UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE TECNOLOGÍA

CARRERA: ELECTRÓNICA Y TELECOMUNICACIONES

DISEÑO DE UN SISTEMA DE SEGURIDAD INALAMBRICA CON CAMARAS IP PARA EL CENTRO DE ACOGIDA NIÑO JESUS

Trabajo de Aplicación – Examen de Grado presentado para obtener el Grado de Licenciatura

POR: CRISTINA VILLCA MAMANI

LA PAZ- BOLIVIA

Noviembre, 2021

AGRADECIMIENTO

En primer lugar agradezco a Dios por darme vida y salud, para superar todos los obstáculos y dificultades que se presentan día a día.

A la Facultad de Tecnología carrera Electrónica y Telecomunicaciones por permitirme formar académicamente y culminar una de mis más grandes metas obteniendo un título profesional en Electrónica y Telecomunicaciones.

Finalmente a todos los docentes y compañeros de la carrera electrónica y telecomunicaciones, por compartir sus conocimientos y amistad.

DEDICATORIA

A mis padres Marcelo y Lucia, en especial a mi tía Nancy de Siles por su apoyo incondicional en todos los momentos de mi vida, por confiar en mí y quererme siempre sin pedir nada a cambio.

A mis hermanos porque han sabido fortalecerme con su cariño y comprensión día a día, familiar y amigos que han estado presentes en todo el trayecto de mi vida dándome todo el apoyo necesario para seguir adelante.

RESUMEN

En la institución hogar niño Jesús se observó mucha injusticia por falta de seguridad así también maltratos psicológicos y físicos hacia a los niños menores por parte de la personas que prestan sus servicios. El propósito de este proyecto es implementar cámaras de seguridad inalámbrica en todos sus ambientes para evitar los maltratos hacia los niños y niñas, como también poder evitar las injusticias que se cometen con el personal encargado del lugar.

En este lugar se presentó este caso del niño Alexander que murió. El 12 de noviembre de 2014 el bebé Alexander se descompuso en el hogar Virgen de Fátima para entonces, en la calle 3 de la zona de Obrajes de La Paz.

La necesidad de adaptar un sistema de seguridad en la institución es importante. Para lo cual se utilizaran dispositivos de tecnología con cámaras de vigilancia inalámbrica con monitoreo desde la oficina, que tenga gran alcance y cubra la necesidad de proporcionar seguridad en el hogar niño Jesús.

El desarrollo del proyecto abarcara todos los ambientes de la institución ya que debe hacerse un reconocimiento de todo el perímetro externos e internos y otros puntos estratégicos para la implementación de las cámaras ip.

Palabras claves: resumen sistema de seguridad con cámaras ip

SUMMARY

In the Niño Jesus' home institution, a lot of injustice was observed due to lack of security, as well as psychological and physical abuse towards minor children by the people who provide their services. The purpose of this project is to implement wireless security cameras in all its environments to avoid mistreatment of children, as well as to avoid injustices that are committed to the personnel in charge of the place.

In this place this case of the boy Alexander who died was presented. On November 12, 2014, baby Alexander decomposed at the Virgen de Fátima home at that time, on 3rd Street in the Obrajes area of La Paz.

The need to adapt a security system in the institution is important. For which technology devices with wireless surveillance cameras with monitoring from the office will be used, which has a wide range and covers the need to provide security in the home of the child Jesus?

The development of the project will cover all the environments of the institution since are cognition of the entire external and internal perimeter and other strategic points for the implementation of the IP cameras must be made.

Keywords: summary of security system with ip cameras

INDICE

AGRADECIMIENTO.....i

DEDICATORIA.....ii

RESUMEN..... iii

CAPITULO I.....1

1. INTRODUCCIÓN 1

1.2 PLANTEAMIENTO DEL PROBLEMA.....2

1.2.1 Identificación del Problema.....2

1.2.2 Formulación del Problema.....4

1.3 OBJETIVOS 4

1.3.1 Objetivo General.....4

1.3.2 Objetivos Específicos 4

1.4 JUSTIFICACION 5

1.4.1 Justificación Tecnológica.....5

1.4.2 Justificación Social. 6

1.4.3 Justificación Académica. 6

1.5 LIMITES Y ALCANCES 6

1.5.1 Limites.....6

1.5.2 Alcances.....6

1.5.2.1 Delimitación Espacial 6

1.5.2.2 Delimitación Temporal.....7

1.5.2.3 Delimitación Temática 7
1.6 SOLUCION PROPUESTA 8
1.6.1 Topología 8
1.6.2 Funcionamiento 9
1.6.3 Central de Monitoreo 9
1.6.4 Protocolo de Acción 10
1.6.5 Adquisición e Instalación del Equipamiento 10
1.6.6 Procedimientos para el Diseño o Implementación del Proyecto 11
CAPITULO II 12
2. FUNDAMENTO TEORICO 12
2.1 Tecnología Hik Visión 12
2.2 Redes IP Convencionales 12
2.3 Redes Inalámbricas 13
2.4 Características y Relevancia 14
2.5 Componentes y Topologías de una Red Inalámbrica 15
2.5.1 Red Inalámbrica 15
2.5.2 Componentes de una Red Inalámbrica 15
2.6 Redes de Área Metropolitana 16
2.7 Packet Tracer 17
2.8 Almacenamiento 18
2.9 Necesidad de Hardware 19
2.10 Almacenamiento Directo Integrado 19

2.11 Switch 20
2.12 Router Inalámbrico 21
2.12.1 Partes más Importantes de un Router 22
2.12.1.1 Componentes Externos de un Router 22
2.12.1.1.1 Conectores RJ-45 22
2.12.1.1.2 Conector RJ-11 23
2.12.1.1.3 Conector SC/APC 23
2.12.1.1.4 Botón de Encendido y Conector 24
2.12.1.1.5 Antenas Wifi 24
2.12.1.1.6 Leds de Iluminación 24
2.12.1.1.7 Botón WPS 25
2.12.1.2 Componentes Internos de un Router 25
2.12.1.2.1 Memoria RAM 25
2.12.1.2.2 CPU 25
2.12.1.2.3 Memoria Interna 25
2.12.1.2.4 Fuente de Alimentación 26
2.13 Componentes de las LAN Inalámbrica 26
2.14 Tipos de Antenas WIFI 27
2.14.1 Antenas Direccionales 28
2.14.2 Antena Omnidireccional 28
2.14.3 Antenas Sectoriales 29
2.14.4 Access Point 29

2.15 Modelo OSI 30
2.15.1 Arquitectura Física 38
2.15.2 Tipos de Enrutamiento 39
2.15.2.1 Enrutamiento Estático 39
2.15.2.1.1 Determinación de Enrutamiento 39
2.15.2.1.2 Rutas Estáticas 40
2.15.3 Enrutamiento Dinámico 40
2.15.4 Encaminadores Inalámbricos 40
2.15.5 Enrutador con Conexiones LAN 41
2.16 Generalidades de Redes de Comunicación 41
2.16.1 Ondas de Radio 41
2.16.2 Espectro Electromagnético 43
2.17 Tipos de Cámaras 44
2.17.1 Cámaras Fijas 44
2.17.2 Cámaras de Cúpula Fijas 45
2.17.3 Cámaras IP PTZ 46
2.17.4 Cámaras IP PTZ con Cúpula 47
2.17.5 Cámaras IP Térmicas 48
2.17.6 Visión Térmica 48
2.17.7 Cámaras de Visión Nocturna 49
2.18 Estándares de la Industria 49
2.18.1 Diferencias Históricas entre Estándares 49

