento.

Lo que va almacenando lo guarda en un disco duro, para que así el usuario pueda revisar videos anteriores, filtrado por fechas y número de cámara deseada. (Argüello, 2023)

Figura 30

DVR



Nota. Conexión y funcionamiento del DVR. Tomado de (Argüello, 2023)

Servidor

Sistema o programa el cual nos puede brindar servicios a diferentes dispositivos en la misma red. Su función es almacenar, compartir archivos, conceder permisos, realizar tareas específicas en la red. (IONOS, 2020)

Hay dos conceptos de servidores:

Servidor (Software)

Programa que brinda un servicio que los demás dispositivos los cuales serán denominados clientes para que puedan ser usados a través de una red. Actúa en cliente-servidor. (IONOS, 2020)

Servidor (Hardware)

Equipo físico en la red, su servicio es almacenar, procesar, controlar y gestionar datos. Son más potentes que una computadora normal, funciona con uno o más softwares para su ejecución, son denominados “host”. (IONOS, 2020)

Servidor de correo electrónico

Permite la recepción, envío y reenvío de correos electrónicos, entre las características avanzadas se encuentra el filtrado de spam, encriptación de correo y sincronización con celulares, son de uso interno o externo dependiendo de lo que requiera la institución. (IONOS, 2020)

Tipos de servidores

Servidor Web

Funciona para alijar y entregar contenido en una web mediante una red de internet, recibe solicitudes de clientes las cuales el servidor web las procesa y las devuelve en forma de páginas web, imágenes o videos. Usan protocolos HTTP o HTTPS, para tener interacción con los clientes. (IONOS, 2020)

Servidor de archivos

Almacena datos accedidos por parte de clientes en la red. Permitiendo a los usuarios subir, descargar o compartir datos en la red. (IONOS, 2020)

Servidor de juegos

Software creados para juegos multijugador online, gestionan los datos de los juegos y permiten las interacción con el mundo virtual. (IONOS, 2020) explica que “La base de hardware de un servidor de juegos se encuentra en el centro de datos de los proveedores especializados o está disponible en una red doméstica local.”

Servidor Proxy

Su función es la de ser interfaz de la comunicación en una red informática, filtra comunicación, controla el ancho de banda, guarda datos por un cierto tiempo, recibe solicitudes en la red y las transmite a través de su propia dirección IP. (IONOS, 2020)

Servidor DNS

Traducen los nombres de host en su correspondiente dirección IP, almacenan información sobre los nombres de los dominios y dirección IP en sus bases de datos convirtiéndose así en un directorio para la red. (IONOS, 2020)

Sistema Operativo

Un sistema operativo es un conjunto de programas que nos permiten administrar la memoria, los discos, los medios de almacenamiento y los diversos periféricos o recursos de nuestras computadoras, como teclados, ratones, impresoras, tarjetas de red, etc.

Los dispositivos periféricos utilizan controladores o controladores desarrollados por cada fabricante de computadoras. Encontramos diferentes versiones de diferentes sistemas operativos como Windows, Linux, MAS OS. Los teléfonos y tabletas también tienen sistemas operativos. (Desarrollarinclusion, 2017)

Tipos de sistemas operativos

Sistema operativo por lotes

Una característica de este tipo de sistema operativo es que se encarga de ejecutar procesos sin requerir que el usuario del sistema interactúe directamente con la computadora. El sistema tiene un operador que agrupa y agrupa los trabajos en función de la similitud. Es un

sistema multiusuario con un bajo nivel de inactividad. Se utiliza principalmente para procesar trabajos grandes y se puede dividir en varios lotes. Este tipo de sistema se utilizó por primera vez en determinados contextos empresariales para actividades como la administración de nóminas o la generación de extractos bancarios. (Universitat Carlemany, 2022)

Sistema operativo multitarea o de tiempo compartido

Este sistema operativo permite que un usuario o varios usuarios realicen diferentes tareas al mismo tiempo. Entonces, cuando el sistema completa una tarea para uno o más usuarios, pasa a la siguiente tarea pendiente. Un ejemplo de tal sistema operativo es Unix.

Sistema operativo en tiempo real

Un sistema operativo en tiempo real es un sistema que deja muy poco tiempo para procesar y responder a la entrada. Se utilizan en sistemas con requisitos de tiempo de respuesta muy elevados y muy críticos. Entre otros, se utilizan en robótica, sistemas encargados del control del tráfico aéreo o sistemas industriales. También en cierto tipo de experimentos científicos. (Universitat Carlemany, 2022)

Sistemas distribuidos

Trabajan con varios dispositivos al mismo tiempo, cada uno con su propio procesador para proporcionar a los usuarios una potente potencia informática. Los cálculos y el procesamiento también se pueden realizar muy rápidamente. Estos son sistemas desarrollados relativamente recientemente que brindan a sus usuarios acceso en cualquier momento a archivos y programas que no están instalados o almacenados en la computadora que están usando, sino en otras computadoras conectadas al mismo sistema. el sistema que utilizan. Esto significa que tiene capacidades de acceso remoto en la misma red.

Sistema operativo de red

Estos son los que se ejecutan y se administran en el servidor. Estos sistemas operativos se pueden utilizar para gestionar diversas funciones de red, así como usuarios, grupos o datos. También la seguridad de todos los equipos conectados a la red local o privada y conectados a este servidor. (Universitat Carlemany, 2022)

Sistemas operativos móviles

Están creados y desarrollados para dispositivos móviles, principalmente teléfonos y tabletas, pero también relojes inteligentes. Como hemos visto, los más conocidos son Android y iOS, pero existen otros sistemas operativos para smartwatch, como webOS y watchOS.

MS/DOS

El sistema operativo DOS, cuyo nombre completo es Disk Operating System o MS/DOS, fue desarrollado por Microsoft para IBM PC en 1981. MS/DOS puede administrar disquetes y archivos, memoria y dispositivos de entrada y salida. Está controlado por mando.

Microsoft Windows

El sistema operativo más famoso es Windows, que Microsoft utiliza ampliamente en las computadoras personales. Microsoft Windows es una familia de sistemas operativos gráficos desarrollados a lo largo de los años. (Toda materia, 2019)

Mac OS

El sistema operativo Macintosh de Apple para computadoras personales y portátiles MAC OS se basa en una interfaz gráfica de usuario y se basa en el núcleo UNIX

Unix

El sistema operativo UNIX fue desarrollado en Bell Labs a principios de la década de 1970 por Ken Thompson, Dennis Ritchie y otros. Es un sistema multiprogramada y multiusuario escrito en el lenguaje de programación C y se utiliza en todo, desde microcomputadoras hasta supercomputadoras. Además, es la base para otros sistemas operativos como MAC OS y Solaris. (Toda materia, 2019)

Linux

Linux es un sistema operativo gratuito de dominio público desarrollado originalmente por Linus Torvalds. En este sistema, los usuarios pueden elegir sus administradores de ventanas preferidos, como KDE y Gnome.

IOS

El sistema operativo iOS pertenece a la empresa Apple Macintosh y se utiliza en sus sistemas móviles: iPhone y iPad. Fue creado en 2007 a partir de MAC OS/X.

Android

El sistema operativo Android está diseñado principalmente para teléfonos inteligentes y tabletas. Fue desarrollado por Google y Open Handset Alliance en 2007 en el kernel de Linux. Debido al uso generalizado de los teléfonos inteligentes, Android es el sistema operativo más utilizado en la actualidad. (Toda materia, 2019)

HongMeng OS/HarmonyOS

La empresa china Huawei ha desarrollado un sistema operativo llamado Hongmeng OS (en chino) o HarmonyOS. Inicialmente, la empresa utilizaba los sistemas operativos de Microsoft.

IBM OS/360

El sistema OS/360 se usó en la serie de computadoras IBM System/360 en la década de 1960.

MVS

IBM introdujo el sistema operativo Múltiple Virtual Storage (MVS) en 1974 para sus computadoras System/370 y System/390. MVS es un sistema multiprogramado y multiprocesador.

VM (Virtual Machine)

Un sistema operativo VM (máquina virtual) hace que una computadora parezca varias computadoras reales. Las máquinas virtuales pueden ejecutar diferentes sistemas operativos y se utilizan principalmente para probar sistemas operativos. (Toda materia, 2019)

Open VMS

OpenVMS es la última versión del sistema operativo VMS (Sistema de memoria virtual) desarrollado para minicomputadoras VAX.

Solaris

El sistema operativo Solaris desarrollado por Sun Microsystems pertenece a la familia de sistemas operativos UNIX. Actualmente se llama Oracle Solaris. Se describe como un sistema multiprocesador simétrico. (Toda materia, 2019)

Ubuntu

Distribución de Linux basada en Debian, es de código abierto, se lo puede utilizar en computadoras, servidores y celulares.

Se enfoca en la seguridad e igual en la privacidad de los usuarios, tiene adaptabilidad para cada requerimiento, su interfaz es intuitiva lo que la hace muy accesible y fácil de usar.

"Cada seis meses se lanza una nueva versión que contengan nuevas funcionalidades, actualizaciones de seguridad u optimizaciones del sistema." (Rodriguez, 2020)

Requisitos para instalar Ubuntu

- Procesador de 2GHz
- Memoria Ram de al menos 4 Gb
- 25 Gb de disco duro
- Lector DVD o una usb para su instalación
- Tarjeta gráfica de 1024x768 de resolución

Figura 31

Interfaz Ubuntu

Nota. Interfaz gráfica de escritorio de sistema operativo Ubuntu. Tomado de (Darkcrizt, 2021)

Radius

Es un servidor de autenticación, autorización y contabilidad AAA, usado para la gestión de acceso de usuarios en diferentes empresas, instituciones, centros comerciales o áreas en las que solo personal autorizado tendría acceso a red de internet, vpn o PPPoE.

Es compatible con base de datos al igual que directorios para que pueda almacenar configuraciones e información de usuarios.

Como dice (Acero, 2018) “Su funcionamiento tiene similitud con lo que se conoce como AAA, Authentication, Authorization and Accounting (Autenticación, autorización y registro)”

Autenticación

Es el encargado de realizar la debida verificación de identidad de un dispositivo o una persona, dando como pregunta (¿Quién eres?). Se usa un usuario y su respectiva contraseña para poder validar la autenticación. (Acero, 2018)

Autorización

Permisos cuales se otorgará al usuario que contenga sea autenticado en el sistema, emitiendo la pregunta (¿Qué permisos se te están permitidos?). Los permisos o reglas las impondrá el administrador dependiendo del tipo de usuario según su perfil, permitiendo acciones asignadas que pueda realizar cada usuario. (Acero, 2018)

Registro

Dado autenticación y autorización al usuario, se procederá a verificar que acciones está realizando con los recursos que se la ha asignado, controlando así la información que hay entre usuario y el servidor, almacenando todos los datos en una base de datos. (Acero, 2018)

Free Radius

- Uno de los servidores Radius más completo que existe hoy en día, se lo puede implementar en pequeños sistemas de pocos usuarios, hasta grandes sistemas de varios usuarios.
- Incluye MySQL, Oracle, PostgreSQL, para base de datos.
- Soporte para poder limitar el número de usuarios.
- Permite el uso de sentencias (#Include) en sus ficheros.

Capítulo III

Desarrollo

Finalizada la parte de investigación bibliográfica, se da paso a realizar el debido proceso para determinar la importancia de los equipos de seguridad de video vigilancia IP como de seguridad en red, por lo cual se recurrió a una socialización con personal de la institución educativa para que nos puedan informar e indicar los lugares donde requieren un incremento de vigilancia para la seguridad estudiantil. Para de esta forma poder adquirir información concreta para la implementación de los equipos.

Figura 32

Colegio Particular Israel N°2

Nota. La figura representa la entrada a el Colegio Particular Israel N°2

Completada la socialización y revisión conjuntamente con el personal encargado de la institución, inicializamos con la comparación de equipos a implementar, detallando los

diferentes componentes técnicos que ofrecen en el mercado referente a los sistemas de seguridad, tomando en cuenta que la institución requiere equipos de seguridad actuales para una mejor durabilidad en su sistema y así beneficiarse para futuras implementaciones en la institución.

Por lo tanto, se detalla los componentes técnicos investigados correspondientes a el equipo NVR cual será parte del sistema de video vigilancia IP, la función del equipo será grabar, gestionar, transmitir imágenes y videos a través de la red, aprobando que el equipo a seleccionar sea el que ofrezca un funcionamiento óptimo y eficiente en el sistema de seguridad a implementar.

Se trabajará con el NVR DHI-NVR1104HS-P-S3

Tabla 5

Características del NVR

GRABADOR NVR	
Modelo	DHI-NVR1104HS-P-S3
Canales de Acceso	4 canales
Capacidad de decodificación	1–canal@8MP(30FPS) o 1–canal@5MP(30FPS) o 2–canal@4MP(30FPS) o 2–canal@3MP(30FPS) o 4–canal@1080P(30FPS)

GRABADOR NVR	
Ancho de banda de la red	80 Mbps para acceso, 80 Mbps para almacenamiento y 60 Mbps para reenvío.
Resolución	8MP/5MP/4MP/3MP/1080P/720P/D1/CIF
Compresión de Video	H.265+ inteligente/H.265/H.264+ inteligente/H.264
Audio	PCM/G711A/G711U/G726/AAC
Protocolo de red	HTTP, HTTPS, TCP/IP, IPv4, IPv6, RTSP, UDP, NTP, DHCP, DNS, P2P
Almacenamiento	Disco duro local y red
Estándar de acceso	ONVIF (perfil T/perfil S/perfil G), CGI, SDK

Nota. La tabla muestra las características que contiene el NVR que será usado para el sistema de video vigilancia.

Escogido el NVR a usar, procederemos a buscar requerimientos técnicos óptimos y compatibles con el equipo de grabación de las cámaras IP, las cuales serán implementadas en el sistema de video vigilancia del Colegio Particular Israel N°2.

