Implementación de un sistema de control de acceso y video vigilancia a través de una red LAN interna en el laboratorio de comunicaciones de la Universidad de Fuerzas Armadas sede Latacunga para precautelar la integridad de equipos tecnológicos.

Cumbajin Cumbajin, Alex Fabian

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Monografía, previo a la obtención del título de Tecnólogo Superior en Redes y Telecomunicaciones

Ing. Caicedo Altamirano, Fernando Sebastián

18 de febrero del 2022

Latacunga

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE TECNOLOGÍA DE REDES Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que la monografía, "**Implementación de un sistema de control de acceso y video vigilancia a través de una red LAN interna en el laboratorio de comunicaciones de la Universidad de Fuerzas Armadas sede Latacunga para precautelar la integridad de equipos Tecnológicos.**" fue realizado por el señor **Cumbajin Cumbajin, Alex Fabian** la cual ha sido revisada y analizada en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Latacunga, 18 de febrero del 2022

FERNANDO SEBASTIAN CAICEDO ALTAMIRANO

Ing. Caicedo Altamirano, Fernando Sebastián

C.C.: 180393502-0

COPYLEAKS

Monografía Cumbajin Alex CONTROL DE ACCESO Y VIDEO VI...

Scanned on: 12:45 February 18, 2022 UTC

Identical Words	465
Words with Minor Changes	132
Paraphrased Words	622
Omitted Words	0

COPYLEAKS Website | Education | Businesses

Ing. Calcedo Altamirano, Fernando Sebastián

C.C.: 180393502-0

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE TECNOLOGÍA DE REDES Y TELECOMUNICACIONES

RESPONSABILIDAD DE AUTORÍA

Yo, **Cumbajin Cumbajin, Alex Fabian**, con cédula de ciudadanía **N° 172208504-8**, declaro que el contenido, ideas y criterios de la monografía: **Implementación de un sistema de control de acceso y video vigilancia a través de una red LAN interna en el laboratorio de comunicaciones de la Universidad de Fuerzas Armadas sede Latacunga para precautelar la integridad de equipos Tecnológicos.** es de mi 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 febrero del 2022

ALEX FABIAN
CUMBAJIN
CUMBAJIN

.....

Cumbajin Cumbajin, Alex Fabian

C.C.: 172208504-8

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE REDES Y TELECOMUNICACIONES

AUTORIZACIÓN DE PUBLICACIÓN

Yo **Cumbajin Cumbajin, Alex Fabian** Autorizo a la Universidad de las Fuerzas Armadas Espe publicar la monografía: **Implementación de un sistema de control de acceso y video vigilancia a través de una red LAN interna en el laboratorio de comunicaciones de la Universidad de Fuerzas Armadas sede Latacunga para precautelar la integridad de equipos Tecnológicos,** en el repositorio institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Latacunga, 18 de febrero del 2022

ALEX FABIAN
CUMBAJIN
CUMBAJIN

.....

Cumbajin Cumbajin, Alex Fabian

C.C.: 172208504-8

DEDICATORIA

Mi proyecto de titulación se la dedico en primer lugar a Dios, al ser mi inspirador y brindarme las fuerzas necesarias para continuar en este proceso de obtener uno de los sueños más anhelados.

A mi amada hija Abigail por ser mi motivación e inspiración para superarme cada día más y luchar para que la vida nos conceda un futuro mejor.

A mi amada esposa por ser el apoyo incondicional en mi vida que, con sus consejos, su amor, y paciencia me ayudo a concluir esta meta.

A mi amada madre y hermana quienes siempre me apoyaron con palabras de aliento y no me dejaron decaer para que continuara adelante y siempre sea perseverante cumpliendo con mis ideales.

A mis compañeros y amigos, quienes compartieron su conocimiento, alegrías y tristezas.
A todas las personas que durante estos 2 años estuvieron junto a mi apoyándome y aportaron a que este sueño se haga realidad.

Cumbajin Cumbajin, Alex Fabian

AGRADECIMIENTO

Al finalizar este trabajo quiero gradecer a Dios por todas sus bendiciones, por guiarme, ser mi apoyo y fortaleza en todo este tiempo, por darme la oportunidad de llegar hasta este día tan especial de mi formación profesional.

A mi hija, mi esposa, mi madre y hermana por siempre estar pendientes de mí y apoyarme con sus consejos y amor.

A la Universidad de las Fuerzas Armadas – ESPE, que se convirtió en un lugar donde compartí grandes momentos y me permitió convertirme en un gran profesional.

A mis queridos docentes por haber compartido sus conocimientos y experiencias a lo largo de mi preparación en mi carrera.

A mi director de tesis Ing. Fernando Caicedo un agradecimiento muy especial, por ser quien me ha guiado con su paciencia y su rectitud como docente, por brindarme su apoyo, su confianza hacia mi trabajo y su gran capacidad para poder guiar mis ideas, no solo en el desarrollo de este proyecto sino también en mi formación como profesional. También le agradezco por facilitarme con todos los medios necesarios para haber podido realizar todas las actividades propuestas en el desarrollo de mi proyecto.

A mis compañeros y compañeras gracias por compartir grandiosos momentos durante estos años.

Gracias a todos

Cumbajin Cumbajin, Alex Fabian

Tabla de contenido

Índice de figuras

Índice de tablas

Resumen

Durante los últimos años y considerando la consecuencia de la situación económica actual, invertir en la seguridad se ha transformado en una partida indispensable a nivel institucional, empresarial y particular. La industria de la seguridad ha utilizado la evolución de la tecnología en el área de redes y tratamiento de imágenes y lo ha implementado a los nuevos sistemas de circuitos cerrados de televisión (cctv), creando un nuevo modelo que se basa en el protocolo IP. La investigación consiste en la Implementación de un sistema de control de acceso y video vigilancia a través de una red LAN interna en el laboratorio de comunicaciones de la Universidad de Fuerzas Armadas sede Latacunga para precautelar la integridad de equipos Tecnológicos. La instalación va a permitir controlar los accesos al laboratorio, así como resguardad la integridad del personal docente, estudiantes y de los bienes de su interior. Para cumplir con todo lo expuesto, la investigación está estructurada, de varios capítulos, como marco teórico donde se muestra todas tecnologías existentes actualmente, el desarrollo donde se indica cómo se ha avanzado paso a paso la implementación del sistema con las pruebas de funcionamiento necesarias y conclusiones que se lograron llegar las cuales contienen la información correspondiente, la historia y los tipos de redes, el sistemas de control de acceso y sistemas de video vigilancia.

Palabras clave:

- **CONTROL DE ACCESO**
- **EVOLUCIÓN TECNOLÓGICA**
- **REDES LAN**
- **CIRCUITO CERRADO DE TELEVISIÓN**

Abstract

During the last years and considering the consequence of the actual economic situation, investing in security has become in an indispensable start at the institutional business and private level. The security industry has used the evolution of the technology in the network area and image processing and has implemented it in the new closed circuit television systems creating a new model that is based on the IP protocol. The investigation consists in the Implementation of an access control and video surveillance system through an internal LAN network in the communications laboratory of the University of the Armed Forces, Latacunga headquarters, to protect the integrity of technological equipment. The installation will allow to control the access to the laboratory as well as safeguard the integrity of the teaching staff, students and the assets inside. To fulfill with everything exposed above, the research is structured, of several chapters, as a theoretical framework where all currently existing technologies are shown, the development where it is indicated how the implementation of the system has been advanced step by step with the necessary performance tests and conclusions that were reached which contain the corresponding information, history and types of networks, access control systems and video surveillance systems.

Key words:

- **ACCESS CONTROL**
- **TECHNOLOGICAL EVOLUTION**
- **LAN NETWORKS**
- **CLOSED CIRCUIT TELEVISION**

Capítulo I

1. Introducción

1.1. Antecedentes

La seguridad en la actualidad es uno de los puntos más importantes dentro de cualquier organización a nivel mundial, muchos investigadores han desarrollado diferentes técnicas de seguridad con el avance de la tecnología mejorando y perfeccionando su utilización en sistemas complejos de seguridad para controles de acceso a instalaciones específicas de infraestructuras de gran importancia precautelando material equipo y personal.

Pérez Hugo, en su proyecto de investigación desarrollado en el año 2018 cuyo tema es “Sistema de control de acceso por reconocimiento de iris para el ingreso de personal a la empresa electro servicios Querubín de la ciudad de Puyo” ha realizado la implementación de un sistema de control de acceso utilizando patrones físicos o de retina que son más fiables en referencia a seguridades e identificación, con porcentaje de 0% de falsas aceptaciones y con un 5,56% de falsos rechazos estableciendo una alta confiabilidad el mismo, con lo cual se incrementó el nivel de seguridad el registro de fecha y hora de ingreso y salida a las instalaciones facilitando las revisión de los videos de seguridad. (Vinicio, 2018)

Pablo Castro, en su proyecto de investigación desarrollado en el año 2018 cuyo tema es “Implementación de un sistema de control de acceso biométrico zk-x7 por medio de huella dactilar en el laboratorio de hardware de la carrera de ingeniería en computación y redes.” ha ejecutado la implementación de un control de acceso por lector dactilar que permite guardar e identificar huellas dactilares, con un módulo dactilar que está programando con tecnología LFD (Live Finger Detection) para un único

registro de personas añadidas a la base de datos, aumentando la seguridad y exclusividad de acceso y salida del laboratorio y precautelando los elementos, datos y personal que contiene la instalación para su correcto uso. (MIRANDA, 2018)

El sistema de control de acceso es una de las grandes soluciones a la seguridad de empresas y lugares donde se desea limitar el acceso de personas particulares a zonas determinadas, salvaguardando la integridad de las instalaciones, la comodidad y la confiabilidad que ofrece. Este tipo de tecnologías permite verificar las actividades del personal que se encuentra en la base de datos del sistema de control acceso, de esa manera se monitorea en base a fechas y horas de entrada y salida.

1.2. Planteamiento del problema

Desde el 16 de junio de 1922, que el señor Presidente de la República, Dr. José Luis Tamayo, mediante Decreto, publicado en el Registro Oficial No. 521, de 20 de junio del mismo año, la Universidad de Fuerzas Armadas ESPE sede Latacunga se ha distinguido por formar profesionales e investigadores de excelencia siendo líderes en ciencia y tecnología, a través de los años la Universidad de Fuerzas Armadas ESPE-L a crecido físicamente sin embargo todavía es necesario realizar ciertas implementaciones a nivel de seguridad.

Desde la creación de la Universidad de Fuerzas Armadas ESPE con sede en Latacunga no existió una estructura tecnológica en referencia al control de acceso automatizado de salida y entrada de docentes que hacen uso del laboratorio de comunicaciones y de sus equipos tecnológicos, por lo cual genera un alto índice de inseguridad y vulnerabilidad de sus instalaciones.

La consecuencia de no existir un registro automatizado de personas que ingresan al laboratorio de comunicaciones generara pérdidas y daños de muebles, enseres y equipos tecnológicos de la instalación lo que lleva a un ambiente de

desconfianza y limitaciones para el uso del laboratorio por los diferentes tipos de informes de descargas para solucionar los problemas suscitados, de continuar con el problema se dificultaría el control por parte del encargado de la instalación, a los docentes autorizados que desarrollan actividades pedagógicas en el laboratorio de acuerdo a los horarios establecidos en el sistema académico y no se podrá precautelar la seguridad e integridad de los equipos tecnológicos que forman parte del laboratorio de comunicaciones.

1.3. Justificación

El sistema de control de acceso es un dispositivo tecnológico que proporciona verificación y monitoreo de fechas y horas de personal perteneciente al establecimiento donde es solicitado el control de seguridad.

Para la universidad de Fuerzas Armadas es muy importante la implementación de mecanismos tecnológicos que verifiquen y monitoreen los laboratorios de uso de docentes y estudiantes para garantizar un control de acceso a las instalaciones y permitan mejorar el aprendizaje y garantizando el desenvolvimiento de las tareas teóricas practicas relacionadas con la parte de redes y telecomunicaciones.

Con el control de acceso se garantiza el monitoreo de los usuarios que utilizan la instalación y así verificar daños o perdidas de acuerdo al personal que ha manipulado los equipos tecnológicos en concordancia con el horario establecidos por el departamento a que pertenece la carrera.

La implementación de este sistema de control acceso y video vigilancia tiene como fin identificar y registrar al personal de docentes autorizados a utilizar el laboratorio de comunicaciones, para precautelar la seguridad e integridad de los equipos tecnológicos existentes, asegurando y verificando el uso correcto de las instalaciones bajo el monitoreo de la persona custodio.

Los beneficiarios de este tema de investigación son la Universidad de Fuerzas Amadas, los docentes y estudiantes de las carreras del departamento que hacen uso del laboratorio de comunicaciones, precautelando los equipos tecnológicos para el mejor aprovechamiento del aprendizaje en la práctica con la manipulación los dispositivos tecnológicos que cuenta el laboratorio de comunicaciones.

1.4. Objetivos

1.4.1. Objetivo General

- Implementar un sistema de control de acceso y video vigilancia a través de una red LAN interna en el laboratorio de comunicaciones de la Universidad de Fuerzas Armadas sede Latacunga para precautelar la integridad de equipos Tecnológicos.

1.4.2. Objetivos Específicos

- Indagar los diferentes sistemas de control de acceso y circuito cerrado de televisión (cctv)y realizar un análisis comparativo para seleccionar la mejor alternativa que cumpla los requerimientos.
- Instalar el sistema de control de acceso y circuito cerrado de televisión (cctv) en el laboratorio de comunicaciones de la ESPEL
- Realizar pruebas de funcionamiento del sistema de control de acceso y circuito cerrado de televisión para garantizar su correcto funcionamiento.

1.5. Alcance

El presente proyecto abarcará la instalación de un sistema de control de acceso con tarjeta magnética que permita tener un registro del personal con el horario del ingreso a las instalaciones a través de una cerradura magnética y este sistema estará integrado a un circuito cerrado de televisión (CCTV) para mantener un registro visual de cualquier novedad que se pueda suscitar en las instalaciones el cual será accedido a través de una memoria microSD. La instalación del control de acceso en el laboratorio de comunicaciones de la universidad de fuerzas armadas ESPE brindara una mejor seguridad de las instalaciones y de equipos tecnológicos que reposan en su interior, controlando y verificando el acceso del personal de docentes y estudiantes de acuerdo a los horarios establecidos por el departamento a cargo para que pueda cumplir sus actividades pedagógicas, verificando el uso correcto de las instalaciones bajo el monitoreo de la persona custodio.

Capítulo II

2. Marco teórico

2.1. Historia de redes de computadora

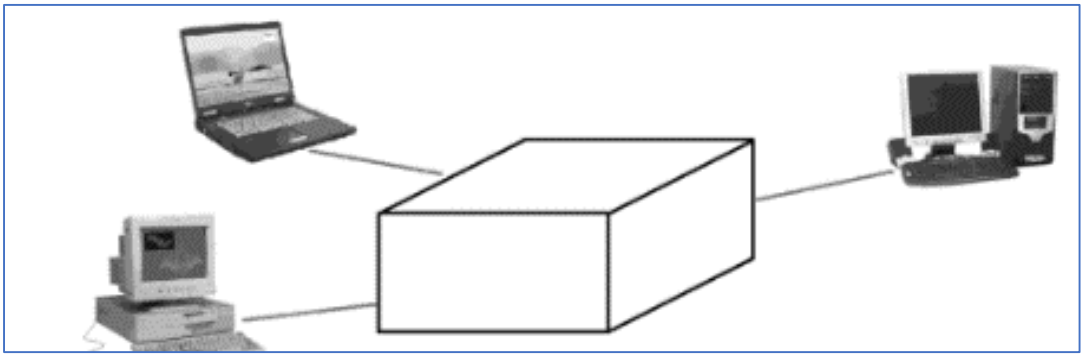
Dado los avances tecnológicos en la actualidad las redes de computadora han ido evolucionando en la mano con la informática en un ordenador o computador. La gran necesidad de recoger información ha ido cambiando su manera de transmitir y recibir el mensaje. Desde las cartas, redes telefónicas, radio y televisión hasta llegar a las redes informáticas, que se utilizaba en organizaciones, oficinas o lugares con la necesidad de compartir recursos. (Chávez, 2016).

Una red de computadoras brinda a los usuarios diferentes oportunidades en materia de software y el hardware. Las primeras redes de computadores fueron diseñadas pensando únicamente en los dispositivos dejando de lado a los programas, los cuales hoy en día componen el elemento principal de la red, puesto que brindan a los interesados gran diversidad en software. (Chávez, 2016).

La evolución se ha llevado a cabo en los últimos diez años y corresponde en mucho, al desarrollo de nuevas corrientes en la gestión de los Servicios Informáticos, el surgimiento de nuevos productos, tecnologías y a las nuevas utilidades que la computación y las redes presentan a la comunidad, las empresas y las instituciones en general. El uso intensivo de las redes de computadoras en todos los centros de educación superior en el país está sentando las bases para lograr cambios cualitativos significativos tanto en la gestión puramente académica como en el resto de los procesos sustantivos que se desarrollan en estos centros (Chávez, 2016).

Figura 1

Diagrama simple de una red de datos



Nota. En la figura se visualiza el diagrama de bloques de una comunicación entre los ordenadores. Tomado de (Chavéz, 2016).

2.2. Definición de redes

Según Douglas (1997), manifiesta que una red de computadoras “es una interconexión de computadoras para compartir información, recursos y servicios, esta conexión de sistemas informáticos puede darse a través de un enlace físico (alambrado) o inalámbrico” (pág. 3).