2.19 VENTAJAS 50
2.19.1 Vigilancia IP 50
2.20 Desventajas de la Vigilancia IP 52
2.21 DVR H.264 52
2.21.1 Características de un DVR 56
2.21.2 Preparación del Sistema 58
2.21.3 Configuración del Router 58
2.21.4. PUERTOS 59
2.22 Protocolo TCP/IP 62
2.22.1 Medios de Transmisión Guiados 63
2.23 Normas 64
2.23.1 Protección de Datos Personales en Sistemas de Video Vigilancia 65
CAPITULO III 66
3. DESARROLLO DEL PROYECTO 66
3.0 Fase de Diseño Lógico 66
3.0.1 Fase de Diseño Físico 67
3.0.2 Simulación 67
3.1 Funciones del Grabador 67
3.2 Cálculo de la Capacidad de Almacenamiento del Grabador 68
3.3 Gestión y Control del Video 68
3.4 Ancho de Banda 70
3.5 Cámara Hik Visión 70

3.5.1 Contenido del Equipo 70
3.5.2 Características de la Cámara 71
3.5.3 Sensor de Imagen 72
3.5.4 Sensor Fotoeléctrico y Procesamiento de Imagen 73
3.5.5 Frame Rate 74
3.5.6 Resolución 77
3.5.7 Iluminación Mínima 78
3.5.8 Longitud Focal Variable 78
3.5.9 Objetivos Multifocales 79
3.5.10 Alcance de Infrarrojos 80
3.5.11 Dimensiones 82
3.5.12 Requisitos del Ordenador 82
3.5.13 Instalación de Hardware 83
3.5.14 Instalación de Software CMS H264 83
3.5.15 Administrador 84
3.5.16 Configuración en los Router 86
3.5.17 Simulaciones en Packet Traicer Centro de Acogida Niño Jesús 89
3.5.18 Configuración DHCP 90
3.5.19 Sala de Monitoreo 91
3.5.20 Centro de Acogida Niño Jesús 92
3.5.21 Ingresos con Contraseña para las Cámaras 93
3.5.22 Funcionamientos de las Cámaras 94

3.5.23 Cámara 1 Funcionando 95
CAPITULO IV 96
4. CONCLUSIONES Y RECOMENDACIONES 96
4.1 Conclusiones 96
4.2 Bibliografía 97
4.3 Páginas Web 97

INDICE DE FIGURAS

FIGURA 1:Topologia 8
FIGURA 2: Redes Inalámbricas 13
FIGURA 3: Interfaz Gráfica del Packet Tracer 17
FIGURA 4 : Página Oficial 18
FIGURA 5 : Switch 20
FIGURA 6 : Router Inalámbrico 21
FIGURA 7 : Antena Direccional 28
FIGURA 8 : Antena Omnidireccionales 28
FIGURA 9 : Access Point 29
FIGURA 10 : Modelo OSI 30
FIGURA 11 : Router 38
FIGURA 12 : Ondas de Radio 41
FIGURA 13 : Espectro Electromagnetico 43
FIGURA 14: Cámaras Fijas 45
FIGURA 15: Cámara Ip fija con Cúpula 45
FIGURA 16: Cámara PTZ con Cúpula 47
FIGURA 17: Cámara IP Termica 48
FIGURA 18 : Vision Termica 49
FIGURA 19 : DVR H264 53
FIGURA 20: EquipoCompleto 55

FIGURA 21: Especificaciones 57
FIGURA 22: DHCP 58
FIGURA 23: Configuración DVR 59
FIGURA 24: Servidor Hik Vision 60
FIGURA 25: Direccionamiento de Puertos 60
FIGURA 26: Protocolo TCP/IP 62
FIGURA 27: Características de la Cámara 72
FIGURA 28: Sensor de Imagen 73
FIGURA 29: 1y 2 Multifocales 3 y 4 Par Focales y 5 Vari Focal 80
FIGURA 30 : Dimensiones 82
FIGURA 31: Instalación de Software CMS H264 84
FIGURA 32 : Centro de Acogida Niño Jesús 89
FIGURA 33: Configuración 90
FIGURA 34: Cámara en Funcionamiento 90
FIGURA 35 : Sala de Monitoreo 91
FIGURA 36 : Centro de Acogida Niño Jesús 92
FIGURA 37 : Ingreso con Contraseña 93
FIGURA 38 : Verificación de las Distintas Cámaras 93
FIGURA 39 : Funcionamiento de las Cámaras 94
FIGURA 40 : Funcionamiento de la Cámara 1 95

INDICE DE TABLAS

Tabla 1 : Capas del Modelo OSI 31

Tabla 2 : Medios de Transmisión 64

Tabla 3 : total de Datos Almacenados en 30 Días: 259.2GB 75

Tabla 4 : Total de Datos Almacenados en 30 días: 171.72 GB 76

Tabla 5 : Total de Datos Almacenados en 30 días: 1170.72GB 77

Tabla 6 : Características de la Cámara Visión 80

Tabla 7 : Materiales a Utilizar 85

CAPITULO I

1.INTRODUCCIÓN

Las cámaras de vigilancia inalámbrica ip como su propio nombre indica, utilizan el Protocolo de Internet para transmitir imágenes y señales de control en circuito cerrado, también son conocidas por el nombre de cámaras de red o network.

Una cámara de red posee la mayoría de las funciones de una cámara estándar de circuito cerrado, pero proporciona muchas más funcionalidades. De hecho, una cámara de red es una cámara analógica capaz de digitalizar sus imágenes y transmitirlas por una red.

La lente de la cámara enfoca la luz sobre el sensor de imagen entre dicha lente y el sensor, la luz atraviesa un filtro óptico que elimina la luz infrarroja de forma que se muestren los colores tal como los percibe el ser humano la necesidad de seguridad de video vigilancia en todas las ciudades a aumentado rápidamente ya sea en fábricas, oficinas, calles ,alcaldías con lo cual se hará la prevención de robos de equipos , las cámaras y videos continuamente van evolucionando para mantenerse día a día con la demanda de la población ,las cámaras de seguridad son confiables de alta calidad , todas las cámaras satisfacen con éxito los requerimientos de seguridad de la población con gran calidad en forma simple y rápida y con resultados óptimos.

El presente proyecto consiste en el despliegue de cámaras de seguridad ip con la finalidad de prevenir con eficacia acciones de injusticia como aquél que se cometió con el médico Jhiery Fernández siendo inocente fue privado de su libertad durante 6 años y medio sin prueba alguna, como también el maltrato físico y psicológico hacia los niños y niñas que habitan en esta institución niño Jesús.

Utilizando la infraestructura de comunicaciones que posee la institución, las imágenes

se enviarán desde las cámaras hacia la central de monitoreo, permitiendo su grabación digital y almacenamiento por un período que puede llegar hasta los cuatro meses dependiendo de la configuración con resultados satisfactorios en lo que respecta a las prestaciones que ofrece el sistema (como por ejemplo nitidez de imagen y capacidad de almacenamiento).

En base a ello, sobre el final de este documento se definirán posibles objetivos ("en todo los albergues") en los que puede resultar factible implementar esta solución tecnológica para dar seguridad y confianza a todos los niños y niñas en orfandad como también al personal encargado del hogar niño Jesús.

Una cámara ip, cámara de red o cámara de video de internet, es un dispositivo encargado de captar y transmitir una señal de video/audio digital a través de una red ip estándar a otros dispositivos de red, como pueden ser un pc, un nvr o un smartphone, mediante una dirección ip dedicada, un servidor web y protocolos de streaming de video, los usuarios autorizados pueden visualizar, almacenar y gestionar video de forma local o remota y en tiempo real. Cada usuario autorizado es capaz de controlar y gestionar varias cámaras al mismo tiempo desde cualquier lugar donde haya conexión de red.