Se trabajará con las cámaras IP Dahua DH-IPC-HFW1431S1N

Tabla 6

Características de cámaras IP

CAMARA IP	
CARACTERÍSTICAS	DH-IPC-HFW1431S1N
Modelo	Bala
Sensor de Imagen	CMOS progresivo de 1/3” y 4 megapíxeles
Pixeles Efectivos	2688 (H) x 1520 (V)
ROM	128 MB
RAM	128 MB
Sistema de escaneo	Progresivo
Mínima Iluminación	0.03 Lux @ F2.0
Distancia IR	30 m (98,4 pies)
Rango de giro / inclinación / rotación	Horizontal: 0 ° –360 ° Vertical: 0 ° –90 °

CAMARA IP	
	Rotación: 0 ° –360 °
Tipo de lente	Fijo
Longitud focal	2,8 milímetros 3,6 milímetros
Campo de visión	Diagonal: 111 ° 3,6 mm: Horizontal: 81 ° Vertical: 44 ° Diagonal: 95 °
Compresión de video	H.265; H.264; H.264B; MJPEG
Códec inteligente	Si
Velocidad de fotogramas de vídeo	Convencional: 2688 × 1520 (1 fps – 20 fps) 2560 × 1440 (1

CAMARA IP	
	fps – 25/30 fps) Transmisión secundaria: 704 × 576 (1 fps – 20/25 fps) 704 × 480 (1 fps – 20/30 fps)
Control de tasa de bits	CBR; VBR
Bitrate de vídeo	H.264: 32 Kbps – 6144 Kbps H.265: 12 Kbps – 6144 Kbps
WDR	120 dB
Red	RJ-45 (10/100 Base-T)
Protocolo	HTTP; TCP; ARP; RTSP; RTP; UDP; RTCP; SMTP; FTP; DHCP; DNS; DDNS; PPPoE; IPv4 / v6; QoS; UPnP; NTP; RTMP; Multidifusión; HTTPS; SFTP; 802.1x; ICMP; IGMP

CAMARA IP	
Teléfono móvil	IOS; Androide
Certificaciones	CE-LVD: EN60950-1 CE-EMC: Directiva de compatibilidad electromagnética 2014/30 / UE FCC: 47 CFR FCC Parte 15, Subparte B
Protección de ingreso	IP67

Nota. La tabla indica las características de las cámaras a implementar en el sistema de video vigilancia.

Finalizada la selección de equipos del sistema de video vigilancia, continuaremos con la selección de equipos con los cuales trabajaremos en el control de acceso, escogeremos diferentes equipos y los diferenciaremos entre ellos para ver sus diferentes funcionalidades y escoger el que sea más accesible para realizar el control de acceso. Tomando en cuenta su precio y características se ha escogido el equipo TL-R940N dispositivo más económico y con de igual manera tiene un sistema de seguridad para el control de acceso, por lo que este dispositivo será muy útil en la implementación.

Tabla 7

Características del access point

ACCESS POINT	
CARACTERÍSTICAS INALÁMBRICO	
Router inalámbrico TL-WR940N 450Mbps	
Estándares Inalámbricos	WiFi 4 IEEE 802.11n/b/g 2,4 GHz
Velocidades WiFi	N450 2,4 GHz: 450Mbps (802.11n)
Rango WiFi	Antenas fijas 3× Múltiples antenas forman un conjunto de refuerzo de señal para cubrir más direcciones y áreas más grandes
Puertos Ethernet	1 puerto WAN de 10/100 Mbps 4 puertos LAN de 10/100 Mbps
Procesador	CPU de un solo núcleo

ACCESS POINT	
Botones	Botón WPS/Wi-Fi Botón de encendido/apagado Botón de reinicio
Poder	9 V ⎓ 0,6 A
Cifrado WiFi	WEP WPA WPA2 WPA/WPA2-Empresa (802.1x)
Seguridad de la red	SPI Firewall Control de acceso Enlace de IP y MAC Gateway de capa de aplicación
Protocolos	IPv4 IPv6
Tipos de WAN	IP dinámica IP estática PPPoE

ACCESS POINT	
Potencia de transmisión WiFi	PPTP L2TP CE: <20 dBm (2,4 GHz) FCC: <30 dBm
Sensibilidad de recepción WiFi	450M: -68dBm@10% POR 216M: -70dBm@10% POR 130M: -78dBm@10% POR 54M: -74dBm@10% POR 11M: -85dBm@8% POR 6M: -88dBm@10% POR 1M: -93dBm@8% POR

Nota. La tabla indica características del access point a implementar.

Seleccionado el equipo que será usado para el control de acceso, ahora definiremos que sistema operativo será el ideal a usar para poder trabajar con el servidor free radius para poder emplear usuarios y credenciales de personal autorizado para que puedan acceder a la red, se trabajará con Ubuntu Server versión 20.04 Lts.

Tabla 8

Características del sistema operativo

SISTEMA OPERATIVO	
CARACTERISTICAS	**UBUNTU SERVER**
Versión	22.04 Lts
Fabricante	GNU Linux
Licencia	Libre
Requerimiento para arrancar el sistema operativo	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-+)
Arquitecturas soportadas	X86, AMD64, SPARC, IA-64, HP PA-RISC
Medio de instalación	DVD, memoria USB

Nota. La tabla muestra características del sistema operativo a usar.

Finalmente, completada la selección del sistema operativo a usar para el control de acceso mediante un servidor radius, se elige la versión 3.0 del servidor free radius la cual contiene compatibilidad con los recursos de la computadora en la cual será implementada.

Tabla 9

Características de Free Radius

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

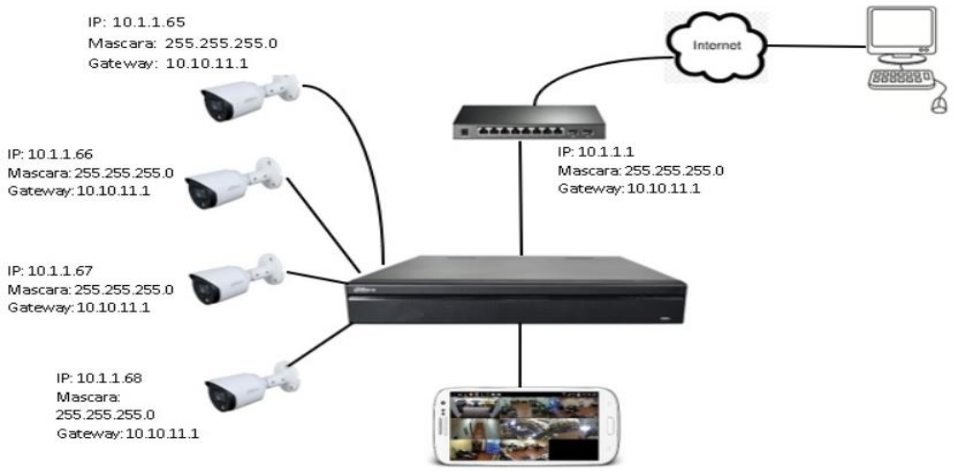
Nota. La tabla muestra características del servidor Free Radius que se ocupara.

Representación Gráfica de la topología del sistema de video vigilancia IP

Concluida la investigación y selección de equipos que nos permitirán ejecutar el proyecto, se representa mediante un diagrama la topología de cómo funcionará el sistema de video vigilancia con todos los equipos a implementar en el Colegio Particular Israel N°2.

Figura 33

Topología del sistema de video vigilancia



Nota. La figura representa la guía estructural de los equipos a implementar en puntos definidos por la institución.

A su vez, conjunto con personal de la institución Israel N°2 se realizó un recorrido por la institución ubicando las zonas requeridas para ubicar el sistema de video vigilancia, obteniendo un incremento en control de la institución, mejorando su seguridad y de los estudiantes.

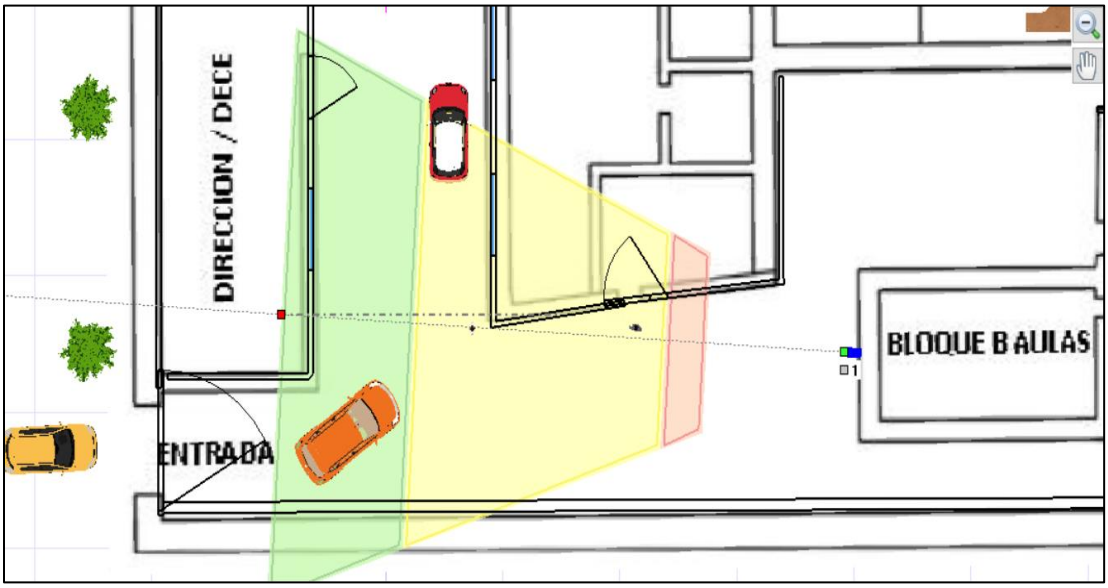
Entrada Principal

Plano 2D

Construcción del plano en 2D de la entrada principal en el programa IP Video System Tool, cuya función es de colocar la cámara de acuerdo a los requerimientos de infraestructura, su cobertura, su altura y ángulo de posición. Permitiendo observar quien entra, que automóvil entra, controlando así el acceso principal a la institución.

Figura 34

Plano 2D de entrada principal



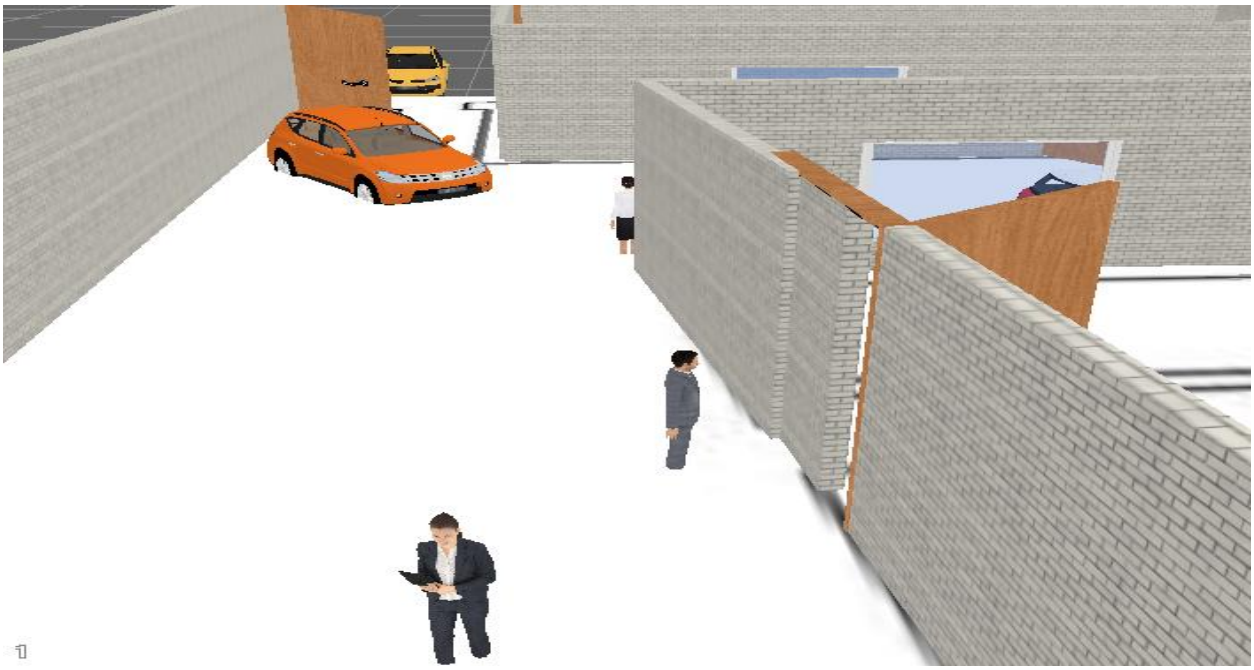
Nota. La figura representa el área que cubre la cámara en la entrada principal.

Visualización 3D

Para lograr una apreciación del área que cubrirá la cámara, usaremos la misma herramienta, pero esta vez la visión de la cámara será en 3D, logrando controlar el ingreso a la institución.

Figura 35

Vista 3D de entrada principal



Nota. La figura muestra en 3D el enfoque que tendrá la cámara en la entrada principal.

Requerimientos para la instalación de la cámara IP

- Localización: Entrada principal
- Altura: 3.5 m
- Resolución de cámara: 4MP
- Alcance: 30 m
- Marca: Dahua
- Modelo: DH-IP-HFW1431S1N
- Tipo: Bala
- Precio: 110

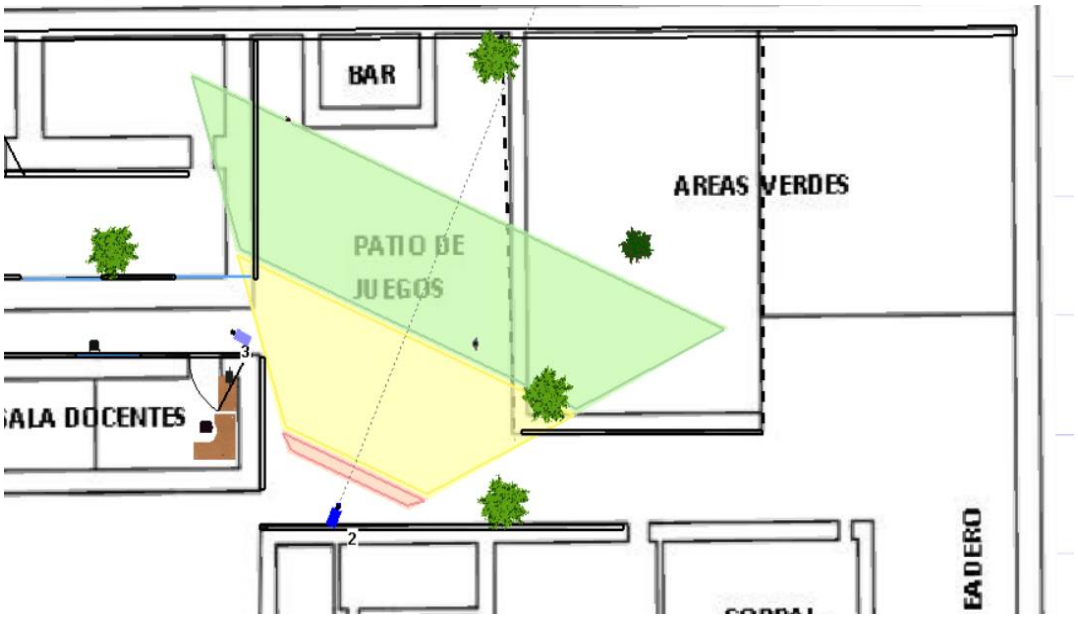
Patio de Juegos

Plano 2D

Construcción del plano en 2D mediante IP Video System Tool, de la zona de patio de juegos, donde se verá parte del bar y áreas verdes de la institución, permitiendo ver la funcionalidad que tendrá la cámara de acuerdo a los requerimientos de infraestructura, su cobertura, su altura y ángulo de posición. Permitiendo observar que actividades están realizando en dichas áreas y quien circula por estas zonas.