Algunos expertos afirman que una autentica red de computadoras se conforma por tres o más los dispositivos o computadoras que se encuentren conectadas. Tiene como objetivo conllevar recursos, haciendo que todos los programas, datos y equipos estén listos para la red que lo requiera, sin importar en qué lugar se encuentre el recurso y usuario. (Valdés, 2021)

El conjunto de herramientas que conforman la gestión de redes en su mayor parte son los de software, ya que son los programas, los que realizan la tarea de administración de la red. El hardware siendo también la parte fundamental se relaciona

con los dispositivos de red que se utilizan para administrar la red y todos los dispositivos que se unen a la misma. (Valdés, 2021)

2.3. Tipos de redes

De manera general las redes están conformadas por una serie de sistemas que tienen como fin compartir información, recurso, programas. Su clasificación se lo realiza en base al área de cobertura, la cual consta de 3 categorías:

- Extensión
- Topología
- Estructura

2.3.1. Red de área local (LAN)

Esta red posee un sistema de comunicación entre las computadoras cuyo fin es intercambiar la información, sin embargo, la distancia entre las computadoras debe ser pequeña. Generalmente son utilizadas para la interconexión de computadoras personales y en los lugares de trabajo cortos debido a su tamaño restringido. (Chávez, 2016)

Las redes de acceso, son de propiedad privada dentro de un solo edificio o campus de hasta unos cuantos metros de corta extensión. Se usan ampliamente para conectar computadoras con objeto de compartir recursos e intercambiar información, se distinguen de otro tipo de redes por tres características; tamaño, tecnología de transmisión y topología, estas utilizan una tecnología de transmisión que se trata de un cable sencillo al cual todas las máquinas están conectadas, la topología o la forma de conexión de la red depende de algunos aspectos como la distancia entre las computadoras y el medio de comunicación entre ellas ya que este determina la

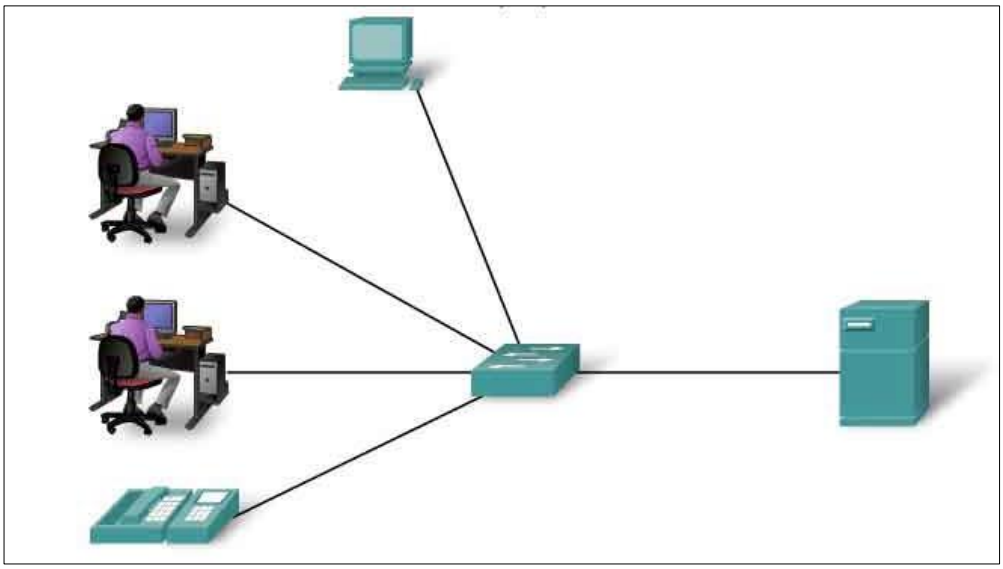
velocidad del sistema; Tradicionalmente operan a velocidades de 10 a 100 Mbps, y la transmisión puede ser variada; dos de ellas son bus y anillo. (Chávez, 2016)

Las siguientes características son las más comunes que poseen las redes LAN:

- Tiene un área limitada
- Transmiten desde 256 kb hasta más de 100 Mb por segundos.
- LAN exclusivamente para transmitir imágenes gráficas y de video.
- Son controladas, operadas y mantenidas por usuarios finales.
- Abaratan costos, comparten hardware y software.
- Promueven la productividad.
- Comparten igual información.

Figura 2

Diagrama simple de una red de datos LAN.



Nota. En la figura se puede observar un diagrama de bloques de una comunicación de una red LAN. Tomado de (Carate & Pozo, 2019).

2.3.2. Red de área metropolitana (MAN)

Este tipo de redes generalmente están localizadas en distancias no superiores al ámbito urbano, una MAN generalmente consta de una o más LAN dentro de un área geográfica común. Se utilizan para enlazar servicios urbanos tales como el control de tráfico y semáforos, servicios públicos como son: Internet inalámbrico, pagos municipales o televisión por cable o servicios privados entre los cuales están los servicios bancarios o comerciales. (Chávez, 2016)

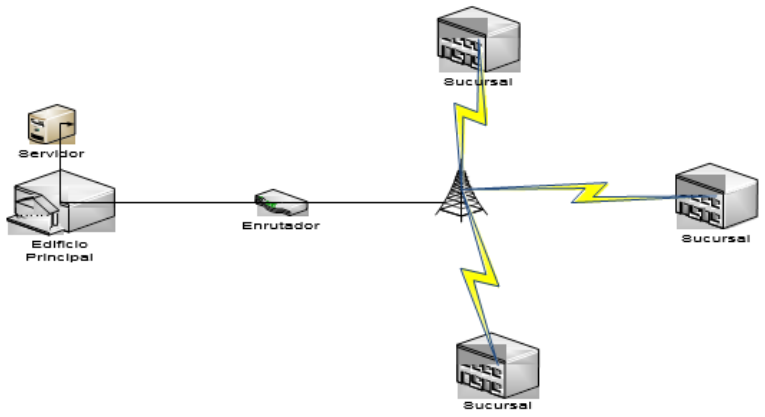
Para obtener un servicio MAN se utiliza un profesional en servicios de conexión para conectar dos o más sitios LAN, utilizando líneas privadas de comunicación o servicios ópticos. También se puede crear una MAN usando tecnologías de puente inalámbrico, enviando haces de luz a través de áreas públicas o mediante antenas de comunicación usando canales de comunicación privados. (Chávez, 2016)

Sus ventajas son:

- Facilita la comunicación entre edificios.
- Tiene la posibilidad de compartir información mediante bases de datos centralizadas en servidores.
- Reduce la duplicidad de trabajos
- Puede generar progresos en lo que se refiere a la seguridad y control de la información.

Figura 3

Red de área metropolitana (MAN).



Nota. En la figura se puede observar un diagrama de bloques de una comunicación de una red MAN. Tomado de (Chávez, 2016).

2.3.3. Redes privadas virtuales (VPN)

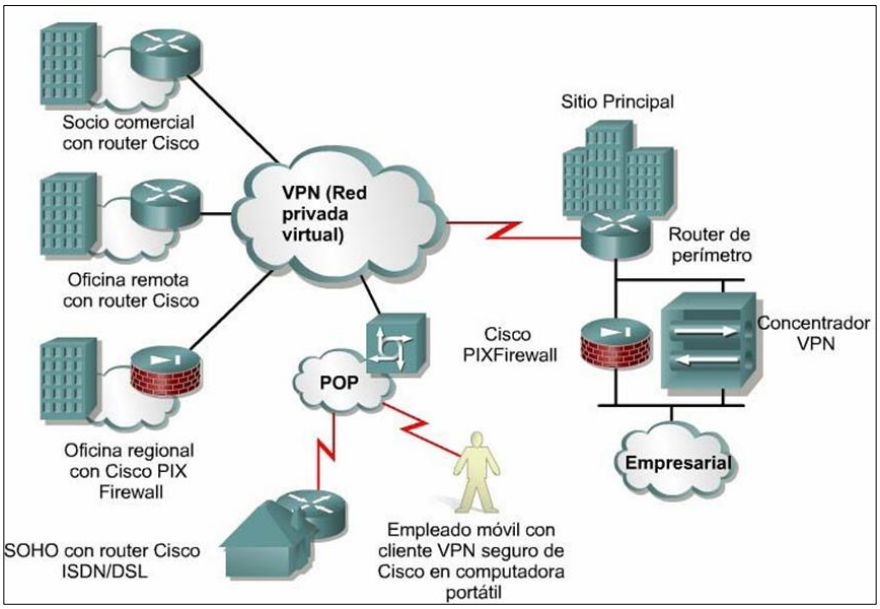
Como López (2018) expresa es su texto:

Una VPN es una red privada que se crea dentro de una base de red pública, como la Internet global. Con una VPN, un usuario a distancia puede tener acceso a la red del sitio de la empresa a través de Internet, creando un túnel seguro entre el PC del usuario y un router VPN en el sito (pág. 5).

La VPN ofrece un servicio de conectividad segura y confiable en una infraestructura de red pública compartida, como la Internet. Las VPN y una red privada mantienen las mismas políticas de seguridad y administración. Son la manera más económica de crear una conexión punto-a-punto entre clientes remotos y la red de un cliente de la empresa (López, 2018, pág. 5).

Figura 4

Redes privadas virtuales (VPN)



Nota. En la figura se visualiza el diagrama de bloques de una comunicación de una red privada virtual. Tomado de (López, 2018)**.**

Entre los VPN se cuenta con 3 tipos:

- **VPN de acceso:** Se trata de usuarios que se conectan a una empresa desde lugares remotos usando Internet como vínculo de acceso. Luego de ser autenticados tienen un nivel de ingreso igual a estar dentro de la red local. (López, 2018)

Esta clase de VPN ofrece un acceso remoto a un operario móvil y una oficina pequeña, al sitio de la red interna o externa, a través de una infraestructura compartida.

Ocupan una tecnología analógica, de acceso telefónico, RDSI, línea de suscripción digital (DSL), IP móvil y de cable para ofrecer un método seguro de conexión.

- **Redes internas VPN**: Estas redes vinculan a las sucursales regionales y remotas haca el sitio de la red interna a través de una infraestructura compartida, ocupando conexiones dedicadas. Las redes internas VPN permiten nada más el acceso a trabajadores de la empresa. (López, 2018)
- **Redes externas VPN:** Estas redes conectan a usuarios comerciales a el sitio de la red a través de una infraestructura compartida, ocupando conexiones dedicadas. Cabe mencionar que para López (2018) “Las redes externas VPN permite el acceso a socio que no pertenecen a la empresa” (pág. 7).

2.3.4. Red de área amplia (WAN)

Este tipo de red a diferencia de las otras se extiende sobre un área geográfica extensa, puede encontrarse distribuido un país o un contienen; tiene una serie de máquinas que se dedican a ejecutar programas de usuario (aplicación) a los que se les se les llama host. Estos se conectan por una subred y su trabajo es conducir mensajes de una host a otra. La separación entre los aspectos de comunicación de la red (la subred) y los aspectos de aplicación (Hosts), facilita el diseño total de la red. Las líneas de transmisión se conocen como circuitos los cuales son encargados de mover los bits de una máquina hacia otra, los elementos de cambio son PC especializadas que se encargan de conectan dos o más líneas de transmisión al momento que los datos ingresan por la línea de entrada, el elemento de conmutación debe elegir una línea de salida para enviarlos como término genérico para las computadoras de conmutación, a los cuales se les llamara enrutadores. (Chávez, 2016, pág. 5).

2.4. Funciones de administración de redes

Un administrador de red sirve a los usuarios: crea espacios de comunicación, atiende sugerencias; tiene las herramientas y el espacio necesario para cada uno de los

usuarios, a tiempo y de manera correcta (si usted fuera usuario como quisiera que fuera el administrador); tiene en correcto estado el hardware y el software de los computadores y la(s) red(es) a su cargo; tiene el archivo que describe la red, el hardware y el software que maneja; respetando la privacidad de los usuarios y promoviendo el buen uso de todos los recursos. La recompensa por el cambio de tantas responsabilidades es el correcto funcionamiento de la esta red como un medio que enlaza personas y de los computadores y programas como herramientas para aligerar ciertas labores que dan tiempo para trabajar otras. (Manuel, 2016).

2.5. Monitoreo

El monitoreo de red es una acción que se realiza con el fin de obtener información efectuada entre una computadora y una red, puede ser de área local o externa, o de área amplia. De igual manera, pueden mostrar desde qué PC están conectadas, identificando sus direcciones IP y la cantidad de información que recorre por medio de una red, así también, las conexiones realizadas en ciertas redes. Toda esta información recolectada se utiliza para el control general de cómo funciona la red desde una visión completa. Un correcto monitoreo de red debe ser de fácil instalación y utilización para el usuario que no está especializado, de tal manera que la asesoría o capacitación sea mínima o, incluso, no necesaria. (Salas, 2020, pág. 10).

2.6. Fallas

Según Machado (2016)) para tener éxito en las labores diaria “el administrador de red debe identificar y solucionar los problemas que se presenten con la red, es muy importante establecer las medidas de prevención y que corrijan con anticipación, por lo que deberá tener un adecuado plan de contingencia” (Machado, 2016, pág. 15).

Tiene como objetivo la detección, registro, notificación a los usuarios, en caso de ser posible, solucionar los problemas de la red de manera automática, con el propósito de tener el correcto funcionamiento de la red.

Envuelve los siguientes pasos:

- Determina los síntomas del problema.
- Aísla el problema.
- Soluciona el problema.
- Demuestra la reparación en todos los subsistemas que son muy importantes.
- Graba la detección del problema y la resolución.

2.7. Control de acceso

Se ejecuta entre la entidad administradora y las personas. Su principal fin es la generar un sistema que impida que el personal no encargado o sin identificación previa pueda ingresar a una zona sin autorización. Entre los tipos de control de acceso tenemos los siguientes:

- Según el sistema de identificación
- Según el tipo de conexión

2.8. Tipos de control de acceso según el sistema de identificación

El sistema de control de acceso tiene las siguientes tres funciones principales:

- La autenticación la cual permite identificar personas o vehículos que desean acceder a una zona privada.
- La autorización la cual gracias al software del sistema trabaja en las comprobaciones y envía la disposición de abrir o no un acceso.

- La trazabilidad la cual permite obtener listados de las personas que están presentes en un lugar.

2.8.1. Sistema de proximidad

Este sistema permite utilizar tarjetas u otros objetos que al acercarlos al terminal comienza la autenticación. En este control de acceso se debe destacar la tecnología innovadora RFID, qué a más de ofrecer alta seguridad, es precisa, fiable y tiene una gran capacidad para almacenar datos. (Spec, 2017, pág. 10)

2.8.2. Sistemas biométricos

Es sistema biométrico es el que está basado en la identificación por medio del reconocimiento de una característica física de una persona que requiere el acceso para que sea verificada de manera instantánea y automática. Este sistema es el más utilizado en las empresas y su uso se lo realiza especialmente en el lector de huella digital, la cual cuenta con muchas ventajas para evitar la suplantación de identidad, terminar con las dificultades de olvido de tarjetas, además es un sistema muy sencillo y totalmente eficaz. (Spec, 2017)

Este es el ámbito en donde la tecnología está evolucionando: y estamos dejando de lado las manos por tal motivo buscamos un libre acceso a través del reconocimiento de la huella dactilar, del iris, del rostro o de nuestra mano. Además, considerando que olvidamos tarjetas, códigos y contraseñas que nos sirven para abrir puertas, podemos valemos de ciertos rasgos humanos que siempre los llevamos con nosotros, garantizando así el ingreso único y personal. Para el reconocimiento por iris, será suficiente con acercar uno de nuestros ojos a 35 centímetros del lector para que este identifique nuestro iris y nos permitiera ingresar, todo esto con la comodidad y facilidad de no utilizar las manos para nada. (Spec, 2017, pág. 20)

2.8.3. Sistemas de reconocimiento de matrícula o TAG

Sistemas de reconocimiento de matrícula: se encargan de “controlar el ingreso a través de la identificación de la persona, del vehículo o de ambas. Los vehículos se pueden identificar por tarjeta/TAG o por lectura de la matrícula”. (Spec, 2017)

2.9. Tipos de control de acceso según la conexión

Para cumplir con las funciones que se necesita los tipos de control de acceso según la conexión pueden ser: Sistemas de accesos autónomos o sistemas de acceso en red.

2.9.1. Sistema de acceso autónomo

Para este sistema no es necesario ningún tipo de conexión, ya que los propios terminales tienen una memoria para la gestión de los usuarios. Este es cosiderado un sistema de baja seguridad y capacidad limitada.

2.9.2. Sistema de acceso en red

Son aquellos que utilizan herramientas como los softwares de control de acceso y ofrecen una seguridad en alto nivel. Se puede controlar infinitas zonas diferentes de la empresa a la vez, acotar los accesos por distintos horarios y permisos, también cuentan con la ventaja que pueden abarcar otras importantes soluciones para todas las empresas como: control horario, de visitas, planes de evacuación y emergencias (Spec, 2017, pág. 6).

2.10. Definiciones y conceptos básicos sobre RFID

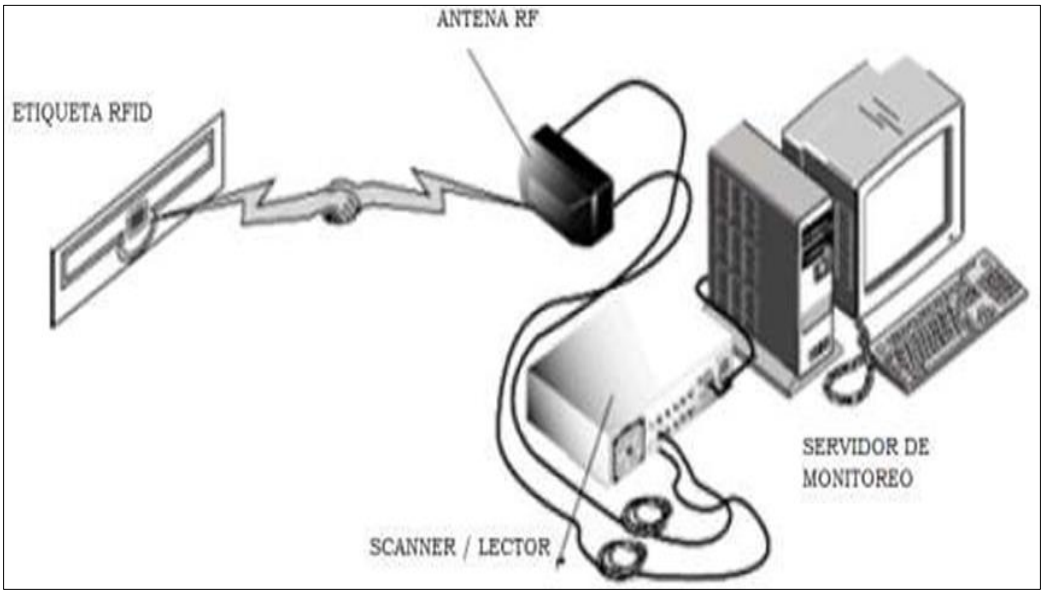
El RFID, “Radio *Frequency Identification” (Identificación* por radio frecuencia), tiene una tecnología que captura datos, en su esencia es muy similar al sistema de código de barras, pero no utiliza un código impreso en lugar de este, utiliza un microchip y un circuito impreso a modo de antena dentro del cual se almacena el código alfa

numérico, capaz de suplantar el actual sistema para leer la etiqueta de código de barras ante un lector. (Chang, 2018, pág. 24)

Así, para este tema podemos mencionar que: “La distancia del código depende de qué capacidad tiene el microchip para almacenar, la etiqueta se une al equipo que se desea inventariar, y se pueden utilizar para rastrearlos a distancia, que facilita el control y mecanización de la logística para monitorizar el producto”. (Chang, 2018, pág. 24).