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 Identificación del Problema

En el hogar niño Jesús se observó que hay bastantes problemas como la injusticia con el personal en este caso con el médico Jhery Fernández que fue acusado sin prueba alguna, maltratos hacia los niños y niñas tanto físicos como psicológicos porque no cuentan con ningún tipo de sistema de seguridad el cual hace aún más difícil de solucionar los problemas que presenta este hogar.

El 12 de noviembre de 2014 el bebé Alexander se descompuso en el hogar Virgen de Fátima, en la calle 3 de la zona de Obrajes de La Paz. Aunque no lo podían todavía saber, ello cambió la vida de varios médicos, enfermeras y cuidadoras, que se vieron envueltos en un infierno de acusaciones, malos entendidos y la perversa acción de los operadores de justicia de Bolivia.

El médico Jhiery Fernández estaba en ese momento en el Instituto de Rehabilitación Infantil (IRI), de la calle 5 de Obrajes, atendiendo a una niña que se había hecho una herida, cuando recibió la llamada de que un bebé, en el hogar Virgen de Fátima, tenía un profuso sangrado. Se fue de inmediato allí, pero cuando llegó, el bebé ya había sido transportado a otro centro y murió al día siguiente.

Fernández pensó que todo había acabado allí en ese respecto. Pero no, al poco tiempo fue acusado nada menos que de violación y de haber causado la muerte del bebé. ¡Aunque demostró, mediante testigos y llamadas telefónicas, que no estuvo en el lugar! Así funciona la enferma justicia boliviana, que se basó en un reporte forense mal efectuado por la médica Ángela Mora. Fernández espera ser liberado tras conocerse un audio filtrado a los medios y en el que la jueza Patricia Pacajes admite que el médico es inocente y que nunca hubo tal violación. El bebé murió aparentemente por una descompensación por una crisis cardio respiratoria. En el audio, la jueza también indica que Mora mantenía un amorío con el fiscal general Ramiro Guerrero.

Junto con Fernández, también fueron sentenciadas a dos años de presidio a la médica internista del Hospital del Niño, Sandra Madeni, y a la enfermera del hogar, Lola Rodríguez, por los supuestos delitos de incumplimiento de deberes y homicidio culposo.

La muerte del bebé causó un impacto mediático y jurídico tan grande, que el hogar tuvo incluso que cambiar de nombre, al de Niño Jesús, donde el personal intentó con el paso de las semanas y los meses recuperar la normalidad de sus actividades.

1.2.2 Formulación del Problema

El presente proyecto busca satisfacer las necesidades de esta institución Centro de Acogida niño Jesús para que pueda recuperar la confianza y seguridad.

El cual consiste en realizar un diseño de un sistema de seguridad inalámbrica con cámaras ip con simulación cisco packet tracer para implementar en el Hogar niño Jesús con la finalidad de tener el control total mediante las cámaras ip las 24 horas y los 7 días de la semana.

1.3 OBJETIVOS

1.3.1 Objetivo General

Diseñar e implementar cámaras ip para mejorar los niveles de seguridad dentro del Centro de Acogida niño Jesús de tal forma que disminuyan los maltratos psicológicos y físicos hacia los niños como también las injusticias a causa de los maltratos que se presentan en esta institución pública brindándoles mayor seguridad y control en este centro orfanatorio para niños de 0 a 6 años de edad, de esa manera se pueda proporcionar una mejor calidad de vida respetando todos los derechos de los niños y niñas.

1.3.2 Objetivos Específicos

- *Implementar cámaras de seguridad para la obtención de imágenes audio y videos de alta calidad.*
- *Garantizar el correcto funcionamiento y actualización del sistema de seguridad ip del hogar para dar soporte de seguridad a la institución, a través de mantenimientos correctivos y preventivos.*
- *Seleccionar el método de seguridad más apropiado para el Centro de Acogida niño Jesús.*

- *Mantener vigilada el Centro de Acogida niño Jesús mediante estas cámaras ip que ofrecen señales de video y audio en directo al cual se puede acceder usando un navegador de internet de esa manera se evitaría la gran parte de injusticia que sufren los niños y niñas.*

- *Aumentar los niveles de satisfacción, confianza y seguridad por parte de la institución con respecto a todo el personal, ampliando las medidas de seguridad y ofreciendo mayores controles contra maltratos por parte del personal que presta sus servicios dentro del Centro de Acogida niño Jesús.*

1.4 JUSTIFICACION

1.4.1 Justificación Tecnológica.

La necesidad de adaptar un sistema de seguridad en la institución es importante. Para lo cual se utilizaran dispositivos de tecnología de punta son cámaras ip con la finalidad que pueden comunicarse mediante la red de manera inalámbrica que quiere decir que cada cámara tiene una dirección ip también tiene la capacidad de almacenar información directamente en la nube.

Antes de instalar un sistema de cámaras IP, es importante saber si la red tiene el ancho de banda (la capacidad de transmitir información) para apoyar a las cámaras que desee utilizar. Requisitos de ancho de banda de cámaras web pueden variar de 100 Kbit / s para una cámara web de los consumidores a 9 Mbit / s o más para una cámara de seguridad de alta resolución. El ancho de banda necesario depende de varios factores, que pueden controlarse para limitar la carga sobre la red.

Como norma general podemos establecer un ancho de banda no menos de 3Mbps con el fin de lograr los mejores efectos de video, el ancho de banda de un canal de HD.

1.4.2 Justificación social.

Este proyecto es muy importante su implementación y aplicación, ya que en el hogar no cuentan con ningún tipo de sistema de seguridad ni policías, para el respectivo control de la institución, es por esto que este proyecto beneficiara tanto, a los niños y niñas Como también a al personal que presta sus servicios en el hogar niño Jesús.

1.4.3 Justificación Académica.

En la implementación del proyecto un pilar fundamental para la ejecución del proyecto son los conocimientos adquiridos de la carrera de Electrónica y Telecomunicaciones a nivel licenciatura de la Facultad de Tecnología de la Universidad Mayor de San Andrés, con la aplicación de los conocimientos teóricos y prácticos de líneas de transmisión y antenas, propagación electromagnética, sistemas de telecomunicaciones, fibra óptica.

1.5 LIMITES Y ALCANCES

1.5.1 Limites

- *El proyecto tiene la finalidad de instalar cámaras con direcciones ip de alta precisión de esa manera poder controlar la institución.*
- *El presente proyecto pretende la implementación de servicio de seguridad con cámaras ip para la seguridad de todos los niños y personal del orfanatorio.*

1.5.2 Alcances

1.5.2.1 Delimitación Espacial

El desarrollo del proyecto abarcara todo el contexto de los ambientes de la institución niño Jesús ya que debe hacerse un reconocimiento de todo el perímetro externos e

internos y otros puntos estratégicos para la implementación de las cámaras ip.

1.5.2.2 Delimitación Temporal

El tiempo estimado de implementación es de 3 meses o más ya que es necesario realizar el cumplimiento de los objetivos establecidos de acuerdo al plan y cronograma de actividades que se va tener luego se deben realizar barias pruebas para el correcto funcionamiento del sistema.

1.5.2.3 Delimitación Temática

En el hogar orfanatorio niño Jesús se presentó bastante maltrato hacia los niños y niñas menores de 6 años, a causa de los maltratos también se cometieron mucha injusticia donde muchos del parte personal encargado fueron afectados injustamente. De esa manera se pensó que es necesario instalar un sistema de seguridad con cámaras ip para brindarles protección y seguridad a todos los niños y el personal encargado del hogar.