Figura 36

Plano 2D de zona de patio de juegos



Nota. La figura muestra el área que tendrá cobertura por la cámara IP en el patio de juegos.

Visualización 3D

Para observar la cobertura que otorgará la cámara, usamos la misma herramienta, pero esta vez en visión 3D, lo cual nos permitirá observar la cobertura y alcance que tendrá nuestra cámara en tiempo real, permitiendo controlar quien transita por esta área.

Figura 37

Vista 3D de la zona de Patio de juegos

Nota. La figura muestra el enfoque y alcance que tendrá la cámara colocada en el patio de juegos.

Requerimientos para la instalación de la cámara IP

- Localización: Patio de Juegos
- Altura: 4

- Resolución de cámara: 4MP
- Alcance: 30 m
- Marca: Dahua
- Modelo: DH-IP-HFW1431S1N
- Tipo: Bala
- Precio: 110

Aulas Bloque A

Plano 2D

Visualización del plano en 2D mediante IP Video System Tool, del bloque de aulas A, permitiendo ver la funcionalidad que tendrá la cámara de acuerdo a los requerimientos de infraestructura, su cobertura, su altura y ángulo de posición. Permitiendo monitorear si los estudiantes salen de las aulas, quien transita por el pasillo y actuar ante accidentes con rapidez.

Figura 38

Plano 2D de bloque de aulas A

Nota. La figura representa la visualización del plano en 2D de la cámara a implementar en el área de Bloque Aulas A.

Visualización 3D

Para poder apreciar cómo será el enfoque y alcance que tendrá la cámara a implementar, usaremos la vista 3D de la herramienta que usamos para realizar el plano 2D, permitiendo controlar quien transita por el pasillo y si salen o no los estudiantes de sus aulas.

Figura 39

Visualización 3D de la zona de Aulas Bloque A

Nota. La figura permite observar cómo sería el enfoque de la cámara a implementar en la zona de Aulas Bloque A.

Requerimientos para la instalación de la cámara IP

- Localización: Aulas Bloque A
- Altura: 2
- Resolución de cámara: 4MP
- Alcance: 30 m
- Marca: Dahua
- Modelo: DH-IP-HFW1431S1N
- Tipo: Bala
- Precio: 110

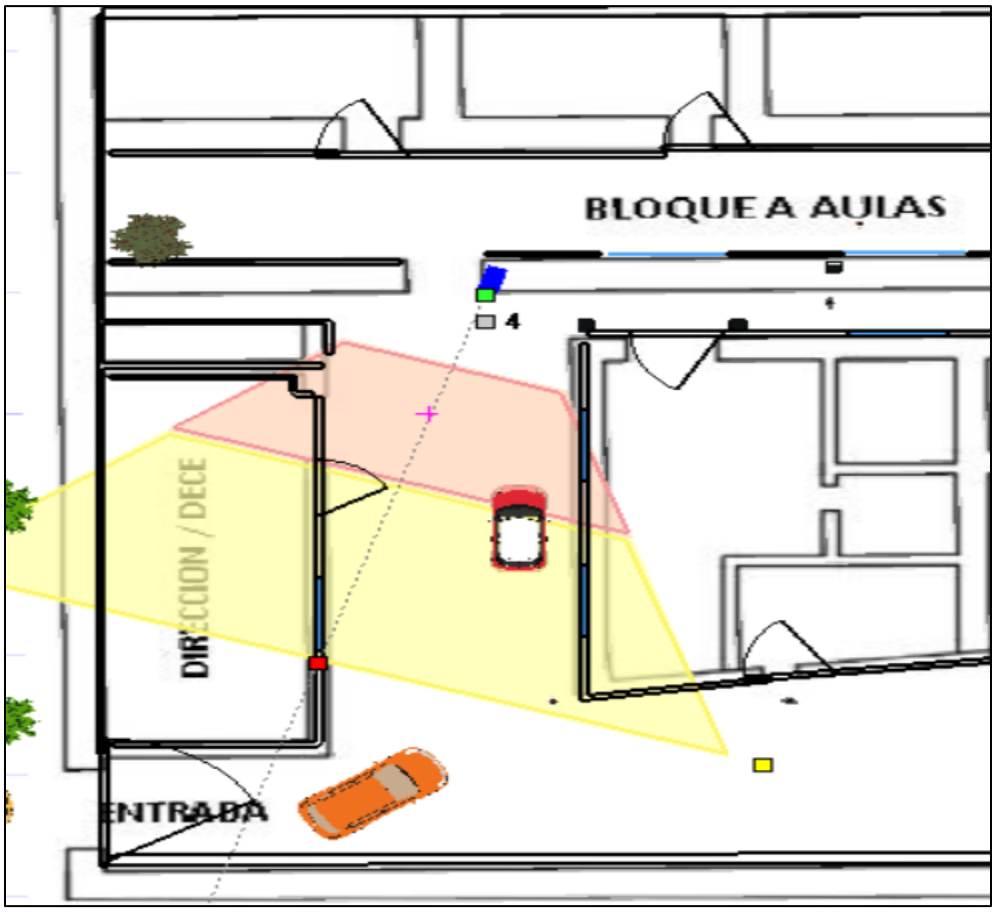
Dirección/DECE

Plano 2D

Para ilustrar de manera gráfica usaremos la herramienta IP Video System Tool, donde se identificará el área de cobertura que se genera por la cámara, ubicar el lugar donde será colocada la cámara, captando el personal que ingrese o salga de la dirección o DECE, así también verificando que automóvil entra y sale.

Figura 40

Plano 2D de la Dirección/DECE



Nota. La figura representa el plano 2D, permitiendo observar donde será la ubicación de la cámara y su zona de cobertura.

Plano 3D

Para visualizar el enfoque que dará la cámara en la zona de dirección, se utilizara la visión 3D, permitiendo así controlar que persona ingresa a las oficinas de dirección de la institución, también aporta la visualización de automóviles que entran a la institución.

Figura 41

Vista 3D de la dirección/DECE

Nota. La figura permite visualizar en 3D lo que enfocará la cámara, permitiendo observar personal que ingresa a la dirección y controlando el ingreso de automóviles a la institución.

Requerimientos para la instalación de la cámara IP

- Localización: Dirección/DECE
- Altura: 2
- Resolución de cámara: 4MP
- Alcance: 30 m
- Marca: Dahua
- Modelo: DH-IP-HFW1431S1N
- Tipo: Bala
- Precio: 110

Implementación y configuración de cámaras IP

Explicada las características de los equipos a usar para el sistema de video vigilancia y su locación, procedemos a implementar las cámaras en los puntos indicados por la institución.

Empezaremos por atornillar la cámara de seguridad y su cableado, al igual que poncharemos el cable categoría 6 ya que la instalación será para exteriores.

Figura 42

Implementación de cámaras IP

Nota. La figura representa como se realiza el cableado y colocación de cámaras IP.

Por consiguiente, se procede a implementar la caja de protección de cada cámara, donde se encontrará la conexión del cable.

Figura 43

Caja de Protección

Nota. La figura muestra la caja de protección que tiene la cámara implementada.

Continuando con la implementación, se coloca seguridad del cable, en este caso se usará canaletas las cuales servirán de protección y guía hasta llegar a conectar cada cámara con el NVR.

Figura 44

Colocación de canaletas para el cableado de cámaras

Nota. La figura representa la colocación de canaletas para guía del cable.

Configuración de grabador y Cámaras IP

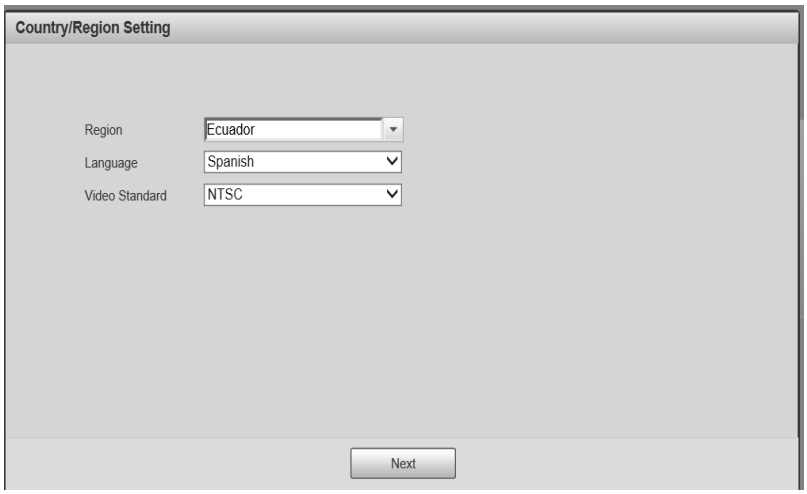
Terminado con los diseños de las áreas de cobertura tanto de las cámaras IP como del punto de acceso y terminado con la instalación de las cámaras IP, se ha realizado la configuración de todos los grupos ubicados en los diferentes ángulos.

Comenzamos por encender la cámara y conectarla a la red local con un cable de red y acceder a ella a través de un sitio web con la IP 192.168.1.108 ya que esta es la dirección IP predeterminada del dispositivo para que podamos inicializar el dispositivo. Si la red está en un área diferente, usamos ConfigTool para cambiar la configuración de red de la cámara.

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

Figura 45

Ajuste de Región y País



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 46

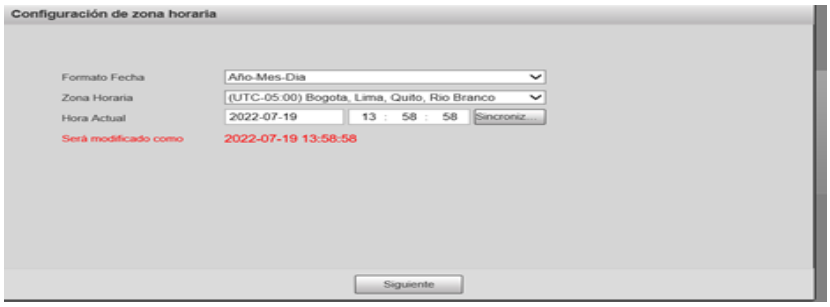
Acuerdo de licencia de software y políticas de privacidad

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, seleccionamos el formato de fecha (Año-Mes-Día), seleccionamos el sector horario adecuado y al finalizar presionamos sincronizar para obtener la hora de hoy, luego de realizar estos pasos procedemos a presionar siguiente como se muestra en la imagen.

Figura 47

Configuración de Zona horaria

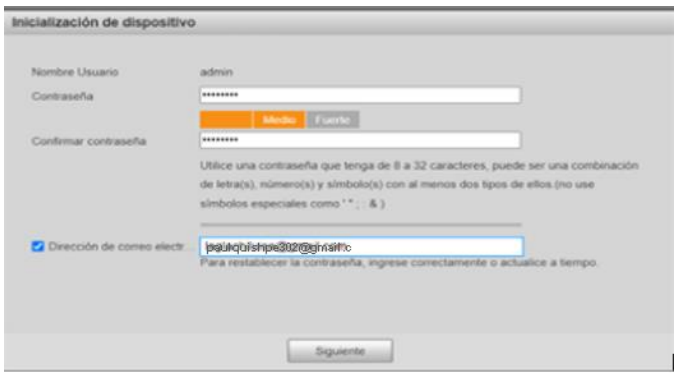


Nota. Configuración de la zona horaria de acuerdo al país en que se encuentra.

Seguimos con la parte de inicialización que nos pide crear la contraseña del cliente administrador, hemos creado una contraseña que debe tener mínimo 8 letras y números y debemos mezclar caracteres, finalmente se encuentra correspondencia electrónica que nos ayudará a recuperar la contraseña en caso de que se olvide. Una vez hecho esto pasamos a la siguiente ventana.

Figura 48

Configuración usuario y contraseña



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

Establecemos parámetros de red en el menú Network. Colocamos en DHCP y nos proporcionara automáticamente la dirección IP del NVR y de igual manera para las cámaras IP.