Figura 5

Sistema RFID.



Nota. En la figura se puede observar el diagrama de sistema básico RFID. Tomado de (Chang, 2018).

2.10.1. Elementos que conforman el sistema RFID

Entre los principales elementos básicos de un sistema RFID tenemos el transmisor y receptor, el transmisor corresponde a las etiquetas y el receptor a las antenas/lector.

Además de estos elementos, se requiere una interface visual y amigable con un usuario, el transponder es un componente pasivo que está compuesto por un chip el cual viene integrado una antena y el lector está compuesto de un circuito y este emite la energía electromagnética por medio de la antena y una electrónica que se encarga de recoger y descodificar la información enviada al transponder. (Chang, 2018, pág. 25).

2.10.2. Etiquetas o TAGS RFID

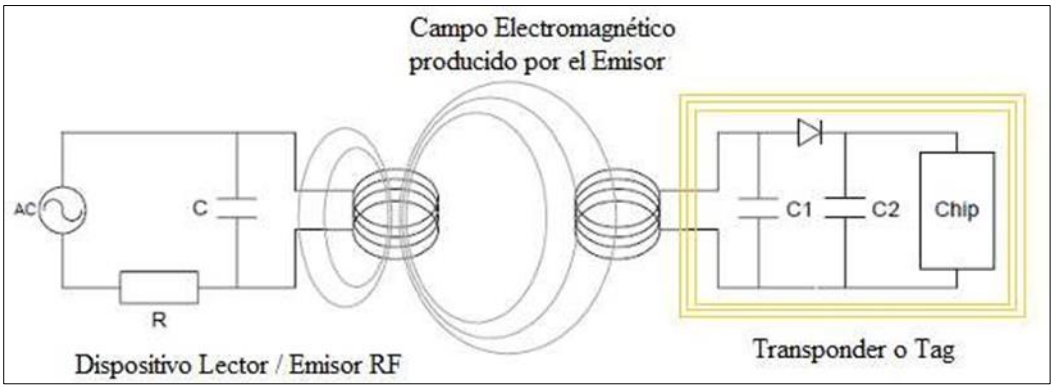
La etiqueta RFID es un chip inmerso en una antena a modo de embalaje laminado, y según su aplicación, lugar o ambiente donde van a ser instalados o el tipo de material al que se van a pegar, puede variar en su composición el material externo, es decir que su diseño va a cambiar según el ambiente, y tienen la capacidad para resistir el agua, cambios de temperatura, polvo, entre otros. La etiqueta tiene la función de transmisión y recepción o “transmitter/response” por eso se le da el nombre de transponder. (Chang, 2018, pág. 25).

Está compuesto por:

1) De 3 tipos de memoria (chip):
   - No volátil, se almacenan los datos del producto
   - ROM, se almacena la programación propia del chip
   - RAM, durante la comunicación con el lector se encarga de almacenar datos
2) Antena bobinada sirve como alimentación para el chip.
3) Componentes electrónicos, buffers, filtros.

Figura 6

Transmisión inductiva de energía.



Nota. En la figura se observa el diagrama de transmisión inductivo de energía. Tomado de (Chang, 2018).

Los microchips RFID trabajan con radio frecuencia, esto significa que trasfieren datos en una longitud de onda específica. Para que un sistema RFID funcione correctamente, se necesita tener una lectora que lea la frecuencia específica de un microchip, es decir, si se utiliza los microchips de 125 KHz, debe haber lectores de 125 KHz y a su vez entiendan el tipo de codificación tiene dicho microchip. (Chang, 2018, pág. 26).

2.10.3. Readers lectores RFID

Los lectores RFID tienen como función alimentar los tags y etiquetas por medio de las antenas a través de la emisión de una señal de radio frecuencia, y al mismo instante capturan datos que son enviados por los tags para ser decodificados e interpretados por el software que corresponde.(Chang, 2018, pág. 27).

El objetivo de los lectores es transmitir y receptar señales además convertir las ondas de radio que son emitidas por los tags en un formato que pueda reconocer la computadora.

Entre los tipos de lectores se tiene:

1) Lectores Fijos
2) Lectores portátiles o manuales
3) Lectores de mesa USB
4) Lectores de carretilla

Figura 7

Varios tipos de lectores RFID.

Nota. En la figura se observa distintos tipos de lectores RFID. Tomado de (Chang, 2018).

Para los lectores fijos se necesita de antenas para que pueda generar la onda que llega a los tags, de igual manera la onda de respuesta es leída mediante estas antenas. Los lectores portátiles ofrecen una forma manual la captura de datos una sola vez y con mayor rapidez comparado con un tradicional código de barras, son muy fiables. Los lectores de mesa o USB, están fabricados para aplicaciones más sencillas y fáciles es decir no requieren grandes lecturas de gran importancia o de grandes prestaciones (Chang, 2018, pág. 29).

2.11. Software de enlace

Para implementar el sistema RFID, se requiere una plataforma de software para la captura y gestión inteligente de datos. El software tiene la capacidad de controlar en tiempo real los movimientos que se descubre a través del lector. Luego que el lector obtiene la información dada por los tags, estos datos se envían a un programa para interpretar y traducir a un lenguaje amigable para las personas. (Chang, 2018)

2.12. Sistema de video de vigilancia

Según Araujo, (2018) en la actualidad los sistemas de video vigilancia han sido muy populares en empresas y en los hogares que han solicitado este servicio, ya que son instalados en lugares internos o externos teniendo como objetivo dar un mayor control del área que se quiere monitorear y observar que está ocurriendo en tiempo real o de manera remota mediante el Internet. Estos sistemas son capaces de crear un efecto persuasivo, al ser vistas por las personas ya que impide cualquier acto antisocial (Muñoz, 2018, pág. 35).

2.12.1. Sistemas Analógicos

De acuerdo con Araujo (2018):

El sistema que se utiliza es el Circuito Cerrado de Televisión CCTV ANALÓGICO, que tiene varios dispositivos como monitores analógicos, grabadores analógicos, cámaras analógicas entre otros componentes analógicos en los que se encuentra diferentes fabricantes y con mayor variedad. Las cámaras de los CCTV analógicos, tienen salidas de video compuesto, estas van conectadas a un cableado que se usa solo para esta instalación, y son visualizados en uno o varios monitores, cuyo objetivo es observar las imágenes de las cámaras que están conectadas. Para la gestión de las cámaras CCTV analógico hacia los monitores se usan unas matrices de

video que trasladan el video a través de microprocesadores las entradas o cámaras hacia las salidas o monitores (pág. 36).

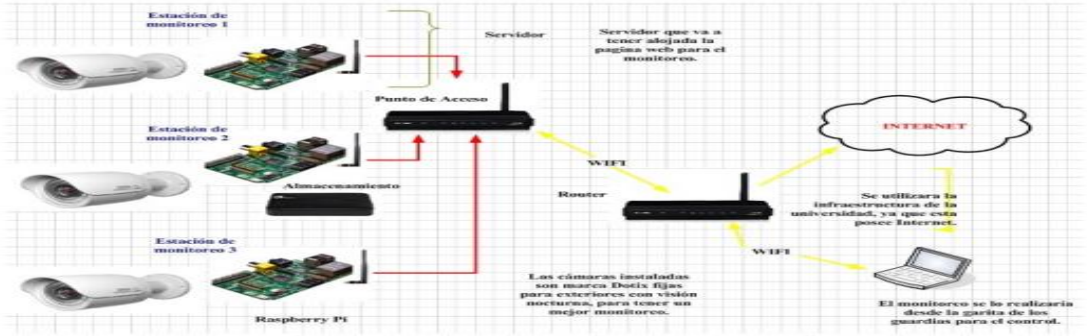
2.12.2. Sistemas Digital TCP/IP

De acuerdo con Araujo (2018) :

La comunicación se basa mediante el protocolo TCP/IP, donde las cámaras se encuentran conectadas directamente a la misma red de computadores que existiera en el lugar donde van a ser instaladas. La transmisión de video desde la cámara o el servidor puede observarse dentro de la misma red local o a través del internet. Para poder observar las imágenes desde internet se puede utilizar el servidor web o ftp, visualizar el streaming de video a través de una página web que está instalado en un servidor o depende del modelo de la cámara se podrá acceder a ellas mediante la intranet del lugar. Este tipo de sistemas crecen demasiado rápido por su funcionalidad, versatilidad, escalabilidad y gran facilidad para la incorporación de tecnologías ya existentes (pág. 37).

Figura 8

Esquema básico de un sistema de vigilancia.



Nota. En la figura se observa el esquema de un sistema de vigilancia. Tomado de (Muñoz, 2018).

2.13. Tipos de cámaras

Como Ortega (2019) menciona su texto:

Si el sistema de vigilancia por vídeo que se va a instalar es un sistema nuevo y no existe ninguna cámara analógica, la mejor alternativa en la mayoría de los casos es usar cámaras IP, que estén disponibles en diferentes modelos y satisfagan una gran variedad de necesidades del ser humano. Con esta variedad de cámaras IP que se cuenta en la actualidad, se logra la mayoría de las exigencias de todos los mercados verticales y tamaños del sistema. Las cámaras IP se presentan en diferentes modelos: Cámaras IP fijas, cámaras IP domo fijas, cámaras IP PTZ, cámaras IP domo, cámaras IP PTZ no mecánicas (pág. 10).

Entre los tipos de cámaras se encuentran diversas variaciones:

- Versiones a prueba de agresiones, en función de la carcasa de protección que se use.
- Versiones resistentes a las condiciones climáticas, en función de la carcasa de protección que se use.
- Versiones de visión diurna/nocturna, lo que significa que la cámara puede cambiar automática o manualmente entre modo diurno con video en color y modo nocturno con imágenes en blanco y negro.

2.14. Clasificación de cámaras

2.14.1. Cámara de red fija

Cuando se necesita de enfocar directamente y que la cámara se pueda ver claramente y sea visible se requiere de este tipo de cámaras y que el ángulo se queda fijo una que vez que la cámara ya está instalada, la cámara se encuentra en la Fig. 9

Figura 9

Cámara de red fija

Nota. Es una cámara de enfoque directo. Tomado de (Muñoz, 2018)**.**

2.14.2. Cámara de red fija tipo domo

La cámara de red es una cámara fija preinstalada en una pequeña carcasa domo como se observa en la figura página 27. La cámara se puede dirigir en cualquier dirección. La diferencia está en la dificultad para visualizar hacia qué dirección apunta la cámara según su diseño. Una de las restricciones de una cámara domo fija está en que muy rara vez tiene una lente intercambiable. La instalación de una de estas cámaras es generalmente en una pared o en el techo. (Muñoz, 2018)

Figura 10

Cámara De Red Fija Tipo Domo

Nota. Es una cámara de enfoque de 360º. Tomado de (Muñoz, 2018)**.**

2.14.3. Cámara de red PTZ^3:

Estas cámaras tienen la capacidad de girar alrededor de los ejes vertical y horizontal, así como acercarse y alejarse de la manera como se puede apreciar en la figura pagina 28, el sistema de manipulación es de forma manual en el cual un operador puede utilizar una cámara PTZ para seguir a un ente especifico, se utilizan en interiores, tiene de un zoom óptico de las cámaras PTC usualmente manera un rango de 10X a 26X. (Muñoz, 2018)

Figura 11

Cámara de red PTZ^3

Nota. Es una cámara con capacidad de rotar alrededor de los ejes vertical y horizontal Tomado de (Muñoz, 2018)**.**

2.14.4. Cámara de red PTZ no mecánica.

La cámara de red PTZ mecánica se puede utilizar principalmente en lugares interiores y en aplicaciones donde se emplean un operador. El zoom óptico en cámaras PTZ varía entre 10x y 26x. Una cámara PTZ se puede ser instalada en el techo o pared. (Muñoz, 2018)

Figura 12

Cámara de red PTZ no mecánica

Nota. Es una cámara que se utiliza para interiores Tomado de (Muñoz, 2018)**.**

2.14.5. Cámara de red domo PTZ (Pan-Tilt-Zoom)

Tiene una mayor cobertura ya que su diseño permite girar 360 grados y una inclinación que puede ser de 180 grados como se muestra en la figura página 29. Este tipo de cámaras de domo son perfectas para el uso en instalaciones reservadas. Puede cubrir un área que equivale a diez cámaras fijas, pero solamente una ubicación puede ser monitorizada en cualquier momento, dejando las demás posiciones sin control. (Muñoz, 2018)

Figura 13

Cámara de red domo PTZ (Pan-Tilt-Zoom)

Nota. Es una cámara que permite un giro 360 grados y una inclinación que suele ser de 180 grados. Tomado de (Muñoz, 2018)**.**

Capítulo III

3. Desarrollo del tema

En el presente proyecto se desarrolló una investigación de carácter descriptivo la cual se llevará a cabo en la Universidad de Fuerzas Armadas sede Latacunga, para la recepción de información es necesaria la obtención de datos. De acuerdo a la metodología por tratarse de un proyecto investigativo se determinó la siguiente documentación.

En la Universidad de Fuerzas Armadas sede Latacunga se implementa un sistema de control de acceso y video vigilancia a través de una red LAN interna en el laboratorio de comunicaciones de la Universidad de Fuerzas Armadas sede Latacunga para precautelar la integridad de equipos Tecnológicos. El sistema va a tener una funcionabilidad de las 24 horas día y noche para aumentar el nivel de seguridad.

El sistema de control de acceso permite el ingreso del personal mediante una tarjeta magnética la misma que será otorgada solo a la persona que este registrado dentro de la Institución, de tal manera en el caso de ingresar personal no autorizado existe una cámara de video vigilancia que es una ventaja del sistema que se encuentra implementado. Mediante una aplicación móvil para (celular, tables, etc.), la cámara podrá ser monitoreada en tiempo real ya que cuenta con una red de conexión (WI-FI), también cuenta con un respaldo de las grabaciones hechas que podrán ser vistas localmente.

En este capítulo puntualizara todo el procedimiento para el desarrollo e instalación del sistema de control y video vigilancia, tanto de hardware como el software a ser implementado. En la primera parte se analiza el esquema a ser utilizado como el área a monitorear y la ubicación escogida para la cámara y el control de acceso. En el

hardware, el detalle de las especificaciones técnicas para cumplir con los objetivos del sistema.

Para la parte del software se dan detalles de cuál fue el sistema operativo instalado como línea de base que parte todo el sistema, aplicaciones utilizadas, la explicación de la interface entre el usuario y el sistema, la comunicación entre el control de acceso. Posteriormente, la instalación de todo el sistema en los puntos estratégicamente seleccionados.

3.1. Tipo de investigación

3.1.1. De campo

Se utilizará la investigación de campo en el transcurso de recopilación de datos existentes en la Universidad de Fuerzas Armadas sede Latacunga, y será utilizada para determinar el mejor sistema de control de acceso y video vigilancia. El levantamiento de la información a través de la observación in situ, lo cual fue útil en el desarrollo del proyecto de investigación, como investigador aportare a la investigación de campo para precautelar la integridad de equipos Tecnológicos.

3.1.2. Bibliografía

Este método se refiere a la recolección de información necesaria para el desarrollo de la investigación, analizar las características de cada sistema de control de acceso y video vigilancia, con lo cual se pueda elaborar y sustentar teóricamente el trabajo investigativo.

3.2. Métodos

3.2.1. Científico

El método científico será aplicado para desarrollar un conjunto de pasos ordenados para hallar nuevos conocimientos en relación a los sistemas de control de acceso y video vigilancia.

3.3. Técnicas

3.3.1. Medición

Por medio de la técnica de medición permite determinar el tipo de conexión, la cual se adecue a los sistemas de control de acceso y video vigilancia y den como resultado la comunicación entre ordenador y sistema en tiempo real, dependiendo de la configuración a CCTV.

3.4. Software para la simulación

Para diseñar y modelar es necesario contar con softwares que aporten al estudio del análisis de los circuitos cerrados de televisión (CCTV), y sistemas de conexión inalámbricas (WI-FI).

3.5. Esquema del Proyecto

3.5.1. Área de instalación

En la Figura 14, se determina el lugar acorde a la necesidad tomada en el Laboratorio de comunicaciones en la Universidad de Fuerzas Armadas sede Latacunga.