1.6 SOLUCION PROPUESTA

1.6.1 Topología

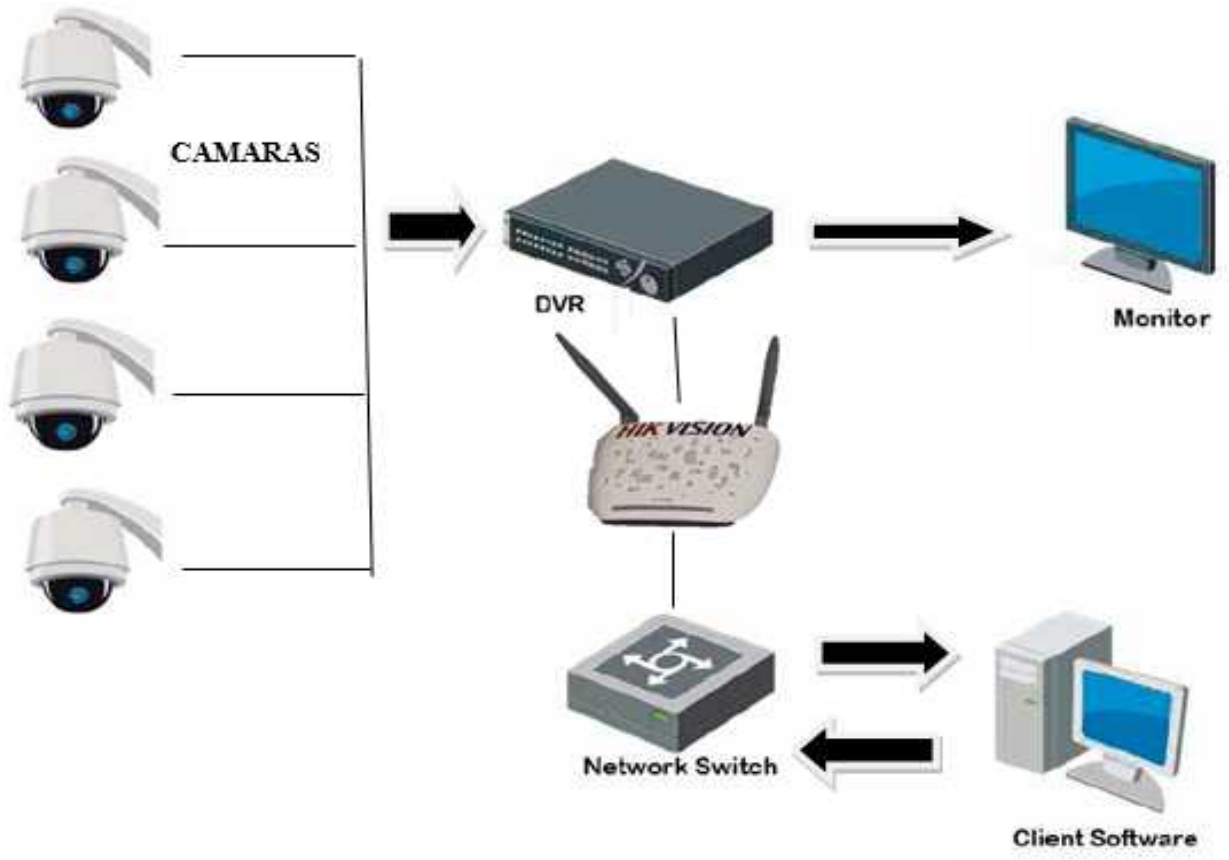

FIGURA 1:Topologia

Fuente: Propia

1.6.2 Funcionamiento

a) ***Primer Paso. -*** *Lista de los Materiales.*
    1. *Cámaras HIK-VISION*
    2. *Swicth*
    3. *Cables de red UTP categoría 6 con conectores RJ 45*
    4. *Router*
    5. *DVRs dispositivo de almacenamiento*

b) ***Segundo Paso.-*** *Instalación del software.*

c) ***Tercer Paso.-****Asignar a cada dispositivo una dirección para configuración del software*

d) ***Cuarto Paso.-****Para capturar imágenes instalar otro software iVMS-4200*

e) ***Quinto Paso.-****Registro administrativo en el software.*

f) ***Sexto Paso.-****Obtención de dispositivos conectados agregar las direcciones.*

g) ***Séptimo Paso.-****Verificar que puertos están trabajando.*

h) ***Octavo Paso.-****Hacer una prueba de conectividad.*

i) ***Noveno Paso.-****Ver la cámara ya instalada.*

j) ***Decimo Paso.-****Finalmente visualizar las cámaras en tiempo real.*

El funcionamiento del presente proyecto se basa principalmente en la instalación de cámaras IP el cual será controlado mediante una computadora como también inalámbricamente por todo el personal autorizado mediante los Smartphone.

1.6.3 Central de Monitoreo

La Central de Monitoreo (CM) es el espacio físico especialmente acondicionado en el cual se almacena, gestiona y controla la información que proviene del sistema de vigilancia por cámaras. Ante un evento reportado los operadores de la central darán intervención a la fuerza policial conforme a un protocolo de acción.

En esta etapa inicial se pretende que la CM comience a prestar servicio las 24 horas de lunes a domingo. Debe asegurarse en el centro de monitoreo el confort necesario para que los operadores puedan actuar en simultáneo, como también el descanso suficiente para cumplir efectivamente su labor. Asimismo se deberán establecer medidas de seguridad y acceso restringido para el resguardo del equipamiento.

1.6.4 Protocolo de Acción

La implementación tiene como requisito excluyente la confección de un protocolo a utilizar por el personal policial asignado al Central de Monitoreo, que debe cumplir con las siguientes condiciones:

- *Debe garantizar la confidencialidad e invulnerabilidad de la información que produce el sistema.*
- *Como actuará el personal policial, ante eventos reportados por las cámaras y ante fallas en el sistema, garantizando el inmediato accionar en salvaguarda de los niños y niñas como también al personal de la institución.*

Se entiende que la elaboración de este documento deberá implicar necesariamente la participación de la Secretaría de Informática y del responsable de las guardias policiales de esta institución debe ser administrada bajo normas estrictas que contemplen la seguridad e inviolabilidad de los derechos de privacidad.

1.6.5 Adquisición e Instalación del Equipamiento

En los pliegos de licitación se deberán prever que el contratista realice la instalación completa, con equipos, materiales y mano de obra necesarios para la puesta en marcha del sistema, incluyendo el cableado interno, hardware y software, documentación y capacitación de los operadores del sistema.

Es necesario que el proveedor brinde capacitación a los operadores del sistema (personal policial) que prestarán servicios en la Central de Monitoreo.

1.6.6 Procedimientos para el diseño o Implementación del Proyecto

Estará a cargo del proveedor del sistema (software, cámaras, hardware) el mantenimiento preventivo y correctivo (incluyendo la actualización del software, en caso de ser necesario). Asimismo de brindar asistencia técnica para la puesta en funcionamiento del mismo.

Por otra parte, la gestión y administración del sistema, comprende las siguientes funciones principales:

- *Configuración y programación de tareas de grabación de eventos, y organizar el archivo digital.*
- *Verificar el correcto funcionamiento del hardware y software.*
- *Establecer los niveles adecuados de seguridad del sistema, asegurando el funcionamiento ante fallas, caída del sistema intencional o no, entre otros aspectos.*
- *Gestión de políticas de derechos de los usuarios, estableciendo distintos usuarios con privilegios de visualización, usuarios con privilegio de reproducción de video grabada, usuario con privilegios de exportación o administrador del sistema para poder ser accedido en forma remota.*

Deberá determinarse si esta función estará a cargo de la Secretaría de Informática, o bien, en función de los recursos actuales de la misma, se contrata en forma externa conjuntamente con la adquisición del equipamiento.