Tabla 10

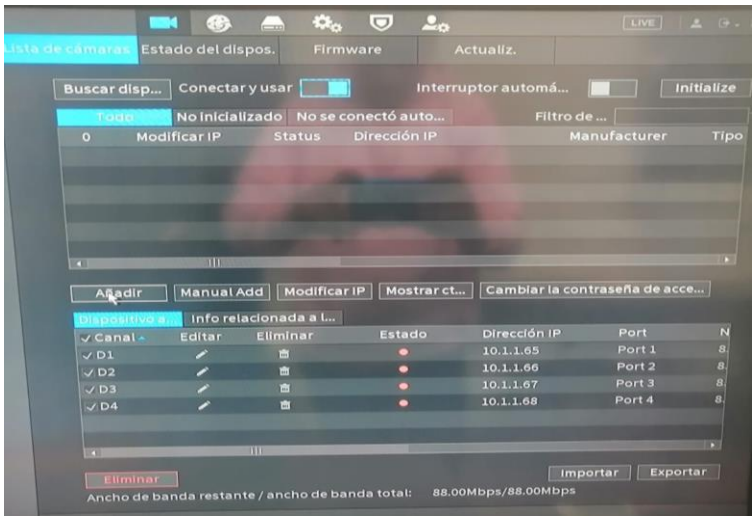
IP designada para cada cámara

Nombre cámaras	IP	Mascara de Red	Gateway
Cámara 1	10.1.1.65	255.255.255.0	10.1.1.2
Cámara 2	10.1.1.66	255.255.255.0	10.1.1.2
Cámara 3	10.1.1.67	255.255.255.0	10.1.1.2
Cámara 4	10.1.1.68	255.255.255.0	10.1.1.2

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

Figura 49

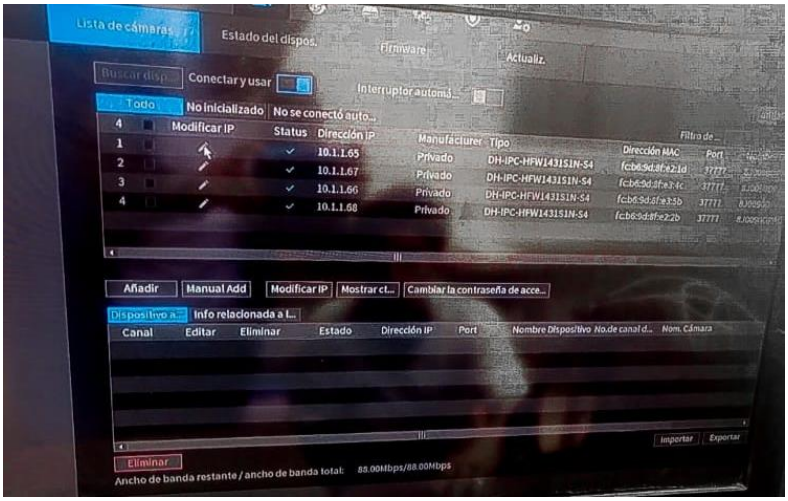
Búsqueda de cámaras en la red



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

Figura 50

Inicialización de las cámaras

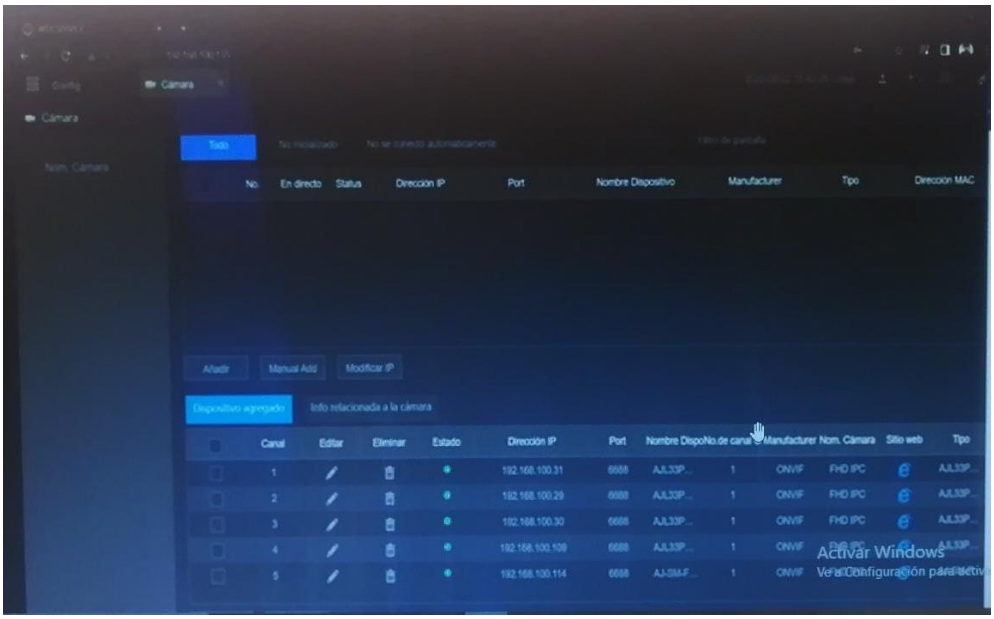


Nota. Se podrán añadir las cámaras después de colocar su contraseña.

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 51

Cámaras en estado de funcionamiento



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

Figura 52

Visualización de las cámaras en los puntos estratégicos

Nota. Visualización de las cámaras que se agregadas al NVR en la red del Colegio Particular Israel N.º 2.

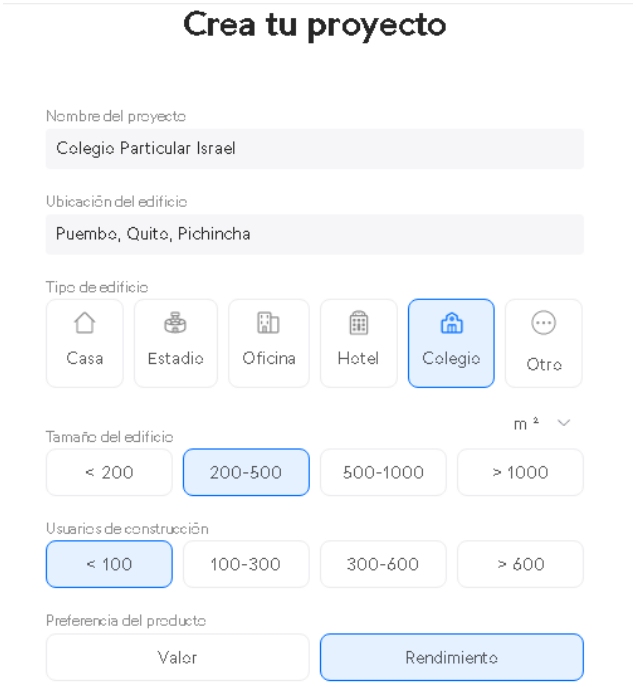
Diseño de la zona de cobertura del AP

Después de seleccionar los accesorios para la seguridad inalámbrica, iniciamos la simulación utilizando la página web de Unifi Design Center. Esta página le permite cargar planos para entidades que diseñan redes inalámbricas. Con este equipo, existe una iniciativa de cobertura que se puede obtener al ubicar APs para ayudar a posicionar de manera óptima a su equipo.

Para visualizar el área de cobertura del punto de acceso se procedió a crear un nuevo plano en el cual colocamos las especificaciones, en esta situación el nombre del plano será Colegio Particular Israel y tal como está, llenamos los campos apropiados con la información relevante para planificar la red WLAN.

Figura 53

Especificaciones para la cobertura del Colegio Particular Israel

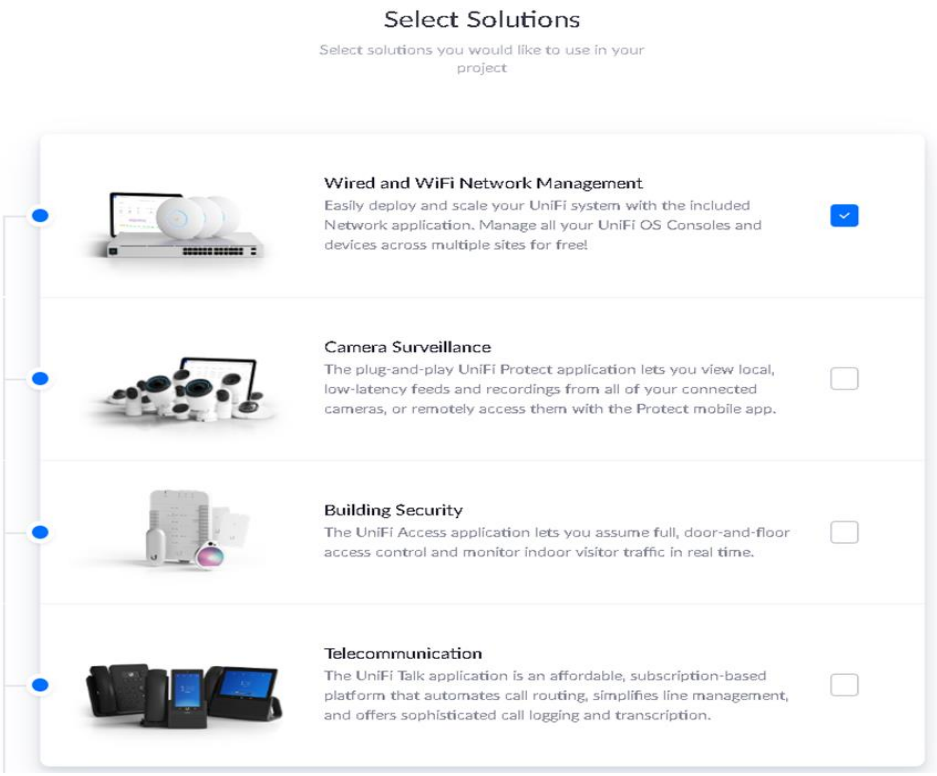


Nota. La siguiente figura representa las respectivas especificaciones para la cobertura de red del Colegio Particular Israel.

Después de hacer clic en Siguiente, seleccionamos los conjuntos que se utilizarán para organizar la red WiFi. En esta parte seleccionamos el fragmento Administración de redes cableadas y wifi y presionamos Siguiente.

Figura 54

Selección del equipo

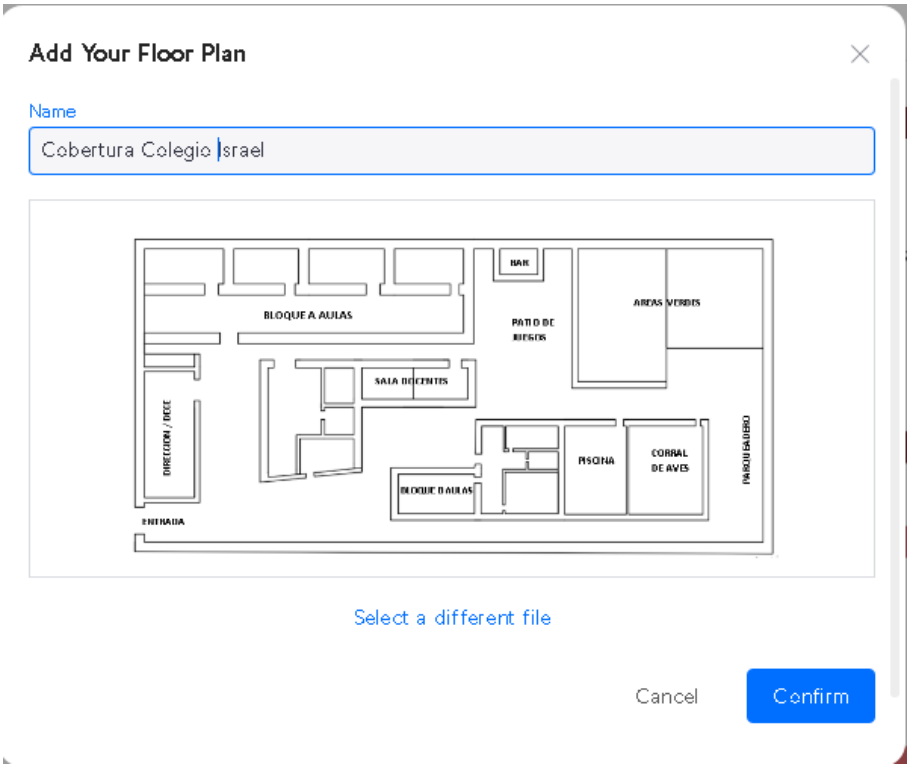


Nota. La siguiente figura representa la selección de equipos inalámbricos.

En esta ventana procedemos a seleccionar plano del Colegio en este caso la cobertura de la red WLAN se necesita para la sala de docentes ya que la red principal se encuentra en la Dirección/DECE de la misma manera colocamos el nombre de Cobertura Colegio Israel y presionamos en créate para generar el área de trabajo de la planificación de la red WLAN para las instalaciones.

Figura 55

Selección del plano



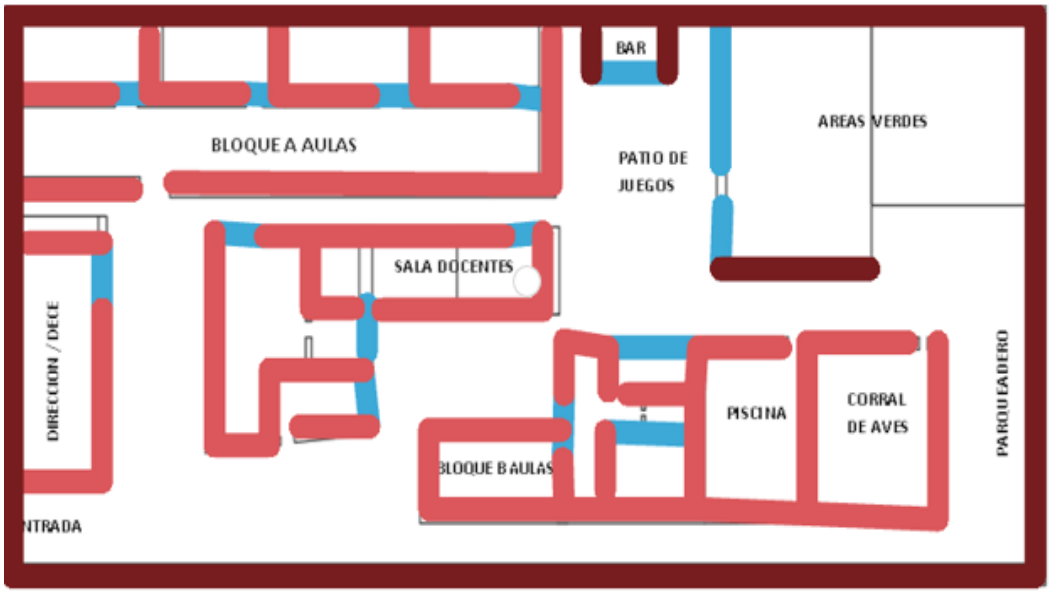
Nota. La figura representa la selección del plano para la ubicación del equipo inalámbrico.

Procedemos a hacer otro dibujo de las paredes en el plano, también dibujamos las puertas y ventanas para que el conjunto pueda distinguir todos esos límites en el plano y al colocarlos verifique el nivel de señal que llega a cada uno parte del campo de casa y poder revisar si aumentar más aspectos de la renta o moverlo primero para que cubra todo y no haya ángulos muertos.

Luego de terminar con la preparación de las paredes, puertas y ventanas, se procedió a tender el equipo inalámbrico en un plano con los respectivos cables del rack como se muestra en la imagen.

Figura 56

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 última parte nació una simulación para visualizar la señal proveniente del punto de acceso a la sala de reuniones y así ver si es necesario agregar más puntos de acceso para cubrir zonas muertas donde no hay señal de la red, la simulación se realiza en el canal de operación 2,4 GHz considerando que el dispositivo seleccionado trabaja en esta frecuencia como se muestra en la figura.