Figura 14

Laboratorio de comunicaciones en la Universidad de Fuerzas Armadas sede Latacunga

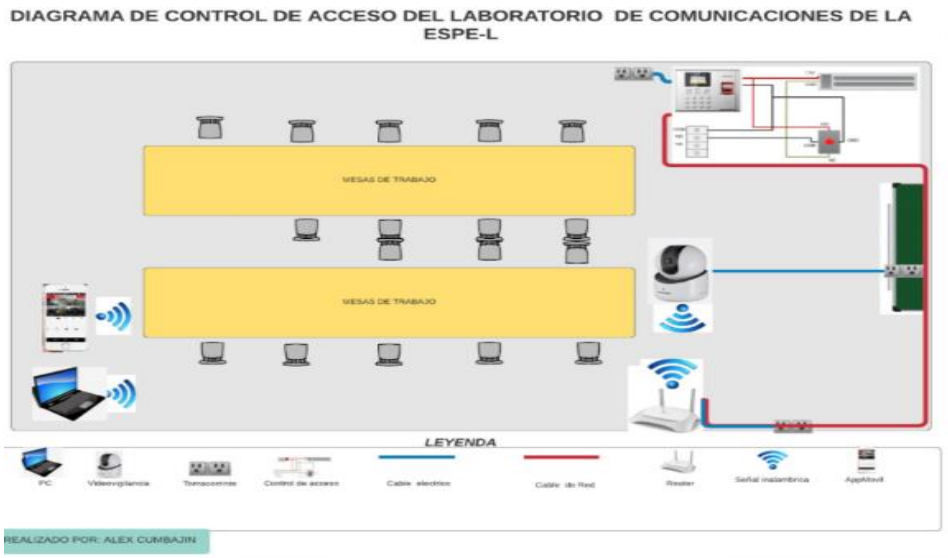
Nota. Es una cámara que permite un giro 360 grados y una inclinación que suele ser de 180 grados.

3.5.2. Diagramas técnicos del proyecto.

En esta sección se precisa el esquema del sistema de control y video vigilancia completo.

Figura 15

Diagrama de conexión



Nota. Diagrama de la red de control de acceso y video vigilancia.

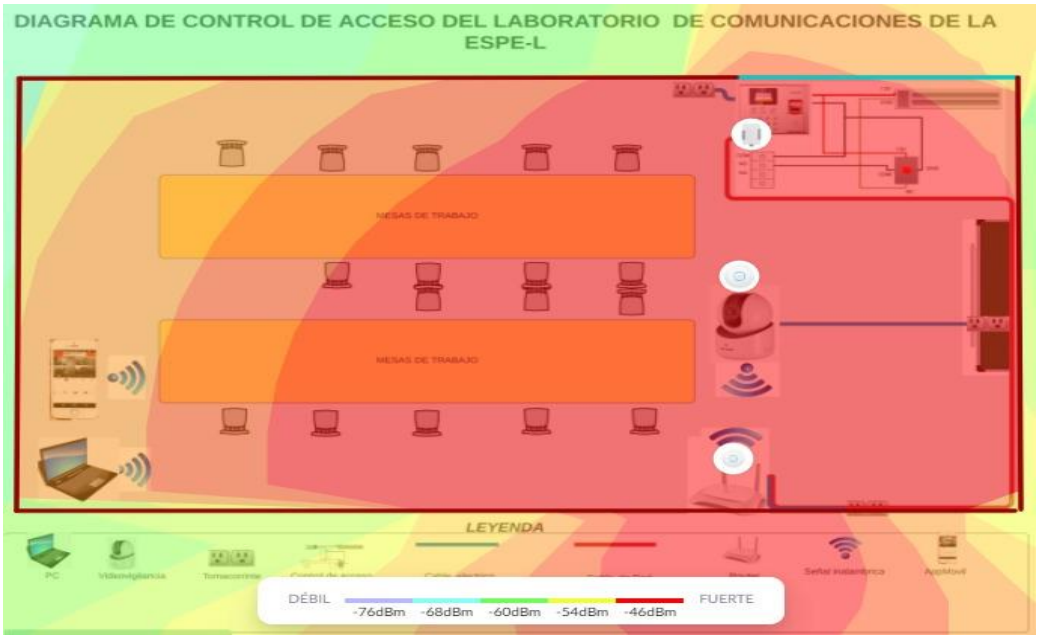
Diagrama técnico del proyecto. Conexión de las partes principales del proyecto

El esquema mostrado en la parte superior detalla los instrumentos principales, dispositivos de conexión para la transmisión de datos que serían utilizados para el proceso de implementación del sistema de control y video vigilancia.

En la figura 16 se muestra el diagrama de calor donde se visualiza el alcance inalámbrico de la cámara IP (wi-fi), y el router inalámbrico en donde podemos constatar que el color rojo que es la intensidad de la señal inalámbrica trabajando a una frecuencia de 2.4 GHz.

Figura 16

Diagrama de calor



Nota. Diagrama de calor de conexiones inalámbricas realiza en el programa Unifi Design Center.

3.6. Fichas técnicas para la selección de los equipos

La investigación de campo permitió establecer las ventajas y desventajas de trabajar con un sistema de control de acceso y circuito cerrado de televisión (cctv) en un área determinada con restricciones de personal, se establece tablas comparativas para la selección de los equipos adecuados según sus características técnicas que cumplirán con los requerimientos específicos dc control de acceso, asistencia y verificación de imagen con una cámara de seguridad, los cuales serán detallados en la tabla 1 y 2 a continuación:

Tabla 1

Tabla comparativa de controles de acceso

Marcas y nombres de controles de acceso

Características técnicas	HIKVISION / DS-K1T8003EF	ZKTECO / MB20-VL	ZKTECO/ProCapture-T	ZKTECO/ MA500
Pantalla	LCD-TFT display screen 2.4-inch	TFT de 2.8 Pulgadas	TFT-LCD de 2.4"	-
Capacidad de Rostros	-	100	3.000	-
Capacidad de Huellas	1,000	500	6.000	3,000
Capacidad de Tarjetas	1,000	-	10.000	30,000
Capacidad de Eventos	100,000	50,000	100.000	100,000

Marcas y nombres de controles de acceso

Comunicación	TCP/IP, USB Host	TCP/IP, USB Host	TCP/IP,RS485 (Lector Esclavo), USB-Host	TCP/IP y RS485
Funciones Estándar	• Generar reportes de asistencia software IVMS4200 o USB en formato Excel. • Con Hik-Connect es posible apertura de la puerta momentáneamente, dejarla abierta, cerrarla y monitorear si se encuentra abierta o cerrada.	ADMS, DST, consulta de autoservicio, cambio de estado automático, entrada T9, cámara, 9 dígitos ID de usuario, múltiples métodos de verificación.	• Niveles y Grupos de Acceso / Días Festivos • Horario de Verano / Timbre Programado • Modo de Coacción • Anti-Passback • Búsqueda de Eventos • Protector y Fondo de Pantalla Personalizable	Tarjeta EM
Fuente de Alimentacion	12 VDC/1 A	5V/2A	12V / 500mA	12VCD/3 A
Métodos de Verificación	Huella / Tarjeta / Contraseña	Rostro / Huella digital	Huella / Tarjeta / Contraseña /Rostro	Huella / Tarjeta

Marcas y nombres de controles de acceso

Interfaz de Control de Acceso	1 relé (salida de bloqueo), 1salida de timbre, 1 botón de salida, 1 contacto de puerta	Cerradura eléctrica, sensor de puerta, botón de salida	Relevador para Cerradura Salida de Alarma / Entrada Auxiliar Botón de Salida / Sensor de Puerta Salida para Timbre	Cerradura Eléctrica, Sensor de Puerta, Botón de Salida y Alarma

Nota: La tabla muestra la comparación de los sistemas de control con sus respectivas características técnicas.

Tabla 2

Tabla comparativa de cámaras de video vigilancia

Marcas y nombres de cámaras de video vigilancia

Características técnicas	HIKVISION / DS-2CV2Q21FD-IW	IMOU / IPC-F22FEP	AXIS / M1065-LW
Resolución	1920 × 1080	1920 x 1080	1920x1080
Tipo De Lente	PTZ digital	Lente fija	PTZ digital

Marcas y nombres de cámaras de video vigilancia

Distancia Focal Y Campo de Visión	2,8 mm, campo de visión horizontal 105,8°	2,8 mm; 108 ° (H), 56 ° (V), 128 ° (D)	2,8 mm, Campo de visión horizontal: 110° Campo de visión vertical: 61°
Suplemento Tipo De Luz	infrarrojos	infrarrojos	infrarrojos
Almacenamiento En Red	Admite tarjeta Micro SD/SDHC/SDXC, hasta 128 GB de almacenamiento local	Admite NVR, almacenamiento en la nube o tarjeta Micro SD (hasta 256 GB)	Compatible con tarjetas microSD/microSDHC/microSDXC Compatible con grabación en almacenamiento en red (NAS)
conexión Wi-fi	Si	SI	SI
Protocolo Wifi	802.11b: CCK, QPSK, BPSK, 802.11g/n: OFDM	IEEE802.11b / g / n (2,4 GHz)	IEEE 802.11a/b/g/n 2,4 GHz, a 5,2 GHz
Alcance Inalámbrico	50 metros (el rendimiento varía según el entorno real)	30 metros	50 metros (el rendimiento varía según el entorno real)

Marcas y nombres de cámaras de video vigilancia

Evento Básico	Detección de movimiento, alarma de manipulación de video, excepción (disco duro lleno, error de disco duro, red desconectada, dirección IP en conflicto, inicio de sesión ilegal)	Ahuyenta a los visitantes no deseados con un foco integrado y una sirena de seguridad de 110 dB.	Grabación de vídeo y audio en almacenamiento local, activación de LED-IR, reproducción de clips de audio, superposición de texto Memoria de vídeo previa y posterior a la alarma
Energía	CC 5 V ± 10 %, máx. 1,4 A, máx. 7 W, interfaz micro USB	12V / 1A	4,75–5,25 V CC, 2,7 W típicos, 5,0 W máx

Nota: esta tabla muestra la comparación de los cámaras de video vigilancia con sus respectivas características técnicas.

En el análisis de las tablas de comparación se consideró 6 dispositivos 3 para el control de acceso y 3 para el circuito cerrado de televisión de diferente marca y modelo que proporciona diferentes características técnicas para la adecuada selección de los dispositivos acorde a la necesidad y planteamiento del proyecto.

Para la selección de los dispositivos que se utilizara en el proyecto se toma en cuenta la capacidad de eventos y registros en el control de acceso y en la disponibilidad, fácil acceso y manipulación inalámbrica de la cámara de seguridad, en la tabla comparativa del sistema de control de acceso se seleccionó el dispositivo HIKVISION / DS-K1T8003EF el cual cuenta con la capacidad de eventos de 100.000 y la capacidad de huellas y tarjetas de 1.000 cada una, en la tabla comparativa de cámaras de seguridad se seleccionó el equipo de video vigilancia HIKVISION / DS-2CV2Q21FD-IW el cual cuenta con conexión inalámbrica y manipulación a través de un control PTZ, conjuntamente los dos dispositivos pueden trabajar en un solo software libre de la mara HIKVISON iVSM 4200 para su registro y monitoreo en un ordenador, acorde a esto se realizó la instalación correspondiente con los equipos necesarios para su respectivo funcionamiento dentro de la institución con las pruebas correspondientes.

En el proceso de la instalación del proyecto, la Institución aporto con el router de la figura 17 de marca LINKSYS SMmart Wi-fi, modelo EA6900, nombre Linksys 21959, que trabaja en un rango de frecuencia de 2,4 Ghz y 5 GHz.

Al contar con un rotuter se establece una tabla de enrutamiento con la dirección IP que está establecida en el dispositivo que consta como 192.168.1.110 al partir de la IP asignada se fijan los demás dispositivos como se detalla en la en la siguiente tabla:

Tabla 3

Tabla de enrutamiento con direcciones IP

Tabla de enrutamiento

Dispositivos	Interfaz	Dirección IP	Máscara de subred	Gateway
Router Linksys	Fast	192.168.1.110	255.255.255.0	192.168.1.1
Cámara Ip/ DS-2CV2Q21FD-IW	VLAN 1	192.168.1.118	255.255.255.0	192.168.1.1
	Fast	192.168.1.120	255.255.255.0	192.168.1.1
Control de acceso/ DS-K1T8003	Fast	192.168.1.130	255.255.255.0	192.168.1.1

Nota. Tabla de enrutamiento con direcciones IP especificando su interfaz, dirección IP, mascara de subred y Gateway que se utilizara en cada uno de los dispositivos.

Figura 17

Router LINKSYS SMmart Wi-fi

Nota. Router *LINKSYS SMmart Wi-fi* designado por la institución para la implementación del proyecto.

El software para la implementación del sistema de control y video vigilancia que se va a utilizar es el iVMS 4200 - Control de Acceso y asistencia, ya que es un software compatible con los dispositivos seleccionados para el presente proyecto, donde se adjuntara el link de descarga: https://n9.cl/0ftwn.

3.7. Implementación de los componentes del proyecto investigativo

De acuerdo a la selección de dispositivos y componentes bajo el análisis técnico de capacidad de eventos almacenamiento y software disponible de las tablas comparativas N° 1 y 2 se realiza la implementación de cada uno los equipos que conforman el sistema de control de acceso y video vigilancia.

3.7.1. Sistema de control de acceso (HIKVISION / DS-K1T8003EF)

El equipo de marca Hikvision permite realizar un control de gestión de acceso y asistencia, agrega huellas digitales al sistema de forma remota, de acuerdo a la operación autónoma agrega localmente información de personas, tarjetas y huellas dactilares. Mediante la tarjeta deslizable permite generar un informe de asistencia a la unidad de flash USB, como muestra en la figura 18.

Figura 18

Control de acceso (HIKVISION / DS-K1T8003EF)

Nota. Permite realizar un control de gestión de acceso y asistencia, agrega huellas digitales, tarjetas de aproximación RFID y clave por consola al sistema de forma remota.

La instalación se la realizo con todas las medidas de seguridad tomando en cuenta los puntos estratégicos establecido por el docente y estudiante, se utilizó herramientas y material profesional para la ubicación del dispositivo de control de acceso, se respetó el espacio físico de las instalaciones estableciendo los materiales y conexiones de manera correcta dejando de una adecuada la estética de la instalación como se puede observar en las figuras N° 19, 20, 21, 22, 23.

Figura 19

Instalación de dispositivos de control de acceso

Nota: Ensamble de dispositivos adicionales para complementación de la instalación de control de acceso.

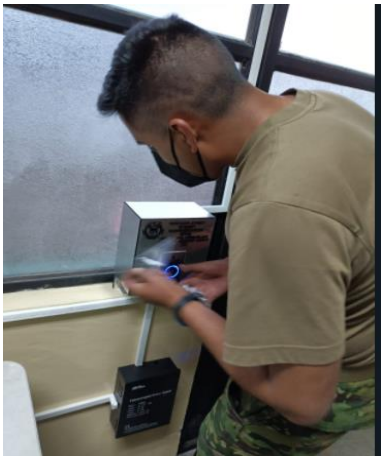
Figura 20

Instalación del regulador de voltaje y batería recargable de 12 v

Nota: Instalacion fija contra la pared de caja metalica que contiene un circuito regulador de voltaje y bateria recargable de 12v.

Figura 21

Instalación de domo del control de acceso y botón sensor de salida



Nota: Alojamiento de caja fija contenedora de control de acceso DS-K1T8003EF y botón sensor de salida.

Figura 22

Cableado de red

Nota: Cableado de red UTP CAT5 25 m. por medio de canaleta y sobre techo del laboratorio de comunicaciones.

Figura 23

Instalación de los dispositivos de la cerradura magnética

Nota: instalacion fija de cerradura magnetica AL-280 Led en puerta de metal con angulos z.

El proceso de instalación del equipo control de acceso (HIKVISION / DS-K1T8003EF), cuenta con varios componentes externos que cumplen con las especificaciones de la estructura del dispositivo para su funcionamiento dentro del laboratorio de la Institución como lo detalla en la tabla 4 y figura 24.

Tabla 4

Descripción del proceso de instalación de los componentes del equipo control de acceso (HIKVISION / DS-K1T8003EF).

Instalación del equipo control de acceso

No.	Descripción
1	El controlador de acceso, tiempo y asistencia fue instalado a 0,90 cm del suelo en una base de concreto fijado con ángulos de metal de 90° en una caja de corte a laser, en su interior se encuentran las conexiones eléctricas correspondientes, está localizado cerca de la puerta de ingreso al laboratorio detrás de una protección de vidrio que permite el ingreso solo por tarjeta de aproximación RFID.
2	El botón de salida de proximidad con sensor óptico infrarrojo es instalado dentro de la estructura del "controlador de acceso" fijado con tornillos en cada extremo para su estabilidad y alimentado eléctricamente por medio del dispositivo de control de acceso, permite salir cuando la mano del usuario tenga una aproximación de hasta 10cm y pueda abrir la puerta.