CAPITULO II

2.FUNDAMENTO TEORICO

2.1 Tecnología Hik Visión

Es el más grande fabricante y proveedor de equipos de video vigilancia a nivel mundial, llevando hasta el último rincón del mundo soluciones concretas con su amplia gama de productos que comercializa, destacando sobre sus competidores por su calidad, alta tecnología, funcionalidad, ingeniería, definición y diseño que armoniza en cualquier lugar donde se vaya a instalar.

Cumple con los estándares más altos de calidad y orientado a la grabación de cámaras de ultra alta resolución sin perder ningún detalle de la imagen.

2.2 Redes IP Convencionales

El primer aspecto a considerar es cuánta potencia de red se necesita en los conmutadores o Switch que permiten a las cámaras y servidores comunicarse entre sí e incluso compartir una conexión a Internet. Como aproximación inicial pesimista, podemos estimar la necesidad de ancho de banda de cada cámara IP en torno a 2 ó 3 Mbits, suponiendo que trabaja en alta definición y una Tasa de fotogramas por segundo alta.

Si se dispone de una LAN o WAN previamente instalada, es preciso determinar lo congestionada que está, dependiendo del número de cámaras que se piensa operar con cada conmutador menos de 10 cámaras IP conectadas simultáneamente, en este caso suele ser suficiente con un conmutador de red básico de 100Mbit, sin considerar restricciones en cuanto al ancho de banda es la solución más habitual y es suficiente con la red local existente en la mayoría de casos.

2.3 Redes Inalámbricas

FIGURA 2: Redes Inalámbricas

Fuente:http://zoominformatica.com/blog/como-configurar-camara-ip/

Extender un cable óptico o entrelazado entre una cámara IP y el resto de la Red de Área Local, no deja de ser un proceso poco práctico y costoso. Como alternativa, las cámaras IP nos brindan la posibilidad de utilizar una red inalámbrica, para ello necesitaremos al menos un puente o un enrutador inalámbrico, que una la cámara IP con el resto de la red local.

Las redes de cámaras sin hilos son especialmente útiles en locales en los que no se pueden realizar instalaciones de cableado, para cambiar fácilmente la ubicación de las cámaras, para poder utilizar emplazamientos en exteriores, para puentear dos redes de vigilancia, o bien para usuarios que simplemente buscan comodidad de instalación.

La principal desventaja de este tipo de redes es que, además de ofrecer un menor ancho de banda, presentan mayores dificultades cuantos más equipos estén conectados a la red. Los tiempos de espera entre peticiones hacen que la red pueda llegar a colapsar totalmente. Una red inalámbrica debe hacerse privada y segura. De lo contrario, cualquier agente exterior podría utilizar los servicios de las cámaras, manipulándolas o anulándolas directamente.

Existen numerosos procedimientos de seguridad complementarios entre sí, pero en redes que no sean de alta seguridad, bastaría con una encriptación. La más utilizada es WEP, basada en RSA RC4 este método no cifra la clave, por lo que se considera básico, existen extensiones del procedimiento como WEP plus, WEP2 o WEP dinámica, que mejoran significativamente la seguridad.

No obstante, el nuevo estándar WPA, que añade una clave cifrada, sería la opción inmediata para mejorar la seguridad de la red inalámbrica en todo caso, cuando se disponga una red inalámbrica, se asumirán una serie de reglas imprescindibles:

1. *Habilitar la encriptación anteriormente descrita en enrutadores y cámaras.*
2. *Habilitar verificación de usuario mediante contraseñas para todas las cámaras conectadas a la red.*
3. *No conectar más de cuatro o cinco, cámaras por punto de acceso. Como ya se ha comentado, los Router inalámbricos no tienen la misma capacidad de conmutación ni el mismo ancho de banda que un Switch de red convencional.*

2.4 Características y relevancia

La función principal de una red inalámbrica es la de establecer una comunicación entre distintos dispositivos sin que en la misma medien cables.

Esta circunstancia tiene una gran relevancia desde el punto de vista de los costos, ahorrándose una gran cantidad de dinero por los cables que serán dejados de lado. No obstante, el principal problema que tienen este tipo de redes es el de la seguridad, circunstancia que ha hecho necesario el hecho de desarrollar estándares específicos para mantenerlas libres de cualquier ataque, de cualquier robo de información que pudiera acaecer; en el caso del internet, estos sistemas de seguridad llevan el nombre de WPA, WP2 y WEP.

2.5 Componentes y Topologías de una Red Inalámbrica

2.5.1 Red Inalámbrica

La red inalámbrica se utiliza para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas, la transmisión y la recepción se realizan a través de puertos.

Una de sus principales ventajas es notable en los costos, ya que se elimina todo el cable Ethernet y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe tener una seguridad mucho más exigente y robusta para evitar a los intrusos.

2.5.2 Componentes de una Red Inalámbrica

La antena es un dispositivo que permite transmitir y recibir ondas de radio, una de las cosas que hace es convertir la onda guiada (señales digitales) por la línea de transmisión (cable o guía de onda) en ondas electromagnéticas que se pueden transmitir por el espacio libre.

Las Antenas Direccionales Orientan la señal en una dirección muy determinada con una haz estrecho pero de largo alcance, actúa de forma parecida a un foco que emite un haz

concreto y estrecho pero de forma intensa (mas alcance), los cuales envían la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor y fuera de la zona de cobertura, la recepción es nula.

2.6 Redes de Área Metropolitana

*Una **red de área metropolitana** (**MAN**, Metropolitana Área Network) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa, proporcionando capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado (MAN BUCLE).[1] La tecnología de pares de cobre se posiciona como la red más grande del mundo una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50 ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades de 10 Mbit/s o 20 Mbit/s, sobre pares de cobre y 100 Mbit/s, 1 Gbit/s y 10 Gbit/s mediante fibra óptica.*

Otra definición podría ser: Una MAN es una colección de LANs o CANs dispersas en una ciudad (decenas de kilómetros). Una MAN utiliza tecnologías tales como ATM, Frame Relay, DSL (Digital Subscribir Line), WDM (Wavelenght División Multiplexing), ISDN, E1/T1, PPP, etc. para conectividad a través de medios de comunicación tales como cobre, fibra óptica, y microondas.

Las Redes MAN BUCLE, se basan en tecnologías Bonding, de forma en que los enlaces están formados por múltiples pares de cobre con el fin de ofrecer el ancho de banda necesario.

Las redes de área metropolitana garantizan unos tiempos de acceso a la red mínimos, lo cual permite la inclusión de servicios síncronos necesarios para aplicaciones en tiempo real, donde es importante que ciertos mensajes atraviesen la red sin retraso incluso cuando la carga de red es elevada.

Entre nodo y nodo no se puede tener, por ejemplo más de 100 kilómetros de cable. Se puede tener en aproximación límite unos 20 km de cable, pero no se sabe en qué momento se puede perder la información o los datos mandados.

Los servicios síncronos requieren una reserva de ancho de banda; tal es el caso del tráfico de voz y vídeo. Por este motivo las redes de área metropolitana son redes óptimas para entornos de tráfico multimedia, si bien no todas las redes metropolitanas soportan tráficos isócronos (transmisión de información a intervalos constantes).