Figura 57

Simulación del Access Point

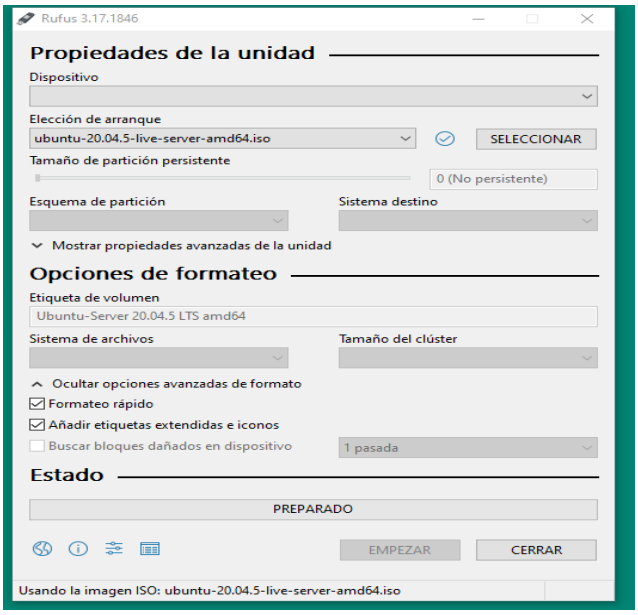
Nota. La figura representa la cobertura que genera el equipo inalámbrico ubicado en sala de reuniones.

Instalación del sistema operativo

Usando un navegador, ingresamos a la página oficial de Ubuntu server y descargamos la imagen ISO del sistema operativo, a continuación, usamos un programa para crear una unidad de almacenamiento usb booteable como se muestra en la imagen.

Figura 58

Herramienta Rufus

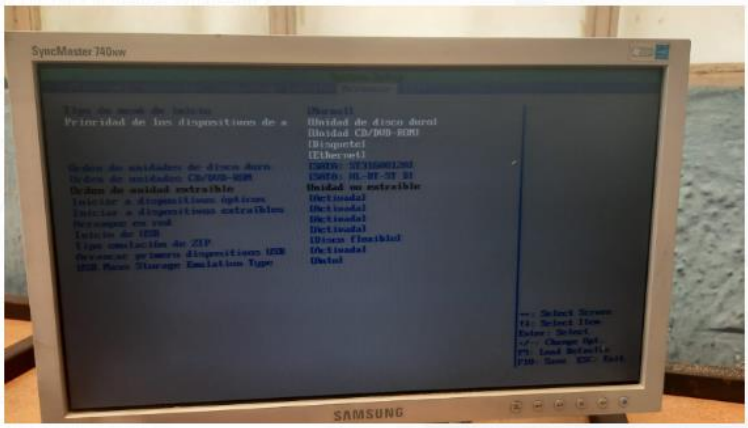


Nota. En la figura se observa la herramienta a usar para crear la unidad de almacenamiento booteable la cual será Rufus.

Conectamos la usb booteable con el sistema operativo en un puerto antes de encender el equipo que cumplirá con la función de servidor de autentificación, ingresamos a la BIOS y cambios el orden de arranque del equipo.

Figura 59

Bios del sistema



Nota. La figura muestra la Bios del sistema en el que se trabajará.

Iniciamos con el proceso de instalación del sistema operativo dentro del cual debemos elegir entre algunas características como el idioma del teclado, la partición o totalidad del espacio del disco que se usara para la instalación, entre otras.

Figura 60

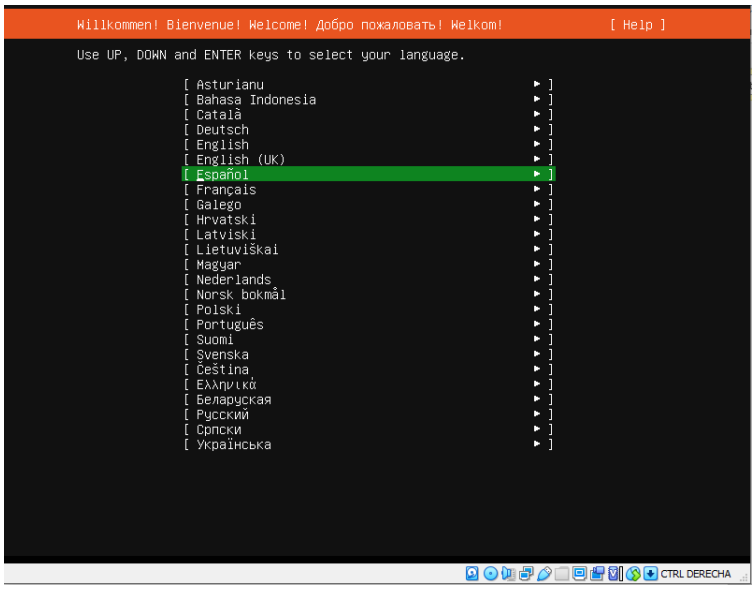
Instalación y configuración del S.O

Nota. La figura muestra el proceso inicial de instalación del sistema operativo.

Seleccionamos el idioma del sistema operativo, en nuestro caso seleccionaremos español.

Figura 61

Selección de idioma

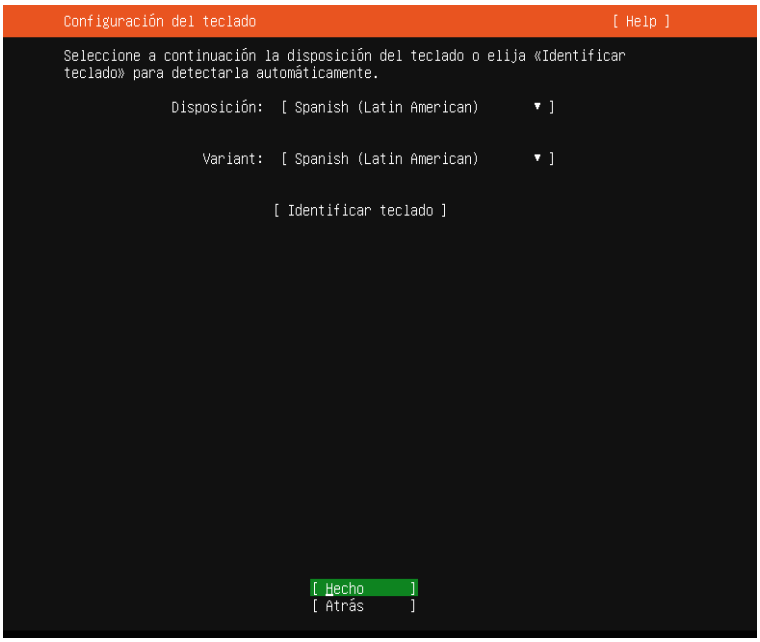


Nota. La figura muestra los diferentes idiomas que ofrece el sistema operativo para su ejecución.

Escogemos ahora el idioma de nuestro teclado puede ser inglés, español o español latinoamericano.

Figura 62

Idioma del Teclado

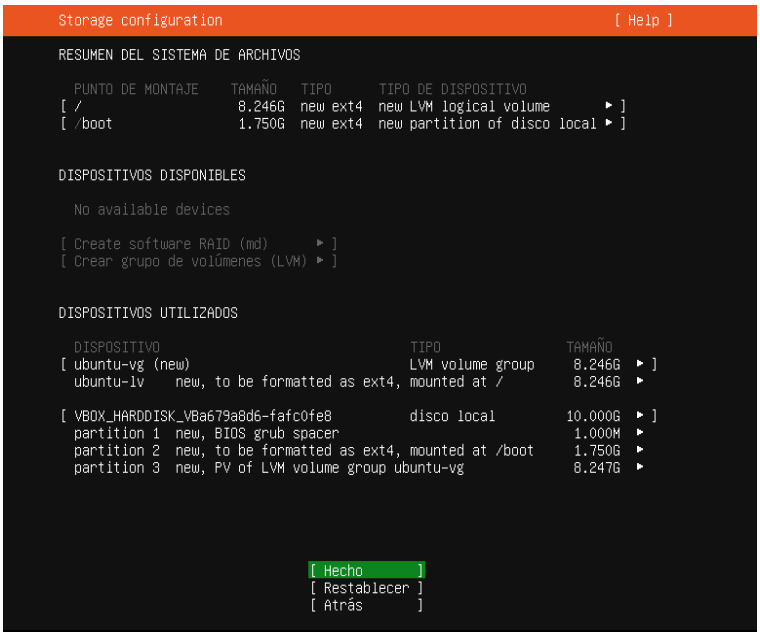


Nota. La figura muestra el idioma con el que trabajará nuestro teclado.

Se muestra un resumen del proceso que hemos realizado hasta el momento donde se puede ver detalles como el espacio de almacenamiento que usara del disco duro, la cantidad de memoria, la unidad de montaje, entre otras.

Figura 63

Detalles del disco duro

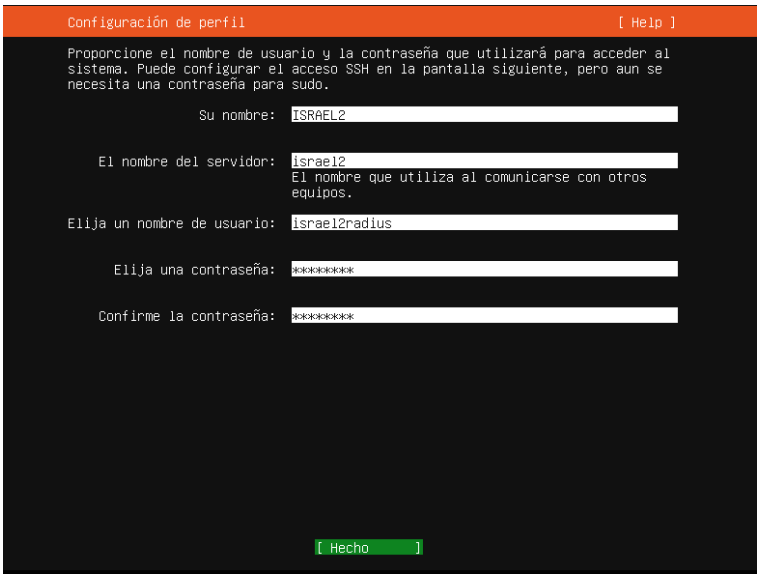


Nota. La figura muestra los detalles que tiene el disco duro del sistema operativo implementado.

Deberemos ingresar un nombre para nuestro equipo conjuntamente con un nombre de usuario y la clave de acceso o inicio de sesión con ese usuario, además esta clave nos servirá para poner realizar modificaciones desde el modo super usuario o sudo.

Figura 64

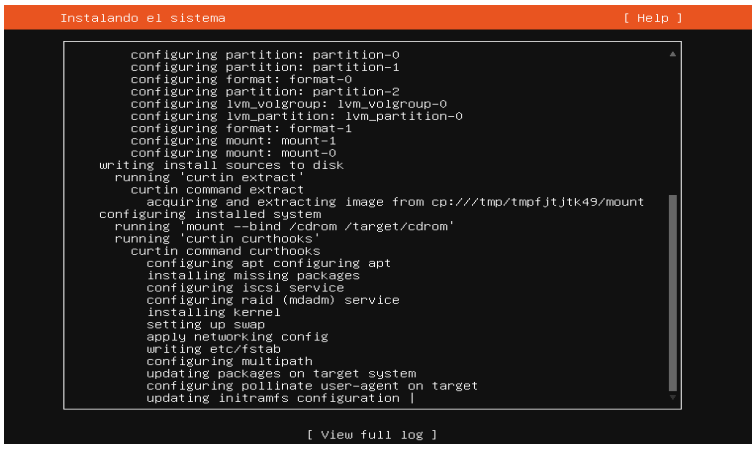
Configuración de Perfil



Nota. La figura muestra lo que solicita el sistema operativo para poder crear el perfil de usuario.

Figura 65

Inicio de instalación

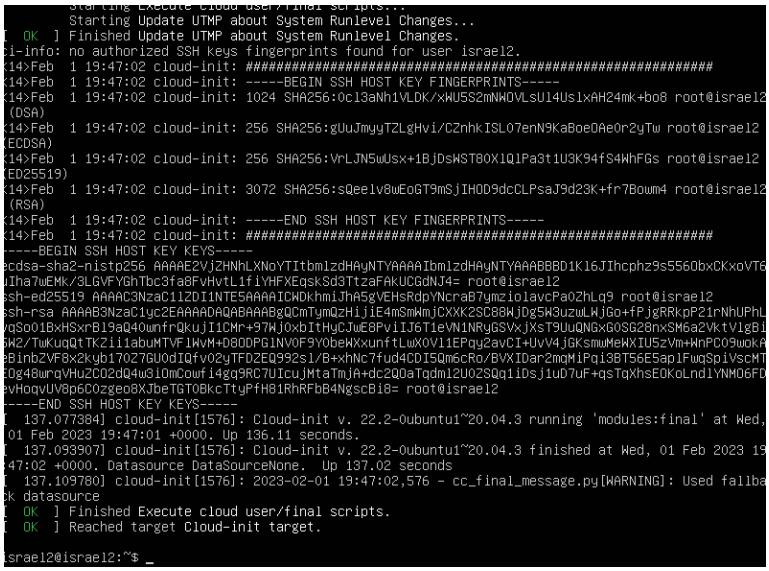


Nota. La figura muestra el inicio de instalación del sistema operativo en nuestro equipo.

Una vez se termina la instalación, retiramos la memoria usb de la computadora y reiniciamos el equipo, esto nos mostrara que la instalación que hemos realizado se ha hecho bien por lo cual podemos seguir con el resto de la implementación.

Figura 66

Confirmación de instalación exitosa



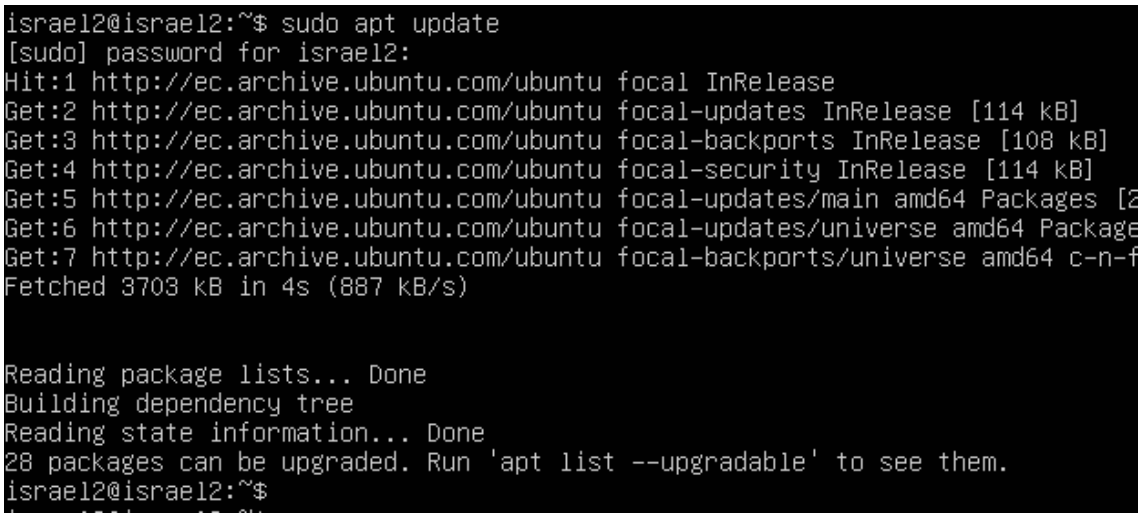
Nota. La figura muestra que la instalación ha sido exitosa.