Instalación del equipo control de acceso

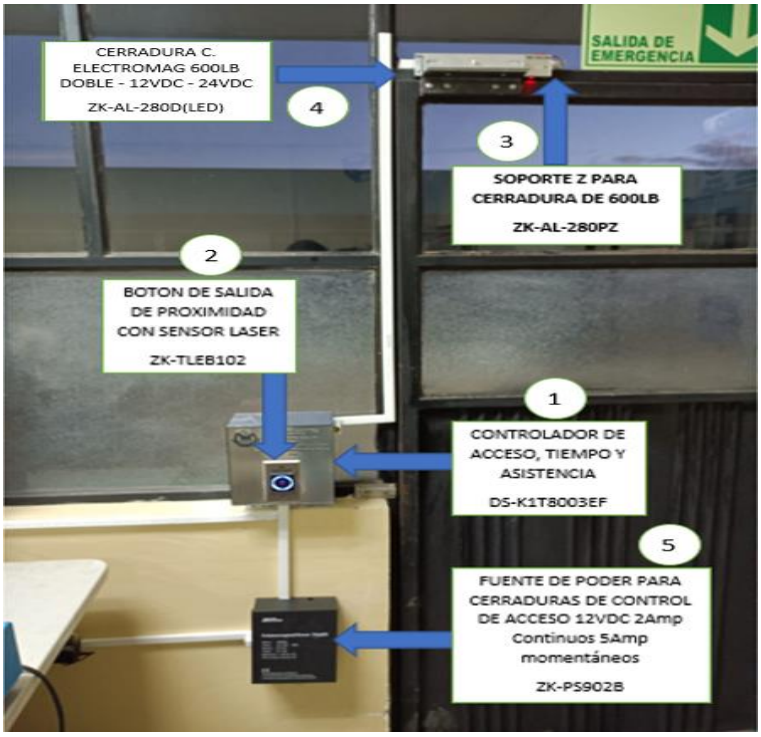
3	El Soporte Z se instaló en la parte superior izquierda de la puerta, fijada con tornillos a la estructura metálica con distancias específicas para no entorpecer el abrir y cerrar de la puerta, está diseñado para cerraduras de 600LB esto quiere decir que va a soportar una fuerza de 272.155 Kg, que es indispensable para la seguridad del laboratorio ya que cumple con la función también de soportar la Cerradura Electromagnética.
4	La instalación de la cerradura electromagnética se lo realiza en los soportes z de aluminio fijadas en la parte superior izquierda de la puerta. La cerradora que soporta 600lb doble - 12vdc - 24vdc, es aquella que permite el cierre y apertura del ingreso de los usuarios, este proceso es mediante la tarjeta magnética mediante el acercamiento de la mano al botón de salida de proximidad
5	Al regulador de voltaje que alimenta al circuito del control de acceso y chapa magnética con 12Vdc va protegida con una caja metálica la cual está instalado a un altura de 0.35 cm del suelo empotrado en la pared de concreto con tornillos y tacos fischer, junto a la fuente de poder para cerraduras de control de acceso 12vdc 2amp continuos 5amp momentáneos, es un elemento ideal que permite que los equipos como el control de acceso, el botón de proximidad y la cerradura magnética funcionen cuando exista un corte de energía y este perdure durante 24 horas en sistema de carga completa en el mismo equipo.

Nota. En esta tabla observamos que se detalla la descripción de los elementos del sistema del control de acceso y de instalación.

El proceso de instalación se lo realizó con herramientas como taladro, destornillador estrella y plano, corta fríos, alicate, tijeras para canaletas, escalera de aluminio pata de gallo y elementos complementarios para la instalación como tornillos de diferente medida, tacos fischer, canaletas o conducto eléctrico, cinta taipe, conductor de corriente (alambre), cable UTP cat5, conectores RJ 45. La instalación se lo realizo Sin ningún contratiempo en el laboratorio de Redes y Telecomunicaciones en la Universidad de Fuerzas Armadas sede Latacunga, donde se Implementa un sistema de control de acceso y video vigilancia a través de una red LAN interna para precautelar la integridad de equipos Tecnológicos. Como se puede observar en la figura 24.

Figura 24

Implementación del control de acceso con sus equipos externos de seguridad



Nota. Se detalla al equipo principal del control de acceso y sus accesorios que conforman la seguridad del sistema de control de entrada y salida del personal del Laboratorio.

Dentro del proceso de instalación se lleva a cabo el reconocimiento del tipo de tarjeta de aproximación RFID que sería un accesorio de habilitación que lleva el usuario para entrar y salir del laboratorio, como se puede observar en la figura 25.

Figura 25

Tarjeta Magnética RFID.

Nota. La tarjeta de aproximación RFID está integrado con un código personal único que se diferencia de las demás.

La identificación de la tarjeta de aproximación RFID, especifica el proceso de registro de la misma a entrada al laboratorio por cada usuario de la tarjeta dejando constancia un registro en la base de datos del sistema del control de acceso.

3.8. Instalación de la Cámara IP WIFI 2MP HIKVISION DS-2CV2Q21FD-IW

Este elemento electrónico de seguridad visual o de vigilancia está instalada en el laboratorio de la Universidad de las Fuerzas Armadas ESPE sede Latacunga como se puede observar en la figura 26.

Figura 26

Cámara IP WIFI 2MP HIKVISION DS-2CV2Q21FD-IW

Nota. Cámara IP inalámbrica HIKVISION disponible para el laboratorio de comunicaciones.

La instalación de la cámara IP inalámbrica DS-2CV2Q21FD-IW HIKVISION se la realiza fijándola en el techo del laboratorio que es de material de cielo raso con dos tornillos utilizando un destornillador estrella en los extremos señalados de la cámara utilizando una escalera de aluminio pata de gallo y conectada a un tomacorriente de 110V para su alimentación eléctrica atreves del cargador que genera 12V, se establece un punto estratégico de 3 metros de separación desde la pared norte y oeste del laboratorio con un altura de 3,20 metros para la verificación de imagen perpendicular de objetos y materiales existentes que desea vigilar y precautelar el docente, para la ubicación del dispositivo de control visual se respetó el espacio físico de las

instalaciones dejando de una adecuada la estética de la instalación como se puede observar en las figuras N° 27 y 28

Figura 27

Realización de cableado eléctrico

Nota: Se realiza un punto de conexion electrico dejando un toma corriente para la alimentacion del cargador de 12v para la camra IP.

Figura 28

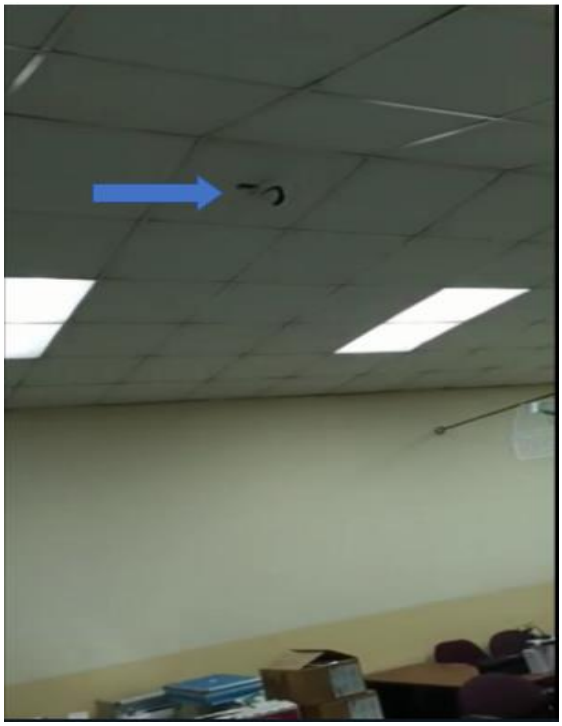
Ubicación de cámara IP inalámbrica

Nota: Ubicación de la cámara IP inalámbrica en el techo del laboratorio de comunicaciones constituido por una superficie plana “cielo raso”.

En la figura 29, se observa el tipo de cámara IP inalámbrica DS-2CV2Q21FD-IW HIKVISION con una rotación de 0º a 355º de forma horizontal y verticalmente de -10º a 90º, tiene la posibilidad de grabar en una tarjeta de memoria de máximo 128gb, de una forma WI- FI con alcance de 2.4Ghz hasta 50m interior, está disponible 2 tipos de vías de audio incluye micrófono, detección de movimiento, la cámara fue instalada en el techo del laboratorio.

Figura 29

Instalación de la Cámara IP WIFI 2MP HIKVISION



Nota. La cámara IP inalámbrica está instalada en el laboratorio con una alimentación 12 v.

3.8.1. Pasos de verificación de funcionamiento de la Cámara IP WIFI 2MP HIKVISION

En la tabla 5, se describe el proceso de como verificar si la cámara cumple con cada uno de los procesos de movimiento en una rotación de 0º a 355º, grabación y almacenamiento, configuración y manipulación de controles de la cámara inalámbrica atreves de la aplicación HIK-CONNET.

Tabla 5

Proceso de verificación de funcionabilidad de la cámara IP WIFI 2MP HIKVISION.

Proceso de verificación de cámara IP WIFI 2MP HIKVISION

No.	Descripción
1	El usuario debe descargarse la aplicación móvil, la misma que se encuentra con el nombre aplicación HIK-CONNET, dentro de la página oficial HIKVISION o en tiendas de aplicaciones móviles con play store y app store.
2	En el sistema HIKVISION dentro de aplicación, existen varios ítems de verificación para la cámara que cumpla la función de estar con sus principales funciones de grabar, audio y cámara.
3	La cámara cuenta con un número de serie G21839857 la cual es que sirve para identificar qué tipo de cámara es.

Proceso de verificación de cámara IP WIFI 2MP HIKVISION

4	El escaneo que tiene es mediante código QR que permite ingresar al sistema de la aplicación móvil para su reconocimiento de marca y modelo, que registrara como un usuario.
5	La conexión se verifica cuando esta nos identifica en el sistema de la app para que esta ingrese y pueda conectarse en forma WI-FI.
6	El sistema permite configurar por RED o WI-FI, es por ello que seleccionamos por la segunda opción.
7	En este paso se considera el nombre de la red (Com_Lab) y su clave de acceso que permita emparejar para que la cámara pueda funcionar mediante WI-FI.
8	Una vez llenado el NetWord y el Password el sistema empezara a verificar la información para que la cámara se empareje.
9	Este paso se puede observar que se emparejo entre cámara y usuario de tal forma que el proceso puede llevar a cabo.
10	El proceso de emparejamiento de la app y la cámara se llevan a cabo cuando la imagen de un visto permite ingresar al sistema.

Proceso de verificación de cámara IP WIFI 2MP HIKVISION

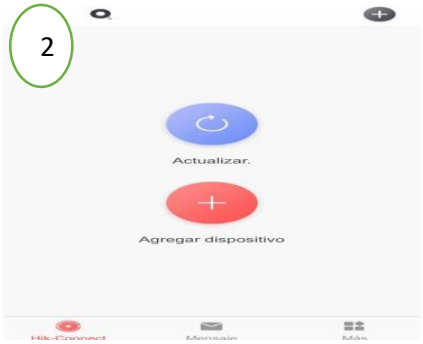
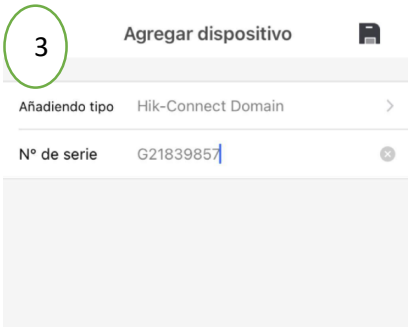
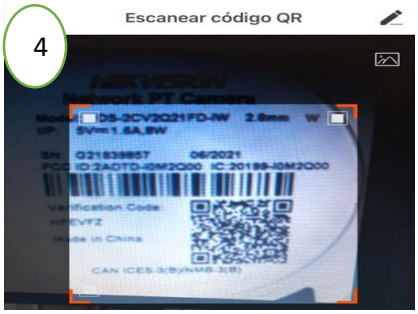
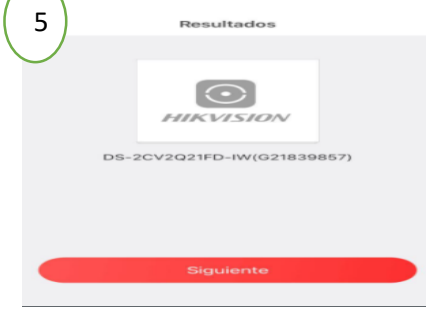
11	Al ingresar al sistema de la aplicación móvil de HIKVISION se observa como la cámara esta presentado en la pantalla del dispositivo móvil, el proceso del movimiento se realiza mediante flechas que permiten mover arriba, abajo, izquierda y derecho en un rango de 0º a 360º, tomar en cuenta que en este proceso no está grabando solo está en el proceso o selección de mostrar imagen.
12	La aplicación móvil permite tomar fotos, grabar y almacenar en la tarjeta micro SD con solo dar un clic y esta se guarde en la memoria del software iVMS 4200 o en la tarjeta micro- SD que se encuentra incorporada.

Nota. En esta tabla se toma en cuenta cada uno de los puntos a seguir para un proceso de verificación de la cámara IP WIFI 2MP HIKVISION y que trabaje correctamente con la aplicación del control de acceso.

Tabla 6

Imágenes de proceso de verificación de aplicación Hik-Connet de la cámara IP WIFI 2MP HIKVISION.

Proceso de verificación de aplicación Hik-Connet

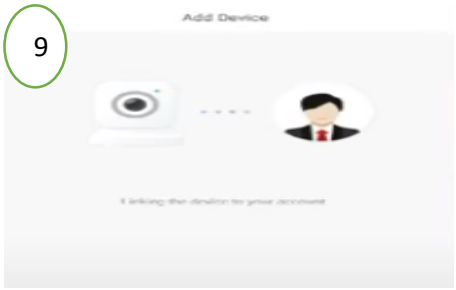
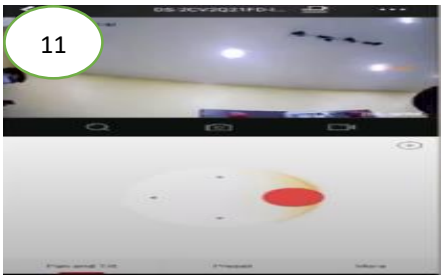
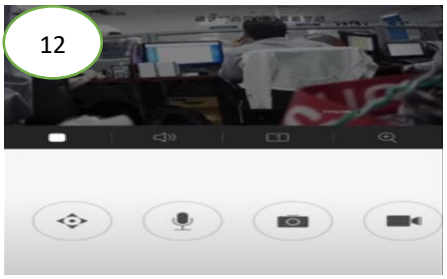
1 	2 
3 	4 
5 	6 

Nota. En esta tabla se observa las imágenes del proceso de verificación de la cámara IP WIFI 2MP HIKVISION de la tabla 5

Tabla 7

Proceso de compatibilidad, grabación y almacenamiento de aplicación Hik-Connet en la cámara IP WIFI 2MP HIKVISION.

Compatibilidad, grabación y almacenamiento de aplicación Hik-Connet

7 	8 
9 	10 
11 	12 

Nota. Se observa las imágenes del proceso de compatibilidad, grabación y almacenamiento de la cámara IP WIFI 2MP HIKVISION y que trabaje correctamente con la aplicación Hik-Connet.

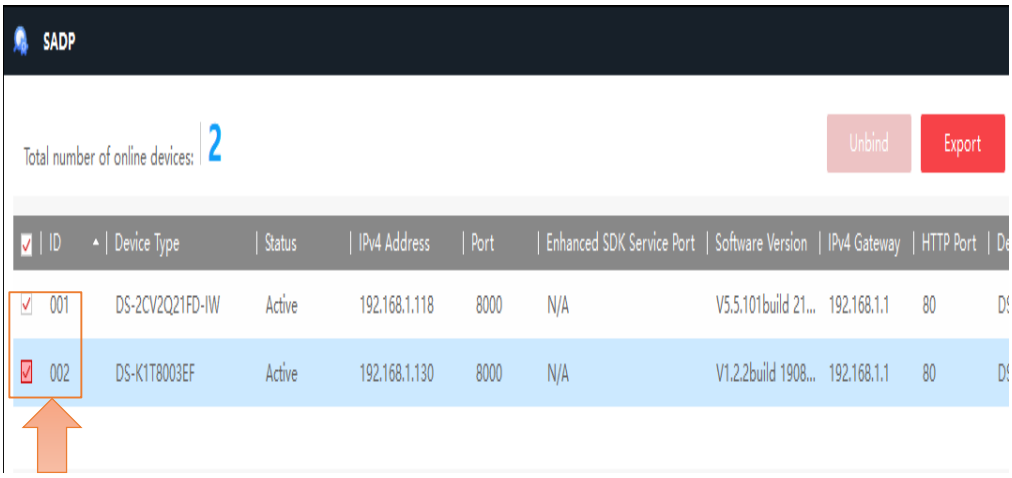
3.8.2. Procedimiento de enlace inalámbrico del control de acceso y de la cámara IP WIFI 2MP HIKVISION

La configuración de la cámara en el programa HIKVISION son los siguientes pasos:

1. Descargar e instalar en el computador la última versión del software SADP disponible en la página oficial del HIKVISION (www.hikvision.com/en/).
2. Conectar al computador el cual tiene instalado el software SADP a la red wifi o al router a través de un cable de red.
3. Conectar la cámara la cual se va a configurar a la red wifi a través de un cable de red al router.
4. Ejecutar el programa SADP, donde se realiza la activación de los dispositivos instalados para el control de acceso y video vigilancia.

Figura 30

Ejecución del programa SADP

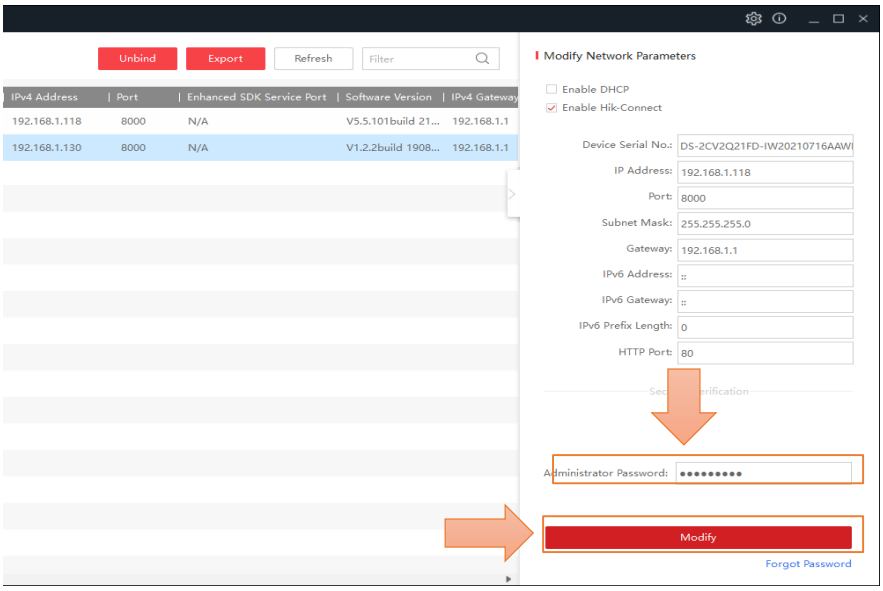


Nota. Selección de dispositivos inalámbricos a través del programa SADP.