2.7 Packet Tracer

Cisco ofrece una herramienta con la que es posible diseñar redes y realizar simulaciones sobre su uso. Esta aplicación gratuita se llama Packet Tracer y puede descargarse desde la web oficial de Cisco.

Con esta herramienta, estudiantes, docentes y profesionales pueden testear el funcionamiento de redes, ciber seguridad y el internet de las cosas (IoT).

FIGURA 3: Interfaz Gráfica del Packet Tracer

Fuente:http://luchotechnical.blogspot.com/2011/11/definicon.html

FIGURA 4 : Página oficial

Fuente:http://luchotechnical.blogspot.com/2011/11/definicon.html

Cisco ofrece una herramienta potente y útil para el aprendizaje, docencia y prueba de redes y dispositivos de comunicaciones, y lo hace de forma gratuita. Al utilizar Cisco Packet Tracer se puede comprobar el funcionamiento de una red y los cambios que se producen en la misma, sin tener que modificar la red real, siendo muy útil para probar nuevas tecnologías y ver cómo afectarían en el comportamiento y rendimiento de la red.

2.8Almacenamiento

Existen dos opciones para el almacenamiento de datos en una red de vigilancia IP completa. La más común consiste en centralizarla en el centro de control, como un disco duro PC del propio puesto de trabajo. Otra opción más descentralizada consiste en implementar cámaras compatibles con memoria interna de gran capacidad, que puede ser descargada o gestionada remotamente gracias al firmware de la propia cámara.

2.9 Necesidad de Hardware

De manera análoga a la que un ordenador personal almacena documentos y archivos, la información de vídeo se debe guardar en un soporte físico, bien en un servidor central dedicado a tal efecto o bien dentro de cada una de las cámaras si estas lo soportan.

La particularidad del almacenamiento de vigilancia reside en la necesidad de guardar continuamente gran cantidad de información de vídeo, substituyendo dos datos antiguos por datos nuevos de forma cíclica e ininterrumpida la voracidad de estos sistemas hacen que el formato de compresión y los servicios de almacenamiento sean críticos en la elección del hardware.

Para estimar las necesidades de almacenamiento debemos tener en cuenta:

1. *El número de cámaras conectadas a la red de vigilancia*
2. *El tiempo que dichas cámaras estarán operando*
3. *La configuración de cada cámara (resolución y fps)*
4. *Método de compresión de Vídeo*

2.10 Almacenamiento Directo Integrado

El almacenamiento directo es probablemente la solución más común para el almacenamiento en discos duros en instalaciones de vigilancia IP. En este caso, el disco pertenece al mismo PC servidor que incorpora los programas de gestión y control del sistema. Con cuatro discos duros de 400 GB suele ser más que suficiente para pequeñas y medianas redes de vigilancia IP.

Para redes masivas o en las que se quiera llevar un historial extenso y detallado, o que

simplemente pueda exceder las limitaciones del almacenamiento directo, puede ser

conveniente dedicar más de un servidor al almacenamiento de vídeo, normalmente se trata de instalaciones de más de 50 cámaras de vídeo y redes basadas en fibra óptica, para las cuales existen dos soluciones principales: NAS y SAN.

2.11 Switch

FIGURA 5 : Switch

Fuente:http://redes-jhair.blogspot.com/

Un Switch es un dispositivo de hardware, que también es conocido como conmutador, utilizado para establecer interconexiones en redes informáticas.

En pocas palabras, es un aparato que se utiliza para filtrar y encaminar paquetes de datos entre segmentos de redes locales y ofrecer conexión a los equipos que conforman una subred LAN.

El Switch opera en la capa de enlace del modelo OSI, siendo completamente independiente de los protocolos que se ejecutan en las capas superior es de la red. Tiene la capacidad de escuchar todos los puertos y construir tablas para realizar un mapeo de las direcciones MAC, con el puerto a través del cual se pueden alcanzar estas direcciones.

El Switch o conmutador opera de manera similar a una pequeña central telefónica. Cada vez que un host envía un mensaje a un segmento de red en donde se encuentra el conmutador, dicho mensaje será leído por el conmutador y enviado directamente al equipo que corresponda, de esta manera, se limita las colisiones de red.

Por lo general, el Switch o conmutador es utilizado para ofrecer servicio de red e Internet a un grupo de equipos alejados de la red principal (subred) y para establecer comunicaciones entre segmentos de redes, sin minimizar la calidad de flujo de información entre los equipos que forman parte de dicha red.

2.12Router Inalámbrico

FIGURA 6 : Router Inalámbrico

Fuente: http://culturacion.com/

Un Router inalámbrico o Ruteador inalámbrico es un dispositivo que realiza las funciones de un Router, pero también incluye las funciones de un punto de acceso inalámbrico. Se utiliza comúnmente para proporcionar acceso a Internet o a una red informática. No se requiere un enlace por cable, ya que la conexión se realiza sin cables, a través de ondas de radio. Puede funcionar en una LAN cableada (local área network), en una LAN sólo-inalámbrica (WLAN), o en una red mixta

cableada/inalámbrica, dependiendo del fabricante y el modelo.

Los Routers Inalámbricos, son pequeños equipos especialmente diseñados para trabajar sin sistemas de cables y ofrecer conexión de red a un ordenador o a un grupo de ordenadores.

Estos dispositivos, están compuestos por una entrada de cable que los conecta a la red y un sistema de antena que realiza el enlace inalámbrico de los equipos que se requiere conectar al servicio de Internet o, a la red interna de una empresa, institución u hogar, según sea el caso.

2.12.1 Partes más Importantes de un Router

Hay que tener en cuenta que un Router dispone de ***componentes internos, externos*** *y también a nivel de software. Hay partes que son más visibles y que por tanto pertenecen a la parte externa, mientras que otras muchas de vital importancia están en el interior y no podemos verlas salvo que abramos el aparato.*

Como cualquier dispositivo para que funcione correctamente va a necesitar que ciertas partes o componentes estén en perfecto estado y no tengan ningún tipo de problema. De esta forma podremos hacer uso de la conexión de manera fluida y estable.

Vamos a explicar ***cuáles son estos componentes****, tanto internos como externos, que resultan vitales en un Router. De esta forma sabremos un poco más sobre el funcionamiento de este aparato y cómo evitar que pueda tener problemas. En ocasiones una mala velocidad o cortes de conexión podrían ocurrir por algún fallo con alguno de estos elementos.*

2.12.1.1 Componentes Externos de un Router

2.12.1.1.1Conectores RJ-45

*Los **conectores RJ-45** o cables de Ethernet están presentes en todos los Routers. Básicamente es el cable al que conectamos el ordenador para poder acceder a la red.*

Normalmente un Router suele venir con cuatro puertos RJ-45, pero la cifra puede variar. El número que tenga será la cifra de dispositivos que podremos conectar mediante cables. Debemos tener en cuenta que hay puertos Gigabit Ethernet y puertos Fast Ethernet. Los primeros son los que nos permiten obtener velocidades de hasta 1 Gbps, algo que es necesario para lograr la máxima velocidad de fibra óptica. Los segundos están limitados a 100 Mbps y están presentes en Routers más antiguos.

Hay que mencionar que no todos los ordenadores tienen este tipo de conector, por lo que solo podremos conectar dispositivos que sean compatibles. También podemos incluir aquí servidores, discos duros NAS, etc. Eso sí, hay conectores USB que permiten también conectar cables RJ-45 y tener Internet en portátiles pequeños.