Instalación y configuración del servidor freeradius

Luego de encender la maquina en la que se ha instalado el servidor tenemos que ingresar el nombre del equipo y la clave de usuario, a continuación, para actualizar el sistema operativo escribimos el comando sudo **apt update** como se presenta en la imagen.

Figura 67

Actualización del sistema

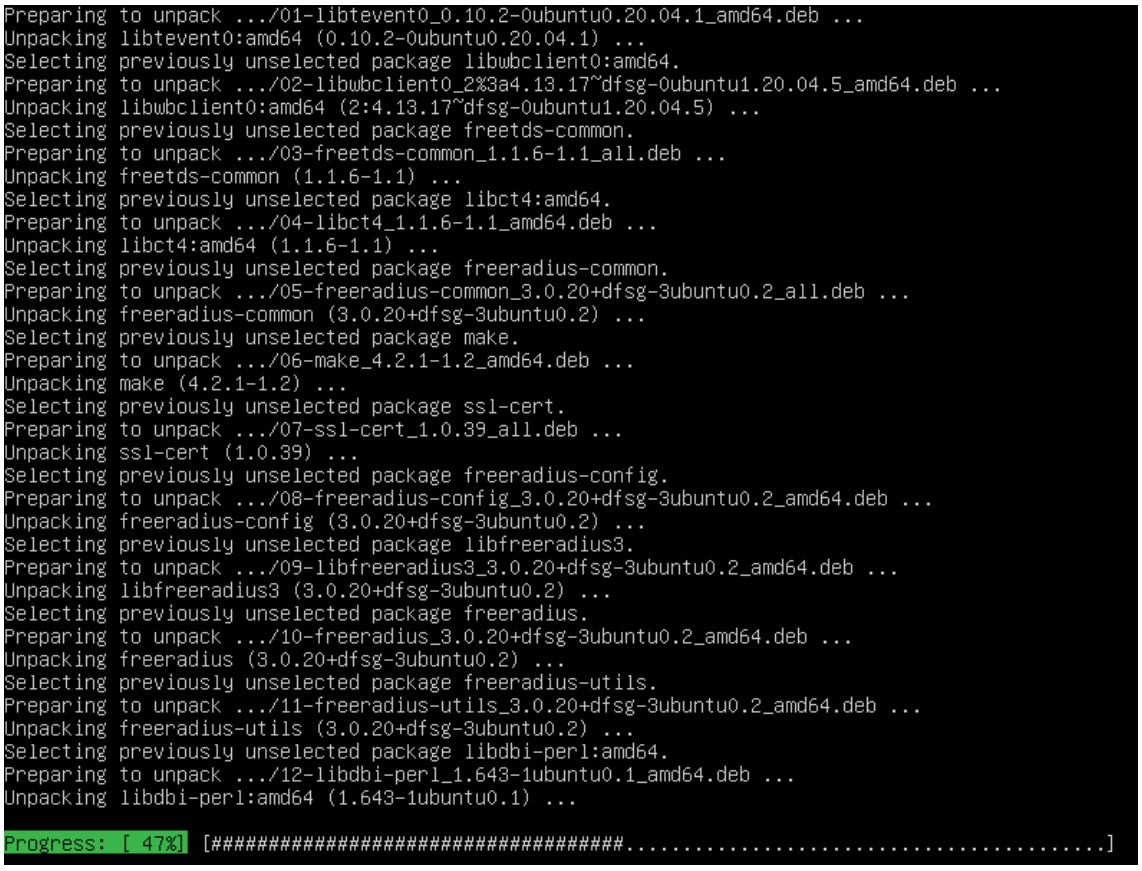


Nota. La figura muestra la actualización del sistema operativo.

Para realizar a cabo la instalación del servidor freeradius se debe escribir el código **sudo apt install freeradius,** a continuación, iniciara el proceso de descarga e instalación de los paquetes necesarios para el funcionamiento de freeradius.

Figura 68

Freeradius

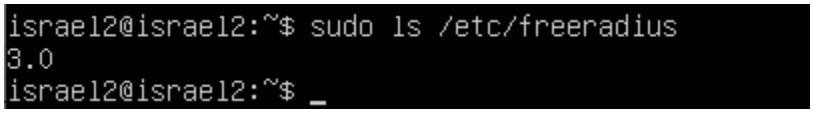


Nota. La figura muestra el proceso de instalación del servidor Freeradius.

Una vez instalado el servidor, para conocer la versión que estamos usando se tiene que escribir el comando **sudo ls /etc/freeradius**

Figura 69

Versión del servidor



Nota. La figura muestra la versión que estamos usando del servidor.

Configuración de usuarios

En nuestro caso será para quince docentes que laboran en la institución, para esto con el comando **sudo vim /etc/freeradius/3.0/users** ingresamos al archivo de usuarios y dentro de este poder agregar los usuarios con sus respectivas credenciales.

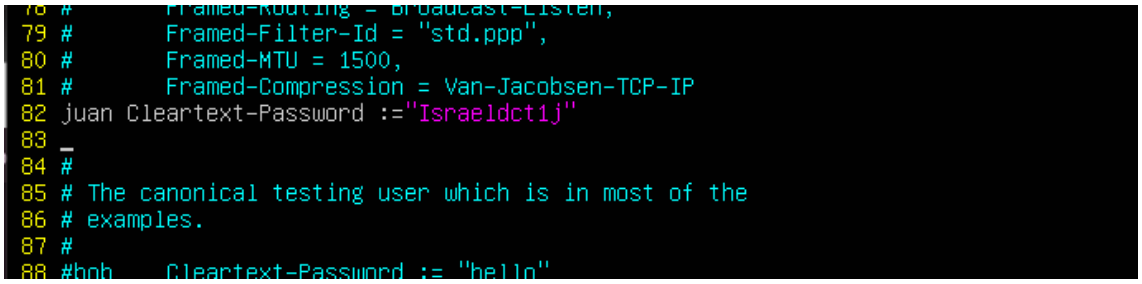
Figura 70

Comando de acceso a archivo usuarios

Nota. La figura muestra el comando ejecutado para acceder a el archivo de usuarios.

Figura 71

Creación de usuario

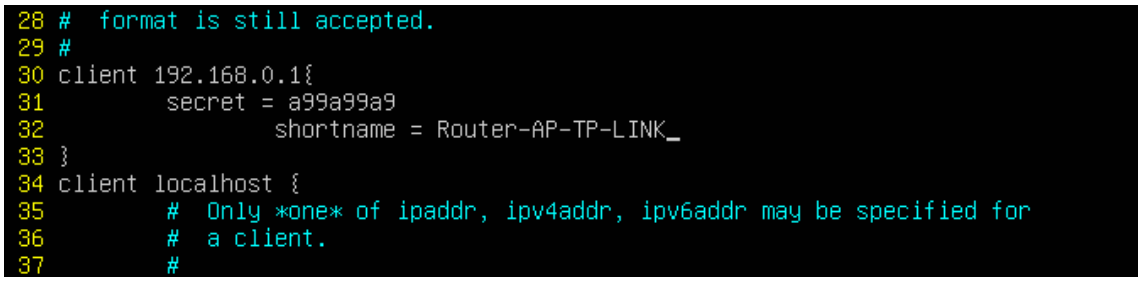


Nota. La figura indica el primer usuario creado.

Una vez que hemos configurados los usuarios, continuaremos con la configuración de los clientes o equipos que se van a relacionar con el servidor de autentificación freeradius y que dentro de sus características tengan el tipo de seguridad inalámbrica wpa2 enterprise como es el caso del Tp-link modelo TL-WR940N. Escribimos el código **sudo vim/etc/freeradius/3.0/clients.conf**

Figura 72

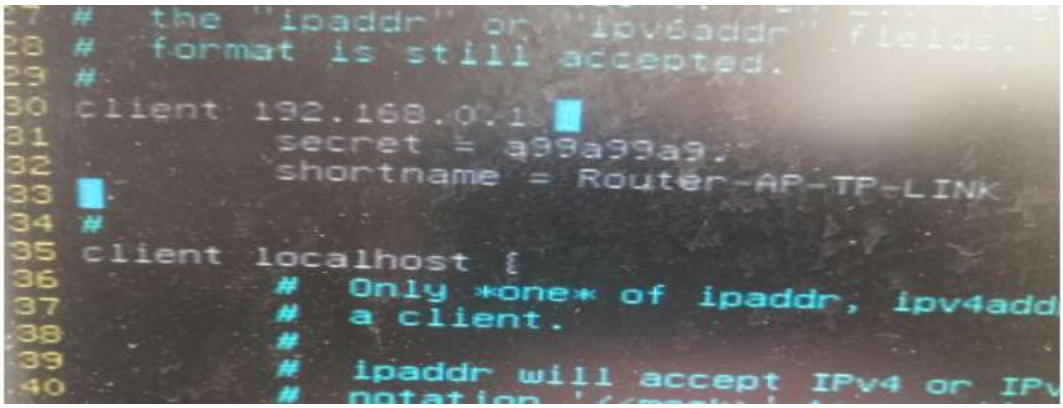
Equipo



Nota. La figura indica el equipo que se va a ocupar conjuntamente con el servidor.

Figura 73

Clientes

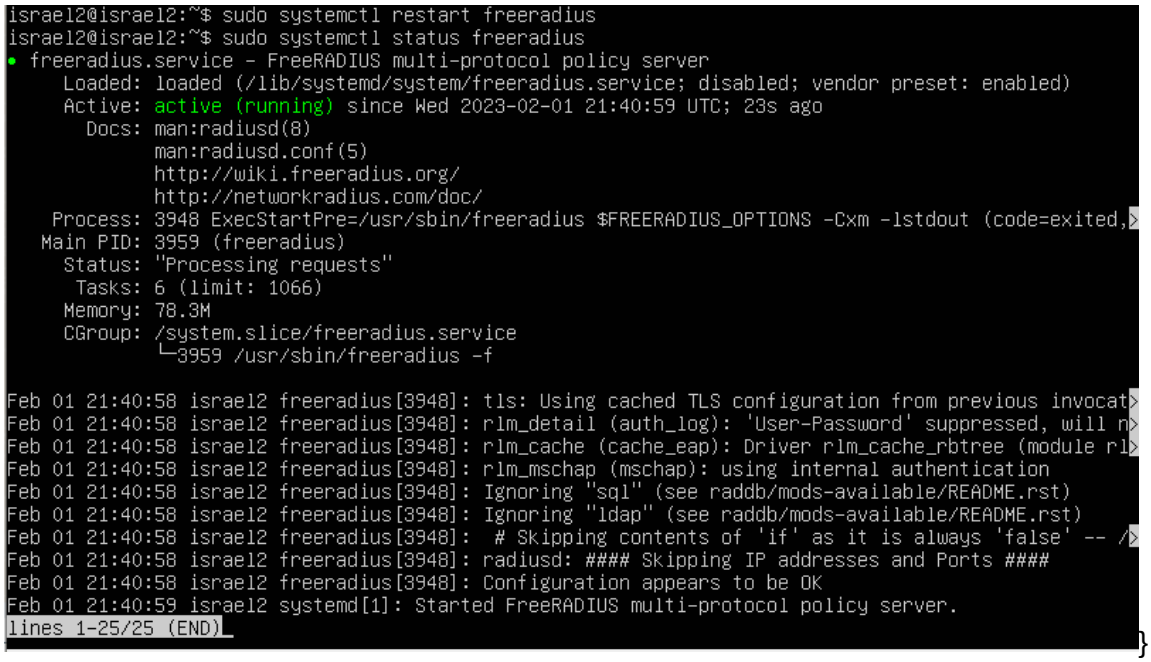


Nota. La figura muestra el cliente que se le creó al equipo.

Reiniciamos el servidor para que se guarden los cambios y las configuraciones que hemos realizado, para esto escribimos el comando **sudo systemctl restart freeradius y** adicionalmente para comprobar que el servidor este encendido y funcionado debemos escribir el comando **sudo systemctl status freeradius**.

Figura 74

Comprobación de funcionamiento del servidor



Nota. La figura indica que el servidor está activo y correctamente funcional.

Se usan los comandos **Ip address** o **ifconfig** para ver la dirección ip que se ha asignado a nuestro servidor, esta dirección ip se usara más adelante en la configuración del equipo para que el servidor y el equipo puedan estar enlazados entre sí y poder llevar a cabo la autentificación de los usuarios que se conecten a la red.

Figura 75

Dirección IP del servidor

Nota. La figura muestra la dirección IP asignada a nuestro servidor.

Y finalmente para poder monitorear a los clientes que se conecten a nuestra red inalámbrica usamos el comando **sudo vim /etc/freeradius/3.0/radiusd.conf**. Dentro de este archivo modificamos de no a yes, a la autentificación del registro de los usuarios e igualmente el registro de contraseñas si es rechazada y si es incorrecta.