5. La recomendación para este paso es colocar una clave con altos niveles de seguridad para no correr el riesgo de un plagio.

Figura 31

Designación de claves

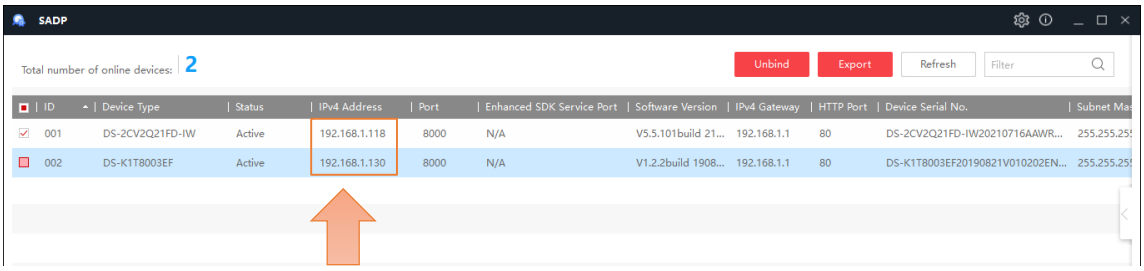


Nota. Creación de claves de dispositivos inalámbricos a través del programa SADP.

6. Una vez realizado la activación se da doble clic en el código o dirección IP

Figura 32

Activación de IP

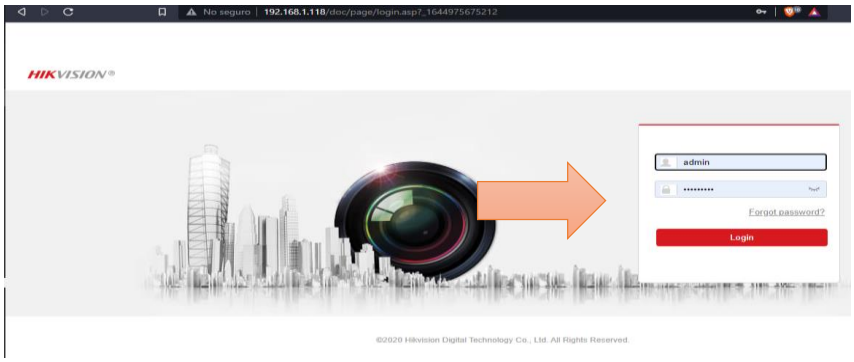


Nota. Activación de dispositivos inalámbricos a través del programa SADP.

7. Ingresar al web browser donde se digitará el usuario y clave creados con anterioridad.

Figura 33

Interfaz del Web Browser

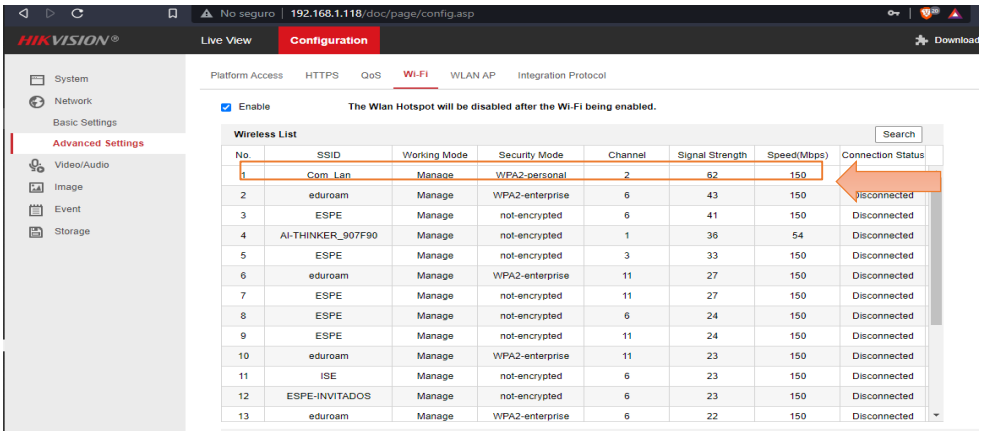


Nota: Autentificación de cámaras a través del Web Browser.

8. Posteriormente en este paso se ingresa a la configuración de la red, luego a la configuración avanzada, siguiente paso se ingresa al WI-FI, posteriormente seleccionar a la red a la cual se va a conectar.

Figura 34

Conexión a la red inalámbrica

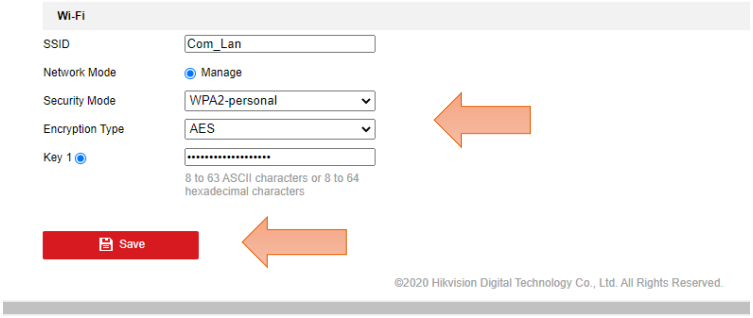


Nota: Conexión a la red inalámbrica asignada a través del Web Browser.

9. En advanced sentting se configura los ítems WI-FI como seguridad del modelo encriptación, pin de code, la clave o llave para acceder a la red inalámbrica.

Figura 35

Configuración de WI-FI

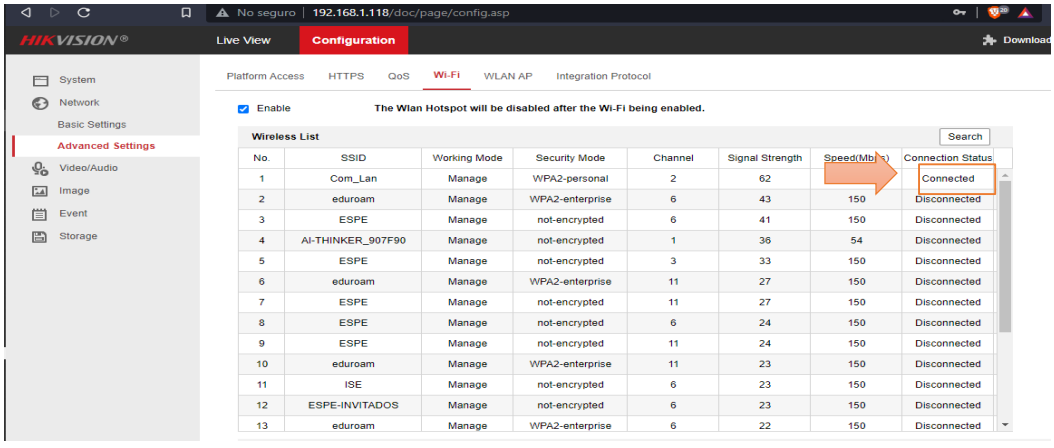


Nota: La configuración de advanced sentting para ordenar y verificar los ítems de seguridad de la red WI-FI.

10. Para verificar que el dispositivo ha sido guardado se da clic en buscar (search) y verificamos que está conectado correctamente.

Figura 36

Verificación de conectividad al router a utilizar

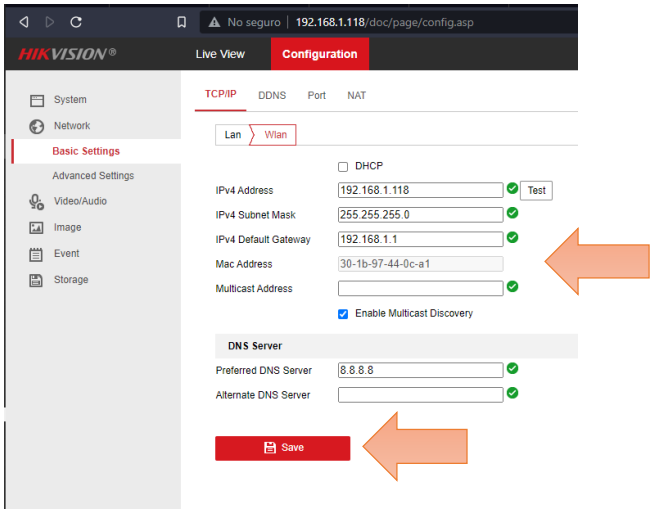


Nota: Verificación de conectividad inalámbrica al router.

11. En este paso se ingresa a configuraciones básicas, luego seleccionar la viñeta WLAN, después dar clic en el botón de prueba (test), verificar que no exista ningún conflicto de IP, cuando no existe ningún cambio de IP observar en la figura que todo este con un visto de color verde y está correctamente instado.

Figura 37

Configuración de WLAN



Nota. Configuración de WLAN del sistema inalámbrico.

12. Una vez realizado la conexión de la cámara a la red wifi, se puede realizar la desconexión del cable de red desde el router y posteriormente la cámara quedara disponible para poder tener acceso a través del web browser

3.9. Instalación del Software iVMS 4200

3.9.1. Configuración de control de acceso y asistencia

El sistema iVMS 4200 - Control de Acceso y asistencia, sirve para ver controles de acceso, control de tiempo de asistencia, alarma y video portería, en donde se registra una base de datos con tiempo y fecha.

Figura 38

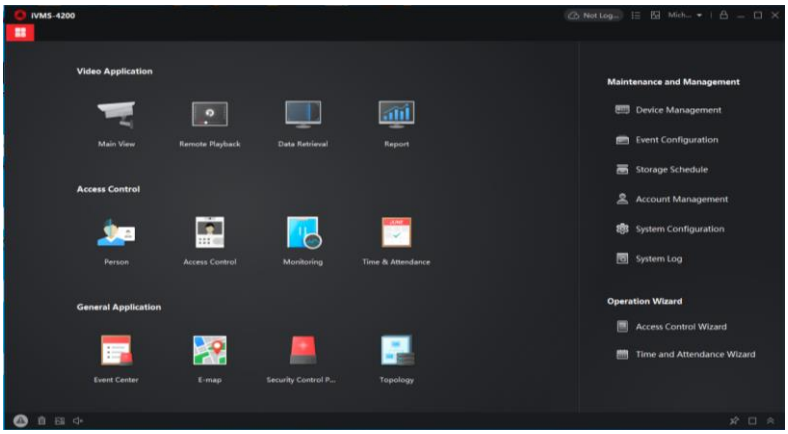
Sistema iVMS 4200 – Control de Acceso

Nota. Logo del programa para realizar el sistema de control de acceso.

En la figura 39, se detalla los iconos que forman parte del sistema Ivms 4200, como video vigilancia, reportes, usuarios que se encuentran agregadas al sistema, configuración de fechas y hora, reporte de posicionamiento, alarmas entre otros.

Figura 39

Pantalla de inicio del programa iVMS 4200

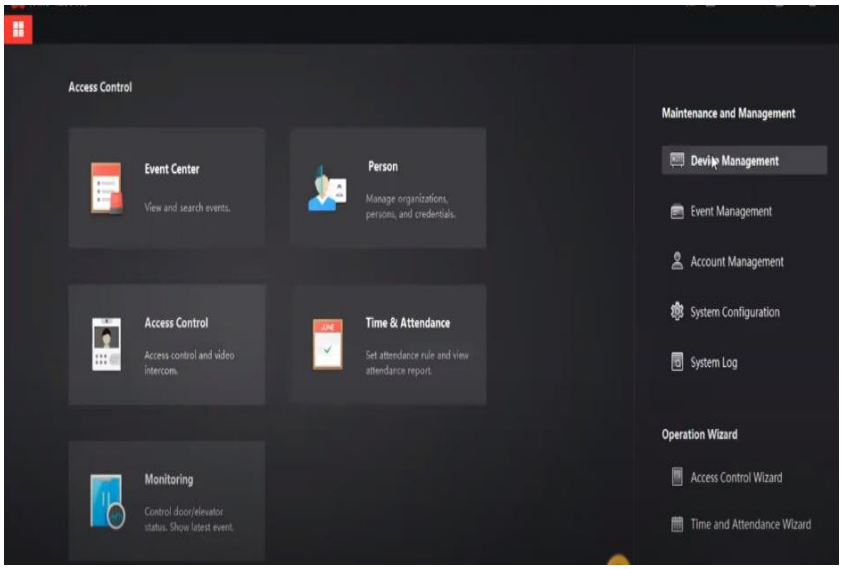


Nota. En la pantalla de inicio del programa cada uno de los iconos para ingresar al sistema.

En la figura 40, se observa los iconos de acceso de control con eventos personalizados, usuarios agregados al grupo específico, monitoreo del sistema entre otros.

Figura 40

Administrador de dispositivos

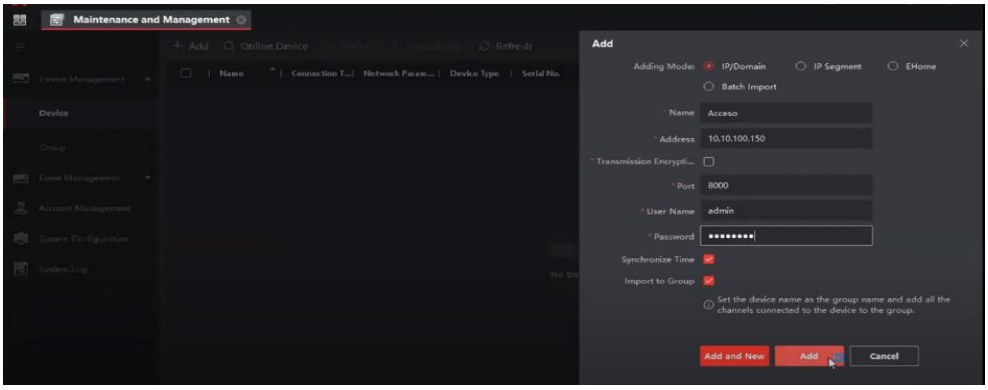


Nota. En el administrador de dispositivos se puede verificar y agregar los usuarios en sus diferentes grupos de trabajo.

Para la selección de dispositivos enlazados a la red inalámbrica del software iVMS-4200, se ingresa en la pestaña selección de agregar el equipo en la cual se debe llenar los parámetros como nombre que se le va a dar al equipo, la IP a la cual está asignada el dispositivo el puerto en el que se va a trabajar el nombre y contraseña.

Figura 41

Selección de agregar equipo (ADD)

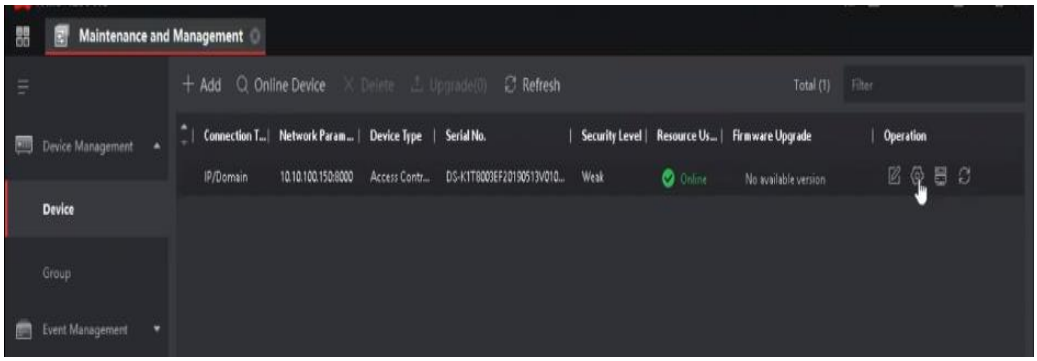


Nota. En la siguiente figura nos da a conocer que hay diferentes puntos para agregar el equipo y que requiere ser colocados.

Una vez agregado los equipos con sus respectivos parámetros los cuales fueron establecidos de acuerdo a las configuraciones iniciales, se reflejará en la bandeja de dispositivos en línea con sus campos reglamentarios llenos, mostrando un círculo verde que significa que está en línea y listo para su conectividad y verificación.

Figura 42

Dispositivo en línea

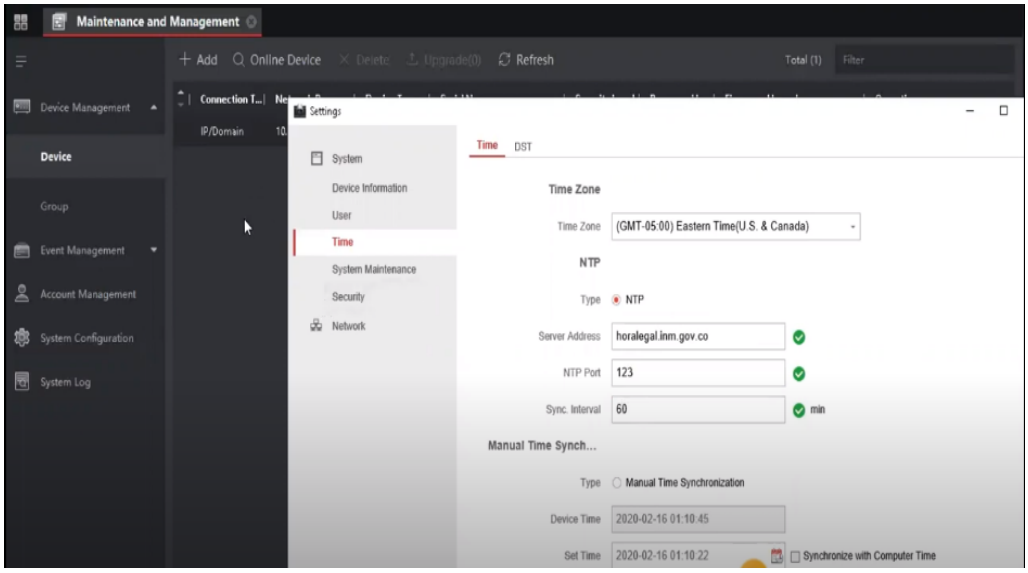


Nota. El sistema indica que los datos están cargados en línea de manera correcta con un visto de color verde.