2.12.1.1.2 Conector RJ-11

*Los Routers cuentan con un **conector RJ-11**. Es el cable de la línea telefónica, algo necesario para poder tener señal de Internet. Es otro de los componentes externos importantes con los que cuenta este tipo de aparato.*

2.12.1.1.3 Conector SC/APC

*Los Routers de fibra óptica cuentan con un **conector SC/APC**. Es un cable más fino que ofrece la conexión de fibra óptica.*

Hay que mencionar que este tipo de conector solo estará presente si tenemos un Router de fibra óptica. No aplica por tanto a los Routers de ADSL, que sería una tecnología más antigua.

2.12.1.1.4 Botón de Encendido y Conector

Algo básico y esencial en un Router es tener un ***botón de encendido*** *y un* ***conector de corriente****. Es algo necesario para conectarlo a la electricidad y poder funcionar.*

Normalmente el botón se encuentra en la parte de atrás y nos permite apagar fácilmente el Router sin tener que desconectar el cable. Una manera rápida de reiniciarlo en caso de tener algún problema. Como consejo, si tuviéramos que reiniciarlo por algún problema, es importante que lo mantengamos apagado al menos 30 segundos. Solo así podremos realizar este proceso correctamente.

2.12.1.1.5 Antenas Wifi

No es algo que esté siempre presente, pero muchos Routers sí que cuentan con ***antenas externas****. Permiten orientar y mejorar la cobertura inalámbrica. Puede ser una o varias. Los aparatos más orientados en el gaming suelen tener de seis a ocho antenas incluso. De esta forma permiten orientar mejor la señal y evitar pérdida de cobertura en determinados momentos.*

En ocasiones podemos encontrarnos con un modelo de Router que únicamente tiene antenas internas. Por tanto no veríamos ninguna antena en la parte de fuera, aunque igualmente tendría la misión de poder ofrecer red de buena calidad hasta una determinada distancia.

2.12.1.1.6 Leds de Iluminación

Prácticamente todos cuentan con diferentes ***LEDs*** *de estado. Se iluminan si estamos haciendo uso de la conexión inalámbrica, por ejemplo, así como cuando pueda haber algún problema.*

En caso de fallar la conexión podría parpadear o iluminarse en rojo, según el modelo. Es una forma de tener información visual del estado de los diferentes componentes y conexiones.

2.12.1.1.7 Botón WPS

Es un botón que nos permite gestionar conexiones con otros dispositivos. Una manera de ***vincular otros aparatos*** *sin tener que introducir la contraseña. Por ejemplo cuando queramos vincular rápidamente un PLC o amplificador. Normalmente los Routers cuentan con este botón.*

2.12.1.2 Componentes Internos de un Router

2.12.1.2.1 Memoria RAM

Es la memoria donde el Router ***almacena la caché****. Es algo básico en cualquier dispositivo y en estos aparatos no pueden faltar. Tiene capacidad suficiente para permanecer encendido durante meses sin problema. Allí se gestiona el tráfico, así como los diferentes aspectos del firmware que tengamos instalado.*

2.12.1.2.2 CPU

Como cualquier otro aparato, un Router también cuenta con una ***CPU****. Es lo que permite procesar las instrucciones e información. Sirve para encender el aparato y que funcione correctamente. La potencia de esta CPU permitirá administrar más o menos dispositivos conectados al mismo tiempo sin tener problemas que afecten al rendimiento.*

2.12.1.2.3 Memoria Interna

Otro de los componentes internos de un Router es la ***memoria interna****. Allí podemos*

instalar el firmware del dispositivo y actualizarlo. También incluso agregar ciertos componentes en algunos modelos. Según el modelo que estemos utilizando, esa memoria interna puede ser de mayor o menor capacidad.

2.12.1.2.4 Fuente de alimentación

Un último componente vital para el buen funcionamiento es la ***fuente de alimentación****. Es necesario para que funcione correctamente el dispositivo. Está presente en cualquier tipo de aparato de este tipo. Algunos Routers además pueden ser portátiles, por lo que cuentan con una batería integrada que permite poder utilizarlo varias horas sin necesidad de enchufarlo a la línea eléctrica.*

En definitiva estos son los componentes más importantes de un Router. Lo hemos dividido en parte externa e interna. Lógicamente son muchos más los componentes que permiten navegar por Internet, pero estos que hemos mencionado son los más importantes y que podíamos calificar como vitales.

2.13 Componentes de las LAN Inalámbrica

NIC: (Network Interface Controller) o tarjeta de interface de red. Una NIC esta desmañada para comunicarse a través de una red informática. Permite a los usuarios conectarse entre sí mediante WIFI en impresoras, pc, Router ETC.; deben tener una tarjeta nic para comunicarse.

La funcionalidad de la nic se encuentra a menudo en el chipset de la placa base, cada nic tiene un número de serie de un código único llamado "acceso a los medos" (dirección MAC).Tienen velocidades diferentes hasta de un1gbps.

Un controlador de interface inalámbrica (WNIC) usa una antena para comunicarse con mayor frecuencia a 2.4GHZ.

2.14Tiposde Antenas WIFI

Estas frecuencias libres son: 902-928 MHz; 2.400-2.4835 GHz; 5.725-5.850 GHZ; tomando como ventaja esta disposición se realizó la elección de las antenas inalámbricas utilizadas para este proyecto, en la frecuencia de 5.15-5.825 GHz, debido a que en este rango de frecuencias existe menos tendencia de interferencia con otros dispositivos inalámbricos y la potencia en esta frecuencia permite garantizar la adquisición de imágenes sin alteraciones por la calidad de la señal.

La tecnología Hiperlan2 es un estándar desarrollado por el ETSI (European Telecommunications Standard Institute) para redes WLAN y hace uso de la tecnología OFDM, cuyas principales bondades son: - Alta velocidad de transmisión (54 Mbps). - Búsqueda automática de frecuencia (selecciona el canal de radio adecuado, basándose en escuchar los puntos de acceso vecinos con el fin de eliminar posibles interferencias). - Orientado a conexión. - Seguridad, movilidad. - Calidad de servicio (QoS). - Bajo consumo.

La tecnología OFDM (Orthogonal Frequency División Multiplexing) es una tecnología de modulación digital, multicanal y se considera una piedra angular para los comunicaciones de radio frecuencia futuras de alta velocidad; su técnica consiste en distribuir los datos en un gran número de canales que se encuentran espaciados entre sí, con distintas frecuencias que son precisas. Es muy útil en lugares dispersos en el espacio, donde las señales de radio son reflejadas.

Una de sus mayores ventajas es la alta resistencia a las interferencias producidas por las ondas reflejadas en los objetos del entorno (eco o multipath). Actualmente se utiliza tanto en redes 802.11b y 802.11g en transmisiones de alta velocidad en redes telefónicas como las ASDL y en radiodifusión de señales de televisión digital terrestre en Europa, Japón y Australia.

2.14.1 Antenas Direccionales

Orienta la señal en una dirección muy determinada con un haz estrecho pero de largo alcance.

FIGURA 7 : Antena direccional

Fuente:http://manejoredes.blogspot.com

2.14.2 Antena omnidireccional

Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. "Envían la información teóricamente a los 360°".

FIGURA 8 : Antena omnidireccionales

Fuente:http://manejoredes.blogspot.com

2.14.3 Antenas Sectoriales

Son la mezcla de las dos antenas anteriores, emiten un haz más amplio que una direccional, pero no tan amplio que una omnidireccional.

Estas antenas se miden por DBI (Decibelio Isotrópico) es una unidad para medir la ganancia de una antena.

2.14.4 Access Point

FIGURA 9 : Access Point

Fuente:http://manejoredes.blogspot.com

Es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica, también puede transmitir datos por los dos medios (alámbrica e inalámbrica). Tiene una dirección IP asignada para poder ser configurado.