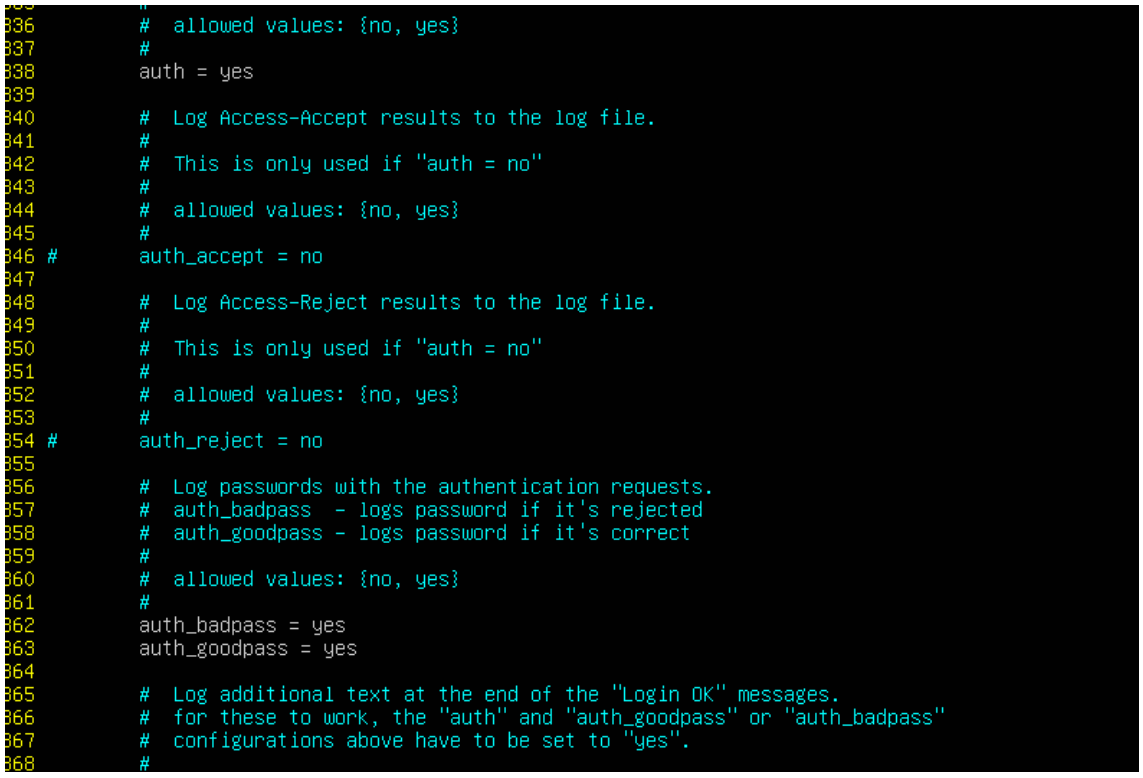
Figura 76

Comando de autenticación

Nota. La figura muestra el comando a usar para acceder al archivo de configuración de autenticación.

Figura 77

Confirmación o denegación

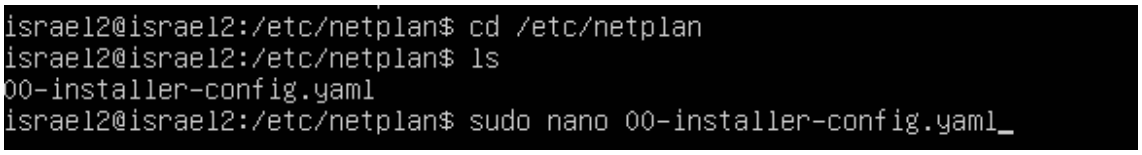


Nota. La figura muestra las configuraciones que se le dará en la autenticación de cada usuario.

Finalmente debemos realizar la configuración de la ip estática del servidor, con el comando **su cd /etc/netplan.** Luego **ls** para la lista de archivos. Luego el archivo que ya está creado. Luego **sudo nano 00-installer-config.yaml** para ingresar al archivo y dentro de este agregamos la dirección ip que le vamos a dar al servidor tomando en cuenta que este dentro del rango establecido por la red a la que está conectado el servidor, luego deshabilitamos el protocolo dhcp y para concluir esta configuración agregamos el Gateway o puerta de enlace y algunos servidores que estén cercanos o sean eficientes como en nuestro caso el de Google 8.8.8.8.

Figura 78

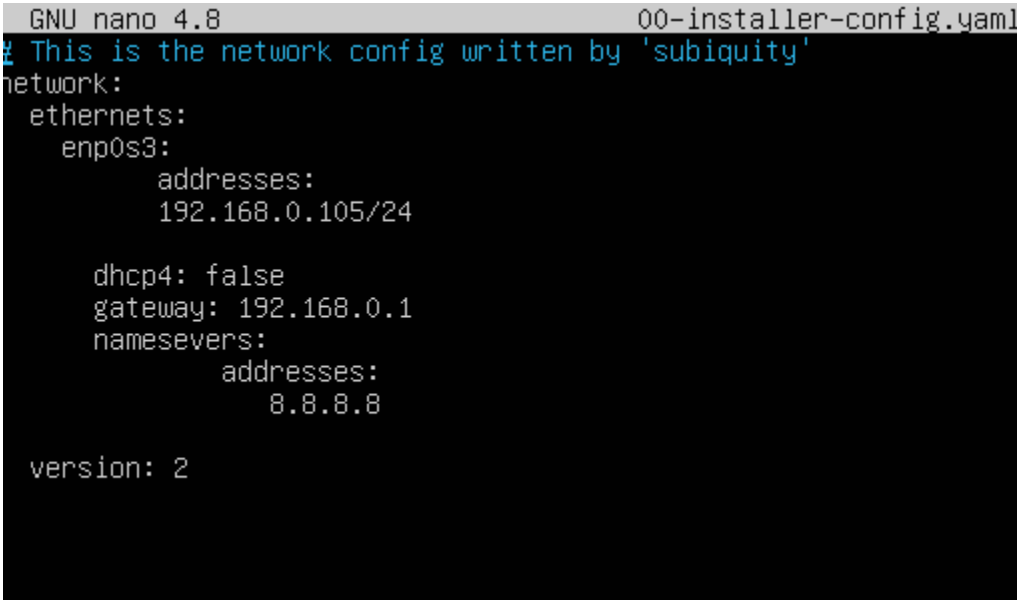
Comando de acceso para agregar IP al servidor



Nota. La figura indica el comando a usar para designar la ip a nuestro servidor.

Figura 79

IP designada



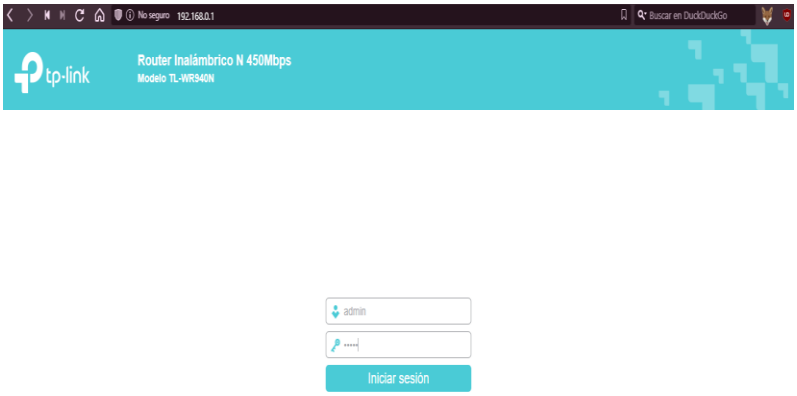
Nota. La figura indica la dirección IP designada al servidor.

Configuración del punto de acceso

Escribimos en un navegador web la direcion ip que se le ha destinado a nuestro equipo, despues con las credenciales de acceso por defecto admin tanto para el ususario como para la clave, ingresamos a la configuracion del equipo.

Figura 80

Interfaz de acceso al equipo



Nota. La figura muestra la interfaz de acceso del equipo a configurar.

Creamos la red WLAN con seguridad wpa2 personal a la que le dimos el nombre de DOCENTES ISRAEL2, para esto debemos dirigirnos a la pestaña inalámbrico , luego a configuración inalámbrica, cambiamos el nombre de la red, guardamos los cambios, luego en la pestaña seguridad inalámbrica escogemos el tipo de seguridad wpa2 personal y escribimos la clave de acceso temporal que tendrá esta red.

Figura 81

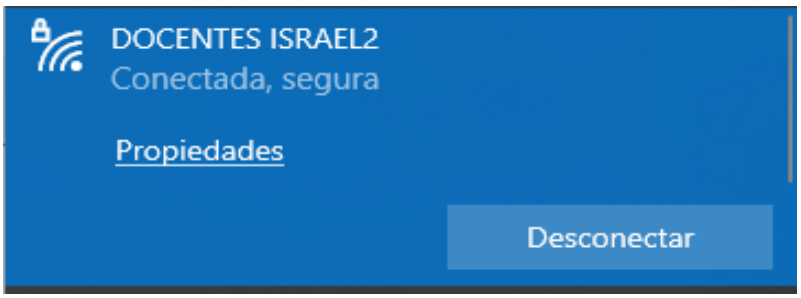
Configuración de red

Nota. La figura muestra las configuraciones de red que tendremos.

Una vez que hemos configurado la red con el tipo de seguridad inalamrica wpa2 personal podremos observar cómo se creó esta red y a la cual se pude acceder con normalidad

Figura 82

Red Creada



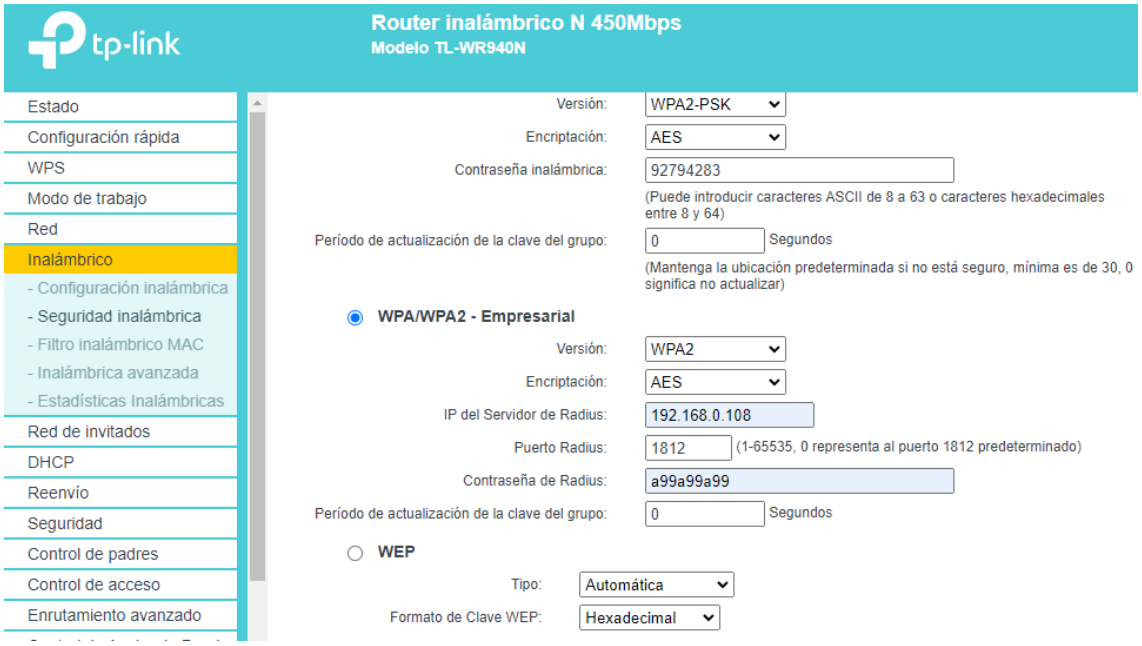
Nota. La figura muestra la red creada y funcional.

Para avanzar con la configuración de nuestra red el próximo paso a desarrollarse es el de cambiar el tipo de seguridad inalámbrica a la que corresponde con el servidor de autentificación, en este caso es la wpa2 enterprise.

Para modificar el tipo de seguridad debemos desde el equipo. En la pestaña seguridad inalámbrica seleccionar la opción de wpa2 enterprise, posteriormente seleccionar la versión y la encriptación WPA2 y AES respectivamente, colocaremos la dirección ip del servidor, luego el puerto por defecto y la clave que pusimos en el archivo clients.conf del servidor. Guardamos los cambios.

Figura 83

Aplicación de seguridad a la red



Nota. La figura muestra las configuraciones correspondientes de seguridad que deberá tener nuestra red.

Capítulo IV

Conclusiones, Recomendaciones

Conclusiones

- Al finalizar la implementación y las pruebas realizadas en el Colegio se concluyó que técnicamente es posible realizar de acuerdo al plan en instituciones que requerían sistemas de seguridad mediante videovigilancia. Sin embargo, además se debe tener en cuenta el componente de precio que conlleva dicho uso, ya que se utilizaron kits y dispositivos que brindan un soporte óptimo en términos de seguridad.
- El sistema de video vigilancia se instala con un total de 4 cámaras, las cuales son de tipo fijo, debido a que el área de grabación y el ángulo no son amplios y se pueden observar de acuerdo a las necesidades del área a monitorear. Cada uno permanece conectado a un videoclip digital montado en el cuarto de rack que dispone la institución para controlar todo el sistema instalado y evitar manipulaciones por parte de personas no autorizadas.
- Con la implementación de un router mediante la configuración para un punto de acceso se logró una mejor administración de la red de igual manera la configuración del servidor freeradius el cual nos permitirá tener un control de acceso a la red, nos permite tener mejor estabilidad y seguridad para los usuarios.
- En el momento de realizar la implementación, el grabador (NVR), se presenta un problema particular con respecto a su inicialización. Esto se debe a que el equipo fue entregado preconfigurado con una contraseña el cual el cliente no tenía conocimiento, cabe recalcar que por ser equipos originales y de una organización de distribución, nos brindan equipos nuevos sin problemas o inconvenientes.

- En definitiva, la implementación de este plan logró ampliar y aplicar los conocimientos adquiridos durante la carrera de redes y telecomunicaciones, y al mismo tiempo pudimos contribuir a la organización educativa optimizando la estabilidad física a través de la videovigilancia y la estabilidad de la red a través del control de acceso a él.

Recomendaciones

- Se recomienda que las unidades USB no autorizadas no se inserten en el NVR por ningún motivo para evitar posibles virus o configuraciones incorrectas del sistema.
- Con el fin de prolongar la vida útil del dispositivo, se ofrece realizar un mantenimiento preventivo del sistema, es decir, limpieza de las cámaras, NVR, así como la revisión periódica del almacenamiento de información.
- Se sugiere que el servidor Freeradius como sistema operativo instalado en la computadora se actualice con una versión nueva y estable de este programa en los años siguientes, mejorando así el rendimiento del dispositivo, y mejorando la estabilidad del mismo sistema.
- Para este tipo de proyectos lo más conveniente es usar un breaker independiente puesto que así no interferimos en las conexiones eléctricas existentes, para ello realizar el cálculo de amperaje conociendo el breaker más óptimo a usar.