La configuración horaria va de acuerdo al régimen del trabajo al que se rigen los diferentes usuarios que forman parte de los diferentes grupos que constan en el sistema de control de acceso, separándoles por jornadas de acuerdo a la necesidad del administrador.

Figura 43

Configuración horaria

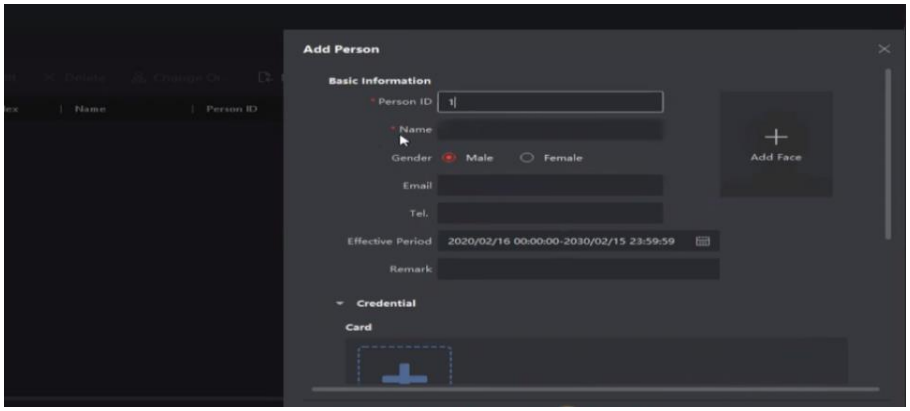


Nota. Este punto es importante para que el personal tome en cuenta los horarios de entrada y salida del personal que correspondan a un horario según el sector o País.

En la figura 44, se añade a los usuarios con parámetros establecidos con el sistema con un ID, el nombre a quien va a pertenecer el usuario, correo electrónico, teléfono, horario de la jornada laboral, se selecciona el modo de acceso que va a utilizar el usuario entre las cuales se puede optar con tarjeta RFID, reconocimiento facial, reconocimiento de huella dactilar y código por teclado.

Figura 44

Pantalla de inicio, agregar usuarios

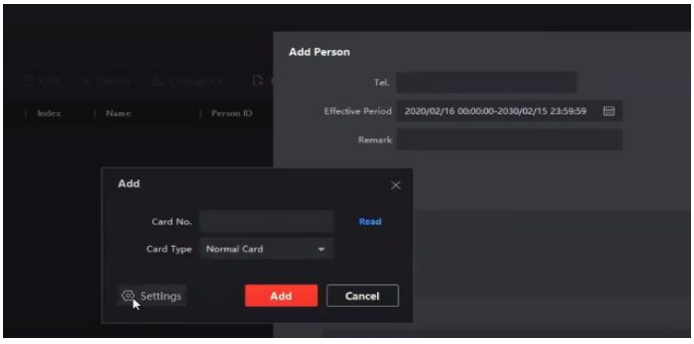


Nota. Se toma en cuenta que el sistema de control permite agregar personas para el ingreso y salida al lugar donde este implementado el mismo.

Para agregar una tarjeta de aproximación RFID, se selecciona el nombre del grupo del control de acceso, se aproxima la tarjeta al lector para el reconocimiento del código el cual aparecerá automáticamente en el monitor y se adicionará al usuario.

Figura 45

Agregar mediante tarjeta de aproximación RFID

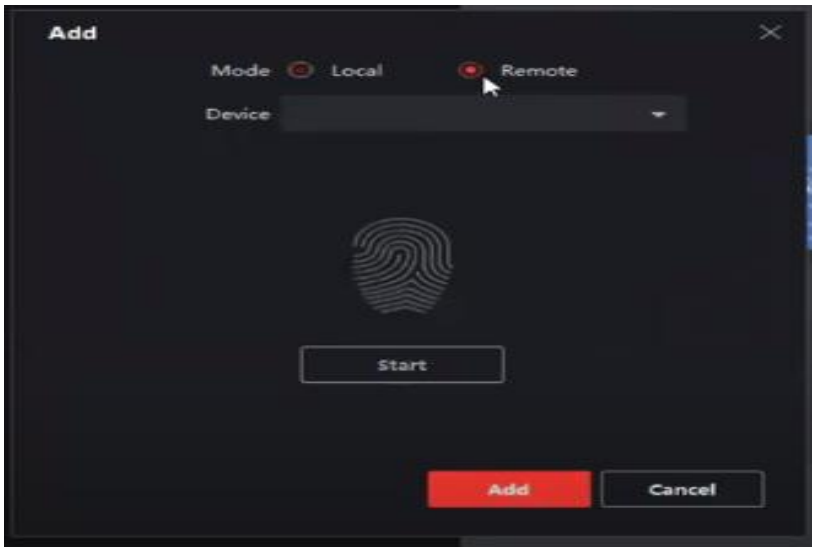


Nota. El proceso de agregar se considera la tarjeta magnética ya que tiene un código para el registro dentro del sistema.

Para agregar el reconocimiento de huella digital, se selecciona el nombre del grupo del control de acceso, se aproxima el dedo al sensor infrarrojo el dedo para el reconocimiento dactilar el cual guardará sus respectivas características y automáticamente el software guardará la respectiva información y se adicionará al usuario.

Figura 46

Agregar huella

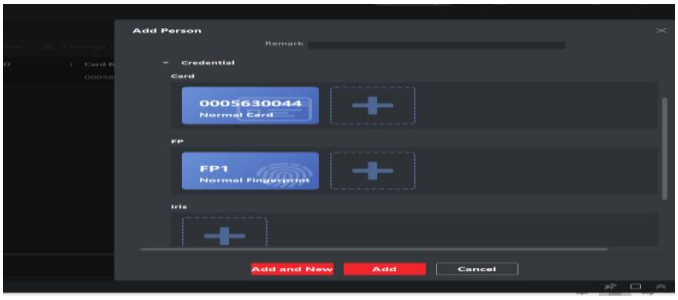


Nota. Agregar huella mediante el usuario este presente para que de manera remota se seleccione el dedo anular.

Para la verificación del correcto ingreso de las credenciales en el software iVMS-4200, se reflejará en el monitor en los campos específicos de estas credenciales de color azul con sus respectivos códigos asignados, como se muestra en la figura 47.

Figura 47

Punto de verificación

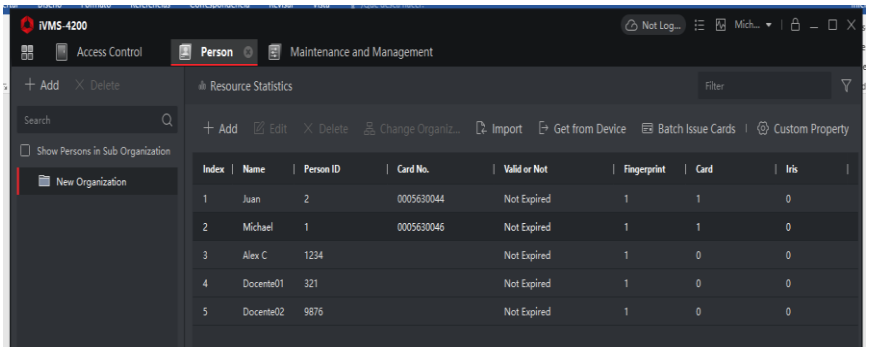


Nota. En esta figura observamos que al agregar un usuario de manera remota mediante clave, tarjeta magnética y huella digital se encuentran agregados de manera visible en el sistema.

En la figura 48 se observa los usuarios que han sido asignados al control de acceso los cuales constan con los campos requeridos para acceder al sistema tales como tarjeta de proximidad RFID, reconocimiento fácil o pin por teclado.

Figura 48

Identificación

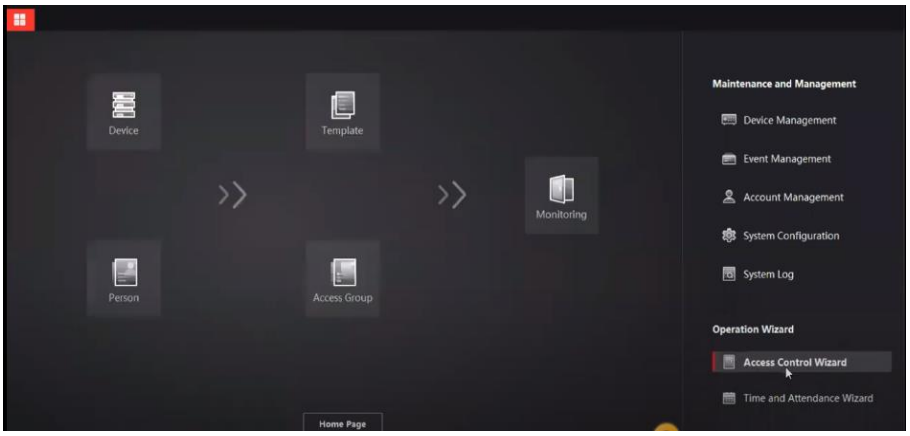


Nota. La figura nos muestra que el sistema funciona correctamente con diferentes personas que tiene la manera de ingresar por huella o tarjeta magnética.

Para el sistema de control de usuarios se dividen en varios grupos los cuales constaran de diferentes horarios de entrada y salida con intervalos de tiempo restringidos para su registro en la base de datos y controles de acceso.

Figura 49

Control de acceso

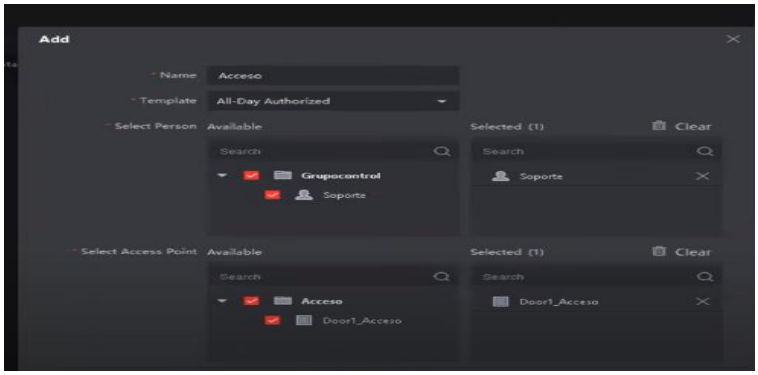


Nota. En este punto se crea el grupo de personas que van a hacer parte del dispositivo:

En la figura 50, se muestra la asignación de grupos de trabajo a los usuarios el cual es el último paso para el registro formal en la base de datos del software iVMS-4200 y del control de acceso.

Figura 50

Detalle de agregar el grupo de acceso

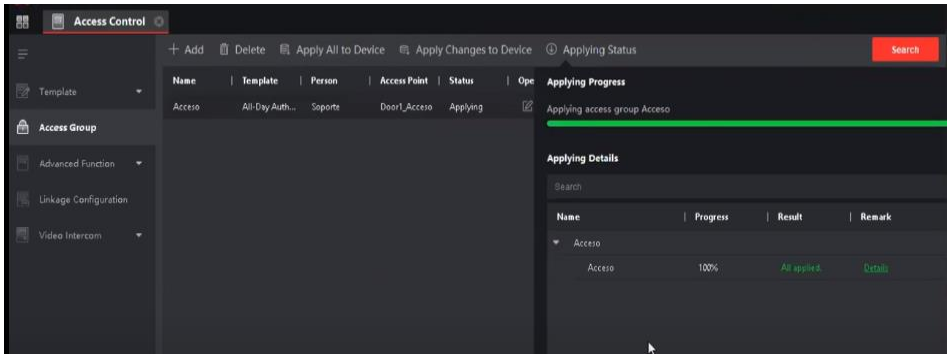


Nota. El sistema permite agregar de manera remota de como personal que da soporte y el sistema permite el acceso de configuración este instalado:

Al terminar el proceso de llenar los parámetros que requiere el software iVMS-4200, para asignar un cupo dentro de la base de datos del control de acceso se debe colocar en color verde applying progress y quedara registrado hasta una nueva modificación.

Figura 51

Verificación de agregados al sistema



Nota. En la figura observamos que una vez llena todos los requerimientos podemos cargar y verificar de manera que el sistema de color verde está listo y poder utilizar el control de acceso.

3.10. Análisis del esquema utilizado

Para el análisis del esquema utilizado se tuvieron en cuenta varios puntos en el desarrollo del proyecto de investigación, como el funcionamiento que se le iba a dar a cada sistema de comunicación:

- La comunicación será de manera inalámbrica, aprovechando la infraestructura mediante un punto de red.

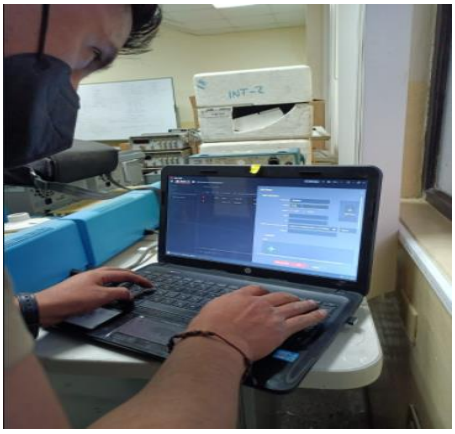
- Para el monitoreo muna vez instalado el sistema se lo podrá realizar desde cualquier elemento que cuente con conexión a internet
- El sistema de control cuenta con un registro de hora de entrada y salida del personal que pueda entrar al laboratorio de la Institución.
- La primera estación es el punto de control de acceso mediante (tarjeta magnética, clave de acceso, huella digital), donde va a estar alojada al ingreso del laboratorio. La segunda estación de video vigilancia se va a ubicar en un punto estratégico del mismo. La tercera estación se va a direccionar los videos que serán almacenados a un disco duro interno que será conectado directamente al Servidor principal caiga este va a poder ser implementado y tendrá que habilitado de manera manual.

3.11. Pruebas de Funcionamiento

Para la verificación del funcionamiento del sistema de control de acceso y video vigilancia se comprueba mediante el software iVMS 4200, constatando la salida de imagen de la cámara en la pantalla del servidor con la manipulación de cámara inalámbrica con controles PTZ y el registro de ingreso de usuarios registrados en la base de datos del sistema del control de acceso, con el accesorio habilitante para el ingreso que es la tarjeta de aproximación RFID, como se muestra en las figuras N° 52, 53, 54, 55.

Figura 52

Verificación del sistema



Nota. Se verifica en el sistema el reconocimiento de las direcciones IP de los dispositivos y su respectivo funcionamiento.

Figura 53

Verificación de ingreso

Nota. Se verifica el acceso al laboratorio con el accesorio habilitante que es la tarjeta de aproximación RFID.

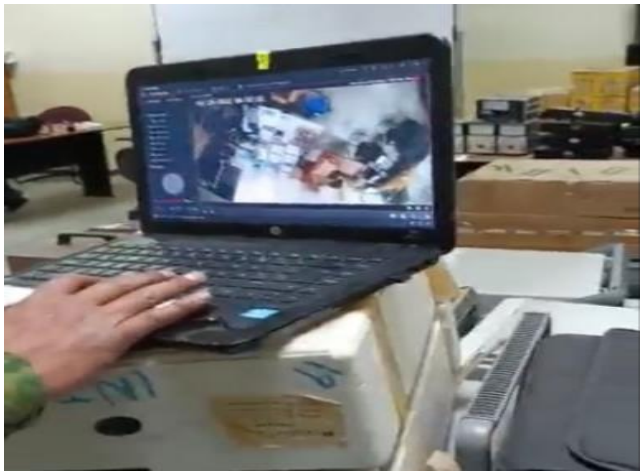
Figura 54

Verificación del botón de salida

Nota. Se verifica el botón de salida instalado en la parte interior del laboratorio de comunicaciones el cual es un sensor por lo que no necesita presión para activarlo.

Figura 55

Verificación de cámara IP



Nota. Se observa la salida de imagen de la cámara IP inalámbrica en el monitor del servidor verificando así su funcionalidad con el control PTZ.

En las pruebas de funcionamiento de presentó inconvenientes al momento de la instalación del software iVSM 4200 en el ordenador del docente la cual era un Mac – Apple mismas que constan con políticas de seguridad extras por parte de la marca fabricante para softwares desconocidos o ajenos a su línea de aplicaciones, se logró solventar este tipo de inconveniente retirando algunas seguridades de la máquina, reiniciando el ordenador y verificando direcciones IP que se encontraban ocupadas por otros dispositivos conectados al router del laboratorio.

Se ocasionó un problema con la conectividad de acceso remoto en la aplicación Hik-Connet por políticas de seguridad de la universidad ya que el puerto que utiliza la cámara IP inalámbrica y el control de acceso es el 8000 y esos puertos se encuentran bloqueados para seguridad de datos de la institución.

3.12. Entrega de proyecto

Al finalizar la instalación del proyecto del sistema de control de acceso y video vigilancia a través de una red LAN interna en el laboratorio de comunicaciones de la Universidad de Fuerzas Armadas sede Latacunga para precautelar la integridad de equipos tecnológicos se realiza la verificando la instalación y funcionamiento con el docente encargado del laboratorio del sistema de control de acceso y video vigilancia comprobado mediante el software iVMS 4200, constatando la salida de imagen de la cámara en la pantalla del servidor con la manipulación de cámara inalámbrica con controles PTZ y el registro de ingreso de usuarios registrados en la base de datos del sistema del control de acceso, con el accesorio habilitante para el ingreso que es la tarjeta de aproximación RFID, dando por concluido la entrega de equipos y accesorios al custodió y administrador de la red LAN interna del laboratorio, como se muestra en las imágenes N° 56, 57, 58.

Figura 56

Verificación del docente del ingreso

Nota. El docente verifico la funcionalidad del dispositivo de control de acceso al laboratorio de comunicaciones con el accesorio destinado para el acceso como es la tarjeta de proximidad RFID.

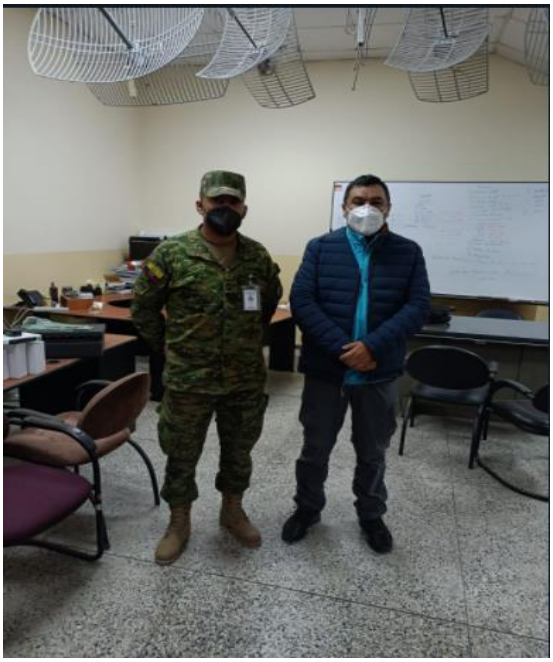
Figura 57

Verificación del docente del botón de salida

Nota. El docente verifico la funcionalidad del dispositivo botón sensor de salida.

Figura 58

Entrega total del proyecto al Sr. Ing. David Rivas



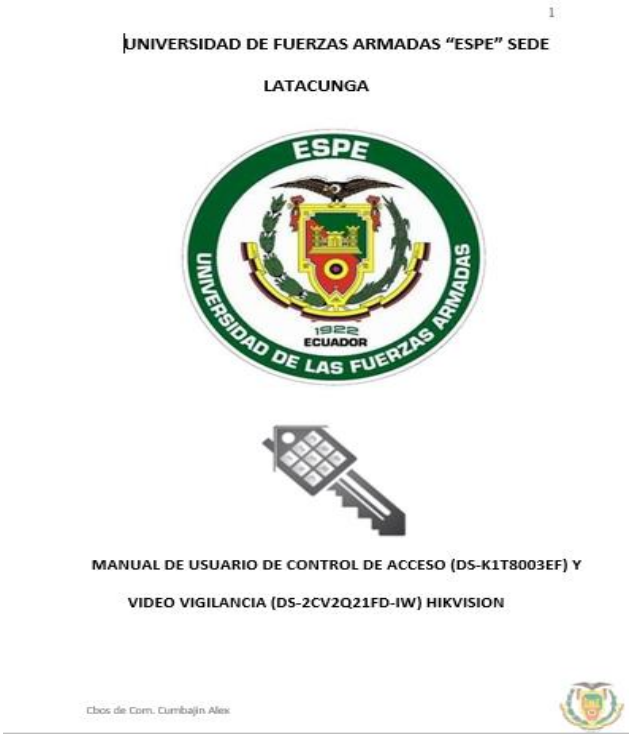
Nota. Se hace la entrega de equipos y accesorios e instalación de software iVMS 4200 en el ordenador destinado como servidor principal de la red LAN interna del laboratorio.

3.13. Elaboración de un manual

Se elabora un manual de usuario para el administrador de la red del laboratorio de comunicaciones y dispositivos con el cual se podrá manipular y establecer las diferentes configuraciones que tienen el sistema de control de acceso y el circuito cerrado de televisión (cctv) o corregir fallas técnicas o de conflicto lógico a través del software iVMS 4200

Figura 59

Manual de usurario de control de acceso y video vigilancia Hikvision



Nota. Se implementa un manual de usuario para la manipulación y programación en los dispositivos control de acceso DS-K1T8003EF y cámara IP DS-2CV2Q21FD-IW HIKVISION.

Capítulo IV

4. Conclusiones y Recomendaciones

4.1. Conclusiones

- Se analizó los diferentes sistemas y dispositivos de controles de acceso y circuito cerrado de televisión (cctv), comparando su funcionamiento y características técnicas, seleccionando e instalando los mejores equipos que se adaptaron a las condiciones y necesidades que se requería en el laboratorio de comunicaciones de la Universidad de Fuerzas Armadas Sede Latacunga
- El programa iVMS 4200 es un software que permite la adaptación del sistema de control de acceso y video vigilancia para su administración ya que los equipos pertenecen a la misma marca de HIKVISION existen una integridad de comunicación y almacenamiento entre los dispositivos, permitiendo que las evidencias sean resguardadas por la seguridad que brinda el sistema.
- El sistema de control de acceso será mediante la tarjeta magnética a pedido de la Institución ya que no podrán ser registrados por clave ni por huella digital, esto brinda mayor seguridad y facilidad de que solo personal autorizado pueda ingresar y salir del Laboratorio.
- La instalación del sistema de seguridad es proporcionada por una cerradura magnética de 600lg fuerza que es muy buena contra cualquier fuerza externa que se desee realizar para ingresar al Laboratorio esto brinda mayor seguridad.
- Al contar con una cámara IP inalámbrica PTZ que tiene una direccionalidad de 355º en horizontal y de -10º a 90º en vertical, se concluye que tiene un rango de vista del 100% de todo el laboratorio de acuerdo a la manipulación del administrador.

- Se realizó las pruebas necesarias para determinar que la instalación del control de acceso y circuito cerrado de televisión (cctv) garantice su correcto desempeño técnico en su uso diario o como bien lo convenga al administrador del sistema de la red LAN interna del laboratorio.

4.2. Recomendaciones

- Se recomienda no usar sistemas operativos como Apple, para la instalación del software iVMS-4200, ya que las políticas de seguridad no permiten que el programa se desarrolle en su totalidad limitando así la configuración de los dispositivos anexados al software.
- En el proceso de agregar a los usuarios se recomienda que solo el administrador tenga acceso a este tipo de preferencias del manejo del sistema de seguridad.
- Se recomienda que la tarjeta magnética no sea entregada a cualquier persona ya que el sistema registra el ingreso de las personas que constan dentro de la base de datos del control de acceso.

GLOSARIO

CCTV: Circuito Cerrado De Televisión

DIRECCION IP: Dirección del Protocolo de Internet

LAN: Local Area Network (Red de Área Local)

LFD: Large Format Display (Pantalla de gran formato)

Mb: Mega byte

Kb: Kilo byte

MAN: Metropolitan Area Network (Red de Área Metropolitana)

VPN: Virtual Private Network (Red Privada Virtual)

WAN: Wide Area Network (Red de Área Amplia)

PC: Personal Computer (Computadora Personal)

RFID: Radio Frequency Identification (Identificación por radio frecuencia)

TAGS: Etiqueta Inteligente

RAM: Random Access Memory (Memoria de Acceso Aleatorio)

KHz: Kilo Herz

USB: Universal Serial Bus (Bus Universal en Serie)

TCP/IP: (Protocolo de control de transmisión/ Protocolo de Internet)

PTZ: Pan-Tilt-Zoom (Panorámica-Inclinación-Zoom)

WIFI: Wireless Fidelity (Fidelidad Inalámbrica)

SADP: Search Active Devices Protocol (Buscar protocolo de dispositivos activos)

WLAN: Wireless Local Area Network (Red Inalámbrica de Área Local)

ID: Identificación

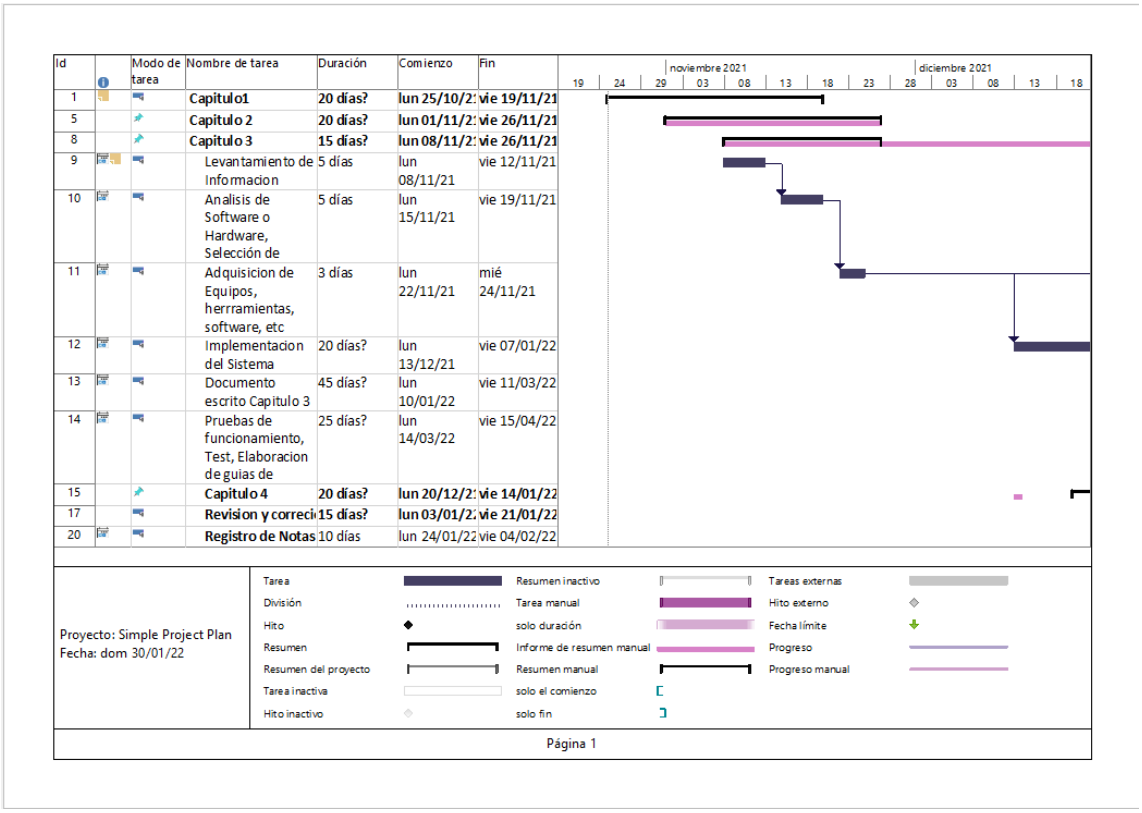
iVMS: Software de gestión de vídeo

CD: Corriente Directa

CRONOGRAMA

Figura 60

Cronograma de presentación del proyecto



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1		**Capitulo1**	**20 días?**	**lun 25/10/2**	**vie 19/11/21**
5		**Capitulo 2**	**20 días?**	**lun 01/11/2**	**vie 26/11/21**
8		**Capitulo 3**	**15 días?**	**lun 08/11/2**	**vie 26/11/21**
9		Levantamiento de Informacion	5 días	lun 08/11/21	vie 12/11/21
10		Analisis de Software o Hardware, Selección de	5 días	lun 15/11/21	vie 19/11/21
11		Adquisicion de Equipos, herrramientas, software, etc	3 días	lun 22/11/21	mié 24/11/21
12		Implementacion del Sistema	20 días?	lun 13/12/21	vie 07/01/22
13		Documento escrito Capitulo 3	45 días?	lun 10/01/22	vie 11/03/22
14		Pruebas de funcionamiento, Test, Elaboracion de guias de	25 días?	lun 14/03/22	vie 15/04/22
15		**Capitulo 4**	**20 días?**	**lun 20/12/2**	**vie 14/01/22**
17		**Revision y correcci**	**15 días?**	**lun 03/01/2**	**vie 21/01/22**
20		**Registro de Notas**	10 días	lun 24/01/22	vie 04/02/22

Nota. Las fechas son basadas con el calendario de la universidad.

PRESUPUESTO

Costos Primarios

Tabla 8

Costos primarios del proyecto

Cantidad	Descripción	V/U	V. TOTAL
1	Controlador de acceso, tiempo y asistencia/DS-K1T8003EF	71,13	71,13
1	Cámara IP domo 2mp inalámbrica 1080p/ DS-2CV2Q21FD-IW	139,39	139,39
1	Botón de salida de proximidad con sensor laser/ ZK-TLEB102	19,1	19,1
1	Fuente de poder/ ZK-PS902B	25,73	25,73
1	Batería recargable 12vdc/ ST-12V-4AMP	16,07	16,07
1	Cerradura c. electromag/ ZK-AL-280D(LED)	55,17	55,17
1	Soporte z/ ZK-AL-280PZ	11,02	11,02
5	Tarjetas RFID	4,02	20,10
		VALOR TOTAL	357,71

Nota. Se encuentra el valor de costos de dispositivos electrónicos y eléctricos para la instalación.

Costos Secundarios

Tabla 9

Costos secundarios del proyecto

Cantidad	Descripción	V/U	V. TOTAL
4	Canaletas data faz	1,80	7,20
25	Cable UTP CAT5	0,35	8,75
12	Cable eléctrico flexible N°14	0.25	3
2	Ángulos de hierro	10	20
1	Tomacorriente	0,50	0,50
		VALOR TOTAL	39,45

Nota. La tabla hace referencia a los gastos de segundo plano que son elementos de instalación complementarios para la instalación del proyecto:

Costo Total

Tabla 10

Costo total del proyecto

Valor total costos primarios	357,71
Valor total costos secundarios	39,45
Valor Total de proyecto	**397,16**

Nota. Se realiza el cálculo total del dinero gastado en el proyecto de implementación de un control de acceso con cámara IP mediante una red LAN interna del laboratorio de comunicaciones.

Bibliografía

Bianchi, A. (2016). *Geocities*. Obtenido de http://www.geocities.ws/abianchi04/textoredes/snmp.pdf

Carate, B. &. (2019). *DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS (NIDS) PARA UNA RED SIMULADA PYMES EN GNS3, IMPLEMENTADA EN UN MÓDULO RASPBERRY PI PORTÁTIL.* UNIVERSIDAD POLITÉCNICA SALESIANA. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/17546/1/UPS%20-%20ST004141.pdf

Carate, B., & Pozo, D. (2019). *DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS (NIDS) PARA UNA RED SIMULADA PYMES EN GNS3, IMPLEMENTADA EN UN MÓDULO RASPBERRY PI PORTÁTIL.* UNIVERSIDAD POLITÉCNICA SALESIANA. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/17546/1/UPS%20-%20ST004141.pdf

Castillo, J. (2016). *"ESTUDIO COMPARATIVO DEL RENDIMIENTO DE SERVIDORES WEB DE VIRTUALIZACIÓN SOBRE LA PLATAFORMA WINDOWS SERVER 2008".* ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO. Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/1946/1/98T00016.pdf

Chang, D. (2018). *Desarrollo e implementación de un sistema para el control e inventario continuo, utilizando tecnología RFID, para la biblioteca de la UPS sede Guayaquil.* Guayaquil: Primera.

Chávez, G. (2016). *Propuesta de red de datos para la gestión de los servicios de red en el campus politécnico de la ESPAM MFL.* Calceta: Primera.

Douglas, E. (1997). *Redes de computadoras, Internet e interredes.* México: Naucalpan.

León, D. (2021). *Servidores de Red: Características, Ventajas y Desventajas*. Obtenido de https://blog.infranetworking.com/servidores-de-red/

López, X. (2018). *Rediseño de la red con calidad de servicios para datos y tecnología de voz sobre ip en el ilustre municipio de ambato.* Ambato: Primera.

Machado, A. (8 de Febrero de 2016). *Naps Tecnología y educación*. Obtenido de https://naps.com.mx/blog/funciones-de-un-administrador-de-redes/

Manuel, S. O. (16 de Septiembre de 2016). *ITD*. Obtenido de https://sites.google.com/a/itdurango.edu.mx/10040372/system/app/pages/sitemap/hierarchy

MIRANDA, P. C. (2018). *http://repositorio.unesum.edu.ec/*. Obtenido de http://repositorio.unesum.edu.ec/bitstream/53000/1487/1/UNESUM-ECU-REDES-2017-19.pdf.Recuperado de

Moreno, A. G. (2015). *Diseño e implementación de un prototipo de software para la administración de red usando snmp v3 sobre el sistema operativo andorid.* Quito: EPN (Escuela Politécnica Nacional).

Muñoz, R. (2013). *Proyecto previo a la obtención del títutlo de tecnòlogo en análisis informaticos.* Quito.

Ortega, A. (2019). *Diseño de un sistema de control de acceso y video vigilancia para la unidad educativa porvenir con la utilización de dispositivos IP.* Cuenca: Primera.

Robles, F. J. (2018). *Planificación y Administración de Redes (GRADO SUP.).* España: RA-MA.

rosa, l. L. (22 de Octubre de 2021). *pandorafms*. Obtenido de https://pandorafms.com/blog/es/protocolos-de-administración-de-redes/

Salas, J. S. (2020). *DISEÑO DE UNA HERRAMIENTA DE MONITOREO Y CONTROL DE SERVIDORES UTILIZANDO COMO EJE PRINCIPAL CACTI. APLICADO A*

UNA PYME MEDIANA. Bogota: UNIVERSIDAD COOPERATIVA DE COLOMBIA.

SANTIAGO, A. C. (2016). *DESARROLLO DE UN SISTEMA INALAMBRICO BASADO EEG PARA EL MONITOREO DEL SUEÑO EN UN CONDUCTOR.* CUENCA.

UNAM. (2017). *UNAM*. Obtenido de https://programas.cuaed.unam.mx/repositorio/moodle/pluginfile.php/931/mod_resource/content/4/contenido/index.html

Valarezo Saldarriaga, G. G., & Simisterra Huila, J. C. (2018). *Implementación de un sistema de gestión y administración de redes basados en el protocolo simple de monitoreo de redes SNMP en la red ESPOL-FIEC.* Guayaquil: ESPOL.

Vega, G. (2018). *IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO PARA EL ANÁLISIS DE LA DISPONIBILIDAD, CAPACIDAD, CALIDAD Y LATENCIA DE ENLACES CORPORATIVOS DE ÚLTIMA MILLA.* Obtenido de http://repositorio.ucsg.edu.ec/bitstream/3317/11890/1/T-UCSG-POS-MTEL-118.pdf

Vinicio, P. L. (08 de 2018). *repositorio.uta.edu.ec*. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/28577/1/Tesis_%20t1465ec.pdf

ANEXOS