Presupuesto

Tabla 11

Presupuesto del proyecto

Descripción	Cantidad	Precio Unitario	Valor Total
NVR 4CH – H.265+ - 1 SATA – 1 HDMI – 4 PoE – MAX. 36W – DHI-NVR1104HS-P-S3/H	1	$120.80	$120.80
DAHUA CAMARA IP TUBO 4MP – 2.8MM – IR30M – PoE – IP67 – SEMIMET – DH-IPC-HFW1431S1N	4	$95.18	$380.72
DISCO DURO 2TB WESTERN DIGITAL GREENPOWER	1	$96.20	$96.20
Router TP-LINK TL-WR930N	1	$33.00	$33.00

Descripción	Cantidad	Precio Unitario	Valor Total
Cable UTP categoría 6	100m	$0.60	$60.00
Conectores RJ45	20 unidades	$0.30	$6.00
Canaletas 20x12	50 unidades	$2.00	$100.00
Tornillos de pared	25 unidades	$0.08	$2.00
Tacos Fisher f6	25 unidades	$0.05	$1.25
Broca de concreto carioca ¼	1	$1.25	$1.25
Cajas de Paso eléctricas 10x10	4	$2.00	$8.00
		Total	$809.22

Nota. La tabla muestra los gastos realizados para la implementación del proyecto

Bibliografía

Abraham. (s.f.). *practicasuptxabraham*. Obtenido de https://sites.google.com/site/practicasuptxabraham/3-1practica-de-laboratorio-investigacion-de-estandares-de-redes

Acero, J. (2018). Obtenido de https://biblus.us.es/bibing/proyectos/abreproy/12446/fichero/PFC-2446-ACERO.pdf

Admin. (17 de Noviembre de 2015). *capta*. Recuperado el 26 de Enero de 2023, de http://www.capta.com.mx/4-beneficios-de-tener-camaras-de-videovigilancia/

Aimeseguridad. (2014). *aimeseguridad*. Recuperado el 26 de Enero de 2023, de https://www.aimeseguridad.com/camaras-de-videovigilancia/

Amortegui, T., & Valencia, G. (13 de Mayo de 2022). *integracademy*. Recuperado el 26 de Enero de 2023, de https://integracademy.com/que-es-tecnologia-full-color-en-camaras-de-seguridad-cctv/#:~:text=Este%20tipo%20de%20tecnolog%C3%ADa%20hace,%3A%20sin%20iluminador%2C%20con%20Iluminador.

Aresseguridad. (30 de Marzo de 2018). *Aresseguridad*. Recuperado el 26 de Enero de 2023, de https://aresseguridad.es/como-funciona-un-sistema-de-videovigilancia/

Argüello, F. (15 de 01 de 2023). *infoteknico*. Obtenido de https://www.infoteknico.com/que-es-un-dvr-y-como-funciona/

aula Clic. (11 de 2020). Obtenido de https://www.aulaclic.es/fotografia-photoshop/t_2_13.htm

Baldo, P. (08 de Agosto de 2014). *clarin*. Recuperado el 26 de Enero de 2023, de https://www.clarin.com/construccion/seguridad-domestica_0_rysjQ59w7e.html

Bdrinformatica. (4 de Junio de 2022). *bdrinformatica*. Recuperado el 26 de Enero de 2023, de https://bdrinformatica.com/beneficios-de-la-videovigilancia-en-tu-empresa/

Cantalapiedra, S. (18 de 04 de 2017). *NIVIAN*. Obtenido de https://www.nivianhome.com/es/que-es-camara-ip-como-funciona/

cartronicgroup. (2023). Obtenido de https://grupocartronic.com/seguridad-perimetral-efectiva/

Casarino, E. (25 de 08 de 2015). rnds. *.tecnología*, 183.

Castillo, J. (15 de 02 de 2019). *Profesional Review*. Obtenido de https://www.profesionalreview.com/2019/02/15/fibra-optica-que-es/

Cisco. (2015). *Cisco*. Recuperado el 27 de Enero de 2023, de https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/wireless-network.html#~introduction

Coimbra, E. (21 de 11 de 2011). Obtenido de http://www.coimbraweb.com/

Coñapes, S. (24 de Marzo de 2015). *Sities Google*. Recuperado el 27 de Enero de 2023, de https://sites.google.com/site/redesinalambricas3/tipos-de-redes-inalambricas

Covertsecurit. (30 de Septiembre de 2022). *covertsecurit*. Recuperado el 27 de Enero de 2023, de https://covertsecurity.es/seguridad-perimetral-que-es-y-cuales-son-sus-beneficios/

Darkcrizt. (14 de 10 de 2021). *DesdeLinux*. Obtenido de https://blog.desdelinux.net/ubuntu-21-10-impish-indri-llega-con-actualizaciones-nuevo-instalador-y-mas/

De Alfonso, C., Caballer, M., & Hernandez, V. (21 de Junio de 2005). *dsic.upv*. Recuperado el 28 de Enero de 2023, de http://www.dsic.upv.es/docs/bib-dig/informes/etd-06242005-121243/DSIC-II-04-05.TechReport.pdf

Desarrollarinclusion. (2017). *Desarrollarinclusion*. Recuperado el 29 de Enero de 2023, de https://desarrollarinclusion.cilsa.org/tecnologia-inclusiva/que-es-un-sistema-operativo/

Diaridetarragona. (16 de Abril de 2019). *diaridetarragona*. Recuperado el 26 de Enero de 2023, de https://www.diaridetarragona.com/patrocinado/la-importancia-de-contar-con-camaras-de-vigilancia-20190416-0006-DRdt201904160006

Elcapored. (2020). *Elcapored*. Recuperado el 28 de Enero de 2023, de https://elcapored.jimdofree.com/normas-568a-568b/

Electronicid. (28 de Julio de 2022). *electronicid*. Recuperado el 27 de Enero de 2023, de https://www.electronicid.eu/es/blog/post/como-funciona-reconocimiento-facial/es

F5 Glossary. (2019). *F5*. Recuperado el 28 de Enero de 2023, de https://www.f5.com/es_es/services/resources/glossary/wireless-network-security

Galán, P. (18 de Novembre de 2018). *elperiodicoextremadura*. (E. S. A, Editor) Recuperado el 25 de Enero de 2023, de https://www.elperiodicoextremadura.com/el-mostrador/2018/11/15/han-evolucionado-sistemas-seguridad-44095206.html

Garcia, A. (16 de 01 de 2017). *avitom*. Obtenido de https://www.avitom.es/elegir-una-camara-de-seguridad-segun-la-resolucion/

Grupo Meyah. (2023). Obtenido de https://grupomeyah.com/reconocimiento-de-matriculas/

Hernandez, W. (6 de Junio de 2016). *sistemasoperativosax.wordpress*. Obtenido de https://sistemasoperativosax.wordpress.com/2016/06/06/ventajas-y-desventajas-de-los-sistemas-de-seguridad/

IONOS. (15 de 09 de 2020). Obtenido de https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-servidor-un-concepto-dos-definiciones/

Irving. (08 de 06 de 2021). *FS Community*. Obtenido de https://community.fs.com/es/blog/utp-or-stp-cables-for-10gbase-t-network.html

LAGE. (27 de 06 de 2022). Obtenido de https://www.lage.com.mx/blog/que-es-y-para-que-sirve-la-seguridad-electronica

Lancastergill. (2023). *Quizlet*. Obtenido de https://quizlet.com/183578966/ats-gcse-biology-rp6-light-intensity-and-rate-of-photosynthesis-flash-cards/

López, J. (03 de 2007).

Martí, S. (2013). Obtenido de https://riunet.upv.es/bitstream/handle/10251/34082/memoria.pdf

Martinez, J. (27 de 01 de 2023). *YMANT*. Obtenido de https://www.ymant.com/blog/que-es-un-ap-access-point-y-que-usos-y-modos-tiene/

Martinez, T. (02 de 05 de 2012). *telequismo*. Obtenido de https://www.telequismo.com/2012/05/seguridad-en-redes-wifi.html/

Merino, M. (20 de Agosto de 2019). *Xataka*. Recuperado el 27 de Enero de 2023, de https://www.xataka.com/inteligencia-artificial/inteligencia-artificial-tambien-esta-carretera-asi-funciona-reconocimiento-automatico-matriculas-anpr

MexicoNewark. (2018). *Mexico newark*. Recuperado el 29 de Enero de 2023, de https://mexico.newark.com/wireless-wifi-technology#:~:text=Fidelidad%20inal%C3%A1mbrica%20(Wireless%20Fidelity)%20es,IEEE%20802.11%20para%20redes%20WLAN.

Montoya, C. N. (2014). *Sistema de seguridad con videovigilancia*. Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/6529/1/TesisCompleta-523.pdf

Novaseguridad. (29 de Noviembre de 2020). *novaseguridad*. Recuperado el 25 de Enero de 2023, de https://www.novaseguridad.com.co/sistema-de-seguridad-beneficios/

PCREDCOM. (18 de 12 de 2021). Obtenido de https://pcredcom.com/blog/seguridad-y-vigilancia/camaras-analogicas/

Profinetuniversity. (22 de Noviembre de 2019). *Profinetuniversity*. Recuperado el 28 de Enero de 2023, de https://profinetuniversity.com/caracteristicas-especiales-profinet/tecnologia-inalambrica-profinet-arquitecturas/

Redes. (3 de Enero de 2017). *Irix*. Recuperado el 28 de Enero de 2023, de https://www.irix.es/blog/control-de-acceso-en-redes-inalambricas/

Redesinalambricas. (22 de Agosto de 2019). *RedesInalambricas*. Recuperado el 28 de Enero de 2023, de https://www.redesinalambricas.es/estandares-wifi/

Rico, M. (20 de 09 de 2017). *telecocable*. Obtenido de https://www.telecocable.com/blog/ventajas-y-desventajas-del-cable-utp/1385

Rodriguez, A. (21 de 08 de 2020). *GoDaddy*. Obtenido de https://es.godaddy.com/blog/que-es-ubuntu-y-para-que-sirve/

Rogel, A. (2016). *repositorio.uisrael.edu.ec*. Recuperado el 26 de Enero de 2023, de http://repositorio.unesum.edu.ec/bitstream/53000/1595/1/UNESUM-ECU-REDES-2019-41.pdf

Romero, J. (05 de 10 de 2021). *Geeknetic*. Obtenido de https://www.geeknetic.es/SoC/que-es-y-para-que-sirve#:~:text=Un%20SoC%20sirve%20para%20concentrar,concentrado%20en%20un%20mismo%20lugar

Ruiz, H. (26 de Marzo de 2018). *teamnet*. Recuperado el 26 de Enero de 2023, de https://www.teamnet.com.mx/blog/ventajas-y-desventajas-de-las-c%C3%A1maras-de-seguridad

Sapalomera. (2006). *sapalomera*. Recuperado el 27 de Enero de 2023, de https://www.sapalomera.cat/moodlecf/RS/3/course/module4/4.3.2.2/4.3.2.2.html#:~:text=IEEE%20802.11i%2FWPA2%3A%20IEEE,protocolo%20de%20cifrado%20m%C3%A1s%20seguro.

Scati. (23 de Febrero de 2022). *scati*. Recuperado el 26 de Enero de 2023, de https://www.scati.com/inteligencia-artificial-videovigilancia/

Sigmixv. (17 de Enero de 2021). *sigmixv*. Recuperado el 26 de Enero de 2023, de https://sigmixv.com/ventajas-de-las-camaras-ip-vs-camaras-analogicas/

SistemSeguridad. (s.f.). Obtenido de https://www.sistemseguridad.com/producto/camara-domo-ptz-ip-2mp-hilook/

Sities Google. (2017). *Sities Google*. Recuperado el 28 de Enero de 2023, de https://sites.google.com/site/ticredin/dispositivos-de-la-infraestructura-inalambrica

Solutech. (2022). Obtenido de https://solutechtelecom.com/redes-y-enlaces-inalambricas/

Sony. (12 de Julio de 2018). *Sony*. Recuperado el 27 de Enero de 2023, de https://www.sony.es/electronics/support/articles/S700023888

Sosio, N. (09 de Junio de 2022). Obtenido de https://www.seguridadsos.com.ar/nvr/

Tecalsa. (s.f.). Obtenido de https://tecalsa.net/camaras-de-conteo/

Tecnit. (19 de 04 de 2019). Obtenido de https://tecnit.com.ec/producto/grabador-de-video-nvr-hikvision-ds-7608ni-k1-8pb-8ch-poe-hdmi-vga-usb-h-265/

Tecnoseguro. (19 de Febrero de 2018). *tecnoseguro*. Recuperado el 26 de Enero de 2023, de https://www.tecnoseguro.com/faqs/cctv/que-es-el-video-ip

Tic.portal. (14 de 03 de 2022). Obtenido de https://www.ticportal.es/glosario-tic/tecnologia-redes

Toda materia. (06 de Noviembre de 2019). *Todamateria*. Recuperado el 29 de Enero de 2023, de https://www.todamateria.com/sistema-operativo/

Todo sobre redes. (10 de 2014).

TST Ecuador. (2023). Obtenido de http://www.tst.ec/ver-producto/cmara-ip-hikvision-mini-domo-fisheye-360-ir-4mp--3898195/cmaras-ip

U.S. Robotics. (2023). Obtenido de https://support.usr.com/support/5451/5451-es-ug/wireless.html

Universitat Carlemany. (14 de Abril de 2022). *Universitatcarlemany*. Recuperado el 29 de Enero de 2023, de https://www.universitatcarlemany.com/actualidad/blog/tipos-de-sistemas-operativos/#:~:text=Sistemas%20operativos%20b%C3%A1sicos%3A%20los%20m%C3

%A1s%20comunes%20y%20utilizados&text=Dentro%20de%20los%20primeros%20est%C3%A1n,varias%20versiones%20de%20funcion

Videoanaliticas.com. (2016). Obtenido de http://videoanaliticas.com/

VIVOTEK. (s.f.). Obtenido de https://www.vivotek.cl/camaras-ip-tipo-box/1150-camara-ip-tipo-box-ip8155hp.html

Walton, A. (21 de 03 de 2021). *CCNA*. Obtenido de https://ccnadesdecero.es/cable-directo-cruzado-y-consola-diferencias/

Wifisafe. (2019). *Wifisafe*. Recuperado el 28 de Enero de 2023, de https://www.wifisafe.com/blog/antenas/#:~:text=Una%20antena%20WiFi%20es%20un,en%20el%20resto%20de%20direcciones.

win. (2020). Obtenido de https://win.pe/blog/red-wifi-mesh-sistema-wifi-de-malla/

Worton. (15 de 07 de 2021). *FS Community*. Obtenido de https://community.fs.com/es/blog/t568a-vs-t568b-difference-between-straight-through-and-crossover-cable.html

Worton. (07 de 08 de 2021). *FS Community*. Obtenido de https://community.fs.com/es/blog/patch-cable-vs-crossover-cable-what-is-the-difference.html

ZCmayoristas. (2023). Obtenido de https://zcmayoristas.com/zcwebstore/producto/dahua-camara-bullet-dh-hac-hfw2501tun-z-a-27135-s2-5mp-lente-motorizado-%C2%B7-2-7-mm-13-5-mm-ir-80m-ip67/

Zoom Informatica. (06 de 10 de 2016). Obtenido de https://zoominformatica.com/blog/que-es-una-camara-ip/

Anexos