El Access Point tiene tres tipos de acceso:

- ***Modo Root:*** *Este es el modo más común donde múltiples usuarios acceden al punto de acceso al mismo tiempo.*
- ***Modo Repeater:*** *Se utiliza cuando se quiere extender más allá la señal.*
- ***Modo Bridge:*** *Se hace un puente inalámbrico entre dispositivos, dos puntos de*

acceso en modo Bridge solo hablaran entre ellos, este tipo de conexión es útil cuando están conectados dos edificios separados sin cables.

2.15 Modelo OSI

El modelo OSI está conformado por 7 capas o niveles de abstracción. Cada uno de estos niveles tendrá sus propias funciones para que en conjunto sean capaces de poder alcanzar su objetivo final. Precisamente esta separación en niveles hace posible la intercomunicación de protocolos distintos al concentrar funciones específicas en cada nivel de operación.

El modelo OSI no es la definición de una topología ni un modelo de red en sí mismo. Tampoco especifica ni define los protocolos que se utilizan en la comunicación, ya que estos están implementados de forma independiente a este modelo.

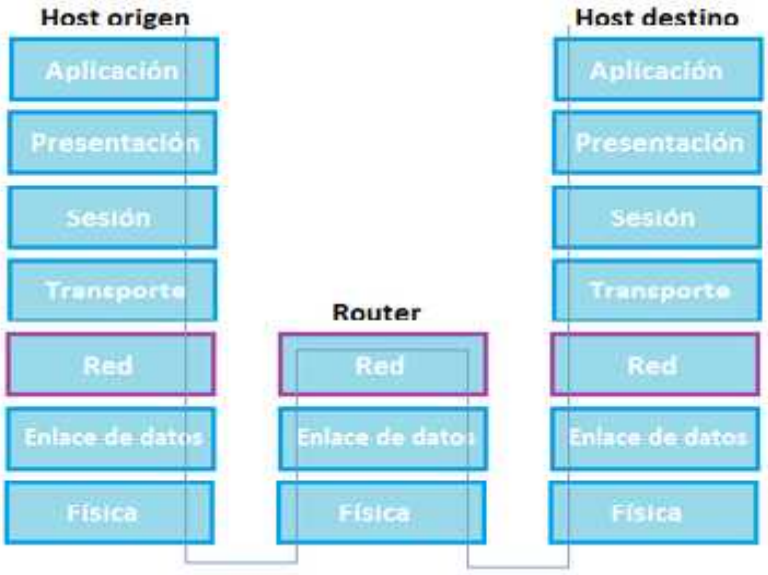

FIGURA10 : Modelo OSI

Fuente: https://commons.wikimedia.org/wiki/File:OSI_model_router.png

Las siete capas de abstracción del modelo OSI pueden definirse de la siguiente manera, en orden descendente:

Tabla 1 : Capas del Modelo OSI

Número	***Nombre***	***Responsabilidad***	***Descripción***
Capa 7	*Aplicación*	*Responsable de los servicios de red para las aplicaciones*	*Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. La capa de aplicación establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos. Esta garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.*

Capa 6	*Presentación*	*Transforma el formato de los datos y proporciona una interfaz estándar para la capa de aplicación*	*Su objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres números, sonido o imágenes, los datos lleguen de manera reconocibles. Esta capa es la primera en trabajar más el contenido de la comunicación que en cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas. Por lo tanto, podemos resumir definiendo a esta capa como la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos.*
Capa 5	*Sesión*	*Establece, administra y finaliza las*	*Esta capa también permite cifrar los datos y comprimirlos. Como su*

		conexiones entre las aplicaciones locales y las remotas	*nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos.* *Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación. Pero este protocolo debe transportarse entre máquinas a través de otros protocolos. Con SAP, los servidores permiten a los enrutadores crear y mantener una base de datos con la información actualizada de los servidores de la interred. La capa de transporte segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema*

			del host receptor.
Capa 4	*Transporte*	*Proporciona transporte confiable y control del flujo a través de la red*	*El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los protocolos de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro capas inferiores se encargan del transporte de datos. TCP crea conexiones a través de las cuales puede enviar flujos de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.*
Capa 3	*Red*	*Responsable del direccionamiento lógico y el dominio del enrutamiento*	*Su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. IPX/SPX Es una familia de protocolos de red desarrollados por novell y utilizado por su sistema operativo de red netware. El IPX Es un protocolo de datagramas rápido*

			orientados a comunicaciones sin conexión que se encarga de transmitir datos a través de la red, incluyendo en cada paquete la dirección de destino. La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico.
Capa 2	*Enlace de Datos*	*Proporciona direccionamiento físico y procedimientos de acceso a medios*	*Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico, la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos. FDDI Proporciona un 100 Mbits/s óptico estándar para la transmisión de datos en una red de área local.*
Capa 1	*Física*	*Define todas las especificaciones eléctricas y físicas de*	*La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y*

		los dispositivos	*funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.* *Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidos por las especificaciones de la capa física. Bluetooth es una especificación industrial para Redes Inalámbricas de Área Personal que posibilita la transmisión de voz y datos entre diferentes dispositivos. ADSL Consiste en una transmisión analógica de datos digitales apoyado en el par simétrico de cobre que lleva la línea telefónica convencional. USB Es un estándar industrial desarrollado en los años 1990 que define los cables, conectores y protocolos usados en un bus para conectar , comunicar y proveer de alimentación eléctrica entre ordenadores, periféricos y*

			dispositivos electrónicos. *Consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional.*

Un roúter, enrutador, (del inglés Router) o en caminador, es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función es la de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

Por ser los elementos que forman la capa de red, tienen que encargarse de cumplir las dos tareas principales asignadas a la misma:

- *Reenvío de paquetes: cuando un paquete llega al enlace de entrada de un en caminador, este tiene que pasar el paquete al enlace de salida apropiado. Una característica importante de los en caminadores es que no difunden tráfico difusivo.*
- *Encaminamiento de paquetes: mediante el uso de algoritmos de encaminamiento tiene que ser capaz de determinar la ruta que deben seguir los paquetes a medida que fluyen de un emisor a un receptor.*

Por tanto, debemos distinguir entre reenvío y encaminamiento. Reenvío consiste en coger un paquete en la entrada y enviarlo por la salida que indica la tabla, mientras que por encaminamiento se entiende el proceso de hacer esa tabla.

2.15.1 Arquitectura Física

FIGURA 11 : Router

Fuente: https://commons.wikimedia.org/wiki/

File:Router.sng

En un enrutador se pueden identificar cuatro componentes:

- ***Puertos de entrada:*** *realiza las funciones de la capa física consistentes en la terminación de un enlace físico de entrada a un en caminador; realiza las funciones de la capa de enlace de datos necesarias para inter operar con las funciones de la capa de enlace de datos en el lado remoto del enlace de entrada; realiza también una función de búsqueda y reenvío de modo que un paquete reenviado dentro del entramado de conmutación del en caminador emerge en el puerto de salida apropiado.*
- ***Entrada de conmutación:*** *conecta los puertos de entrada del enrutador a sus puertos de salida.*
- ***Puertos de salida:*** *almacena los paquetes que le han sido reenviados a través del puerto de conmutación y los transmite al enlace de salida. Realiza entonces la función inversa de la capa física y de la capa de enlace que el puerto de entrada.*
- ***Procesador de encaminamiento:*** *ejecuta los protocolos de ip encaminamiento, mantiene la información de encaminamiento y las tablas de reenvío y realiza funciones de gestión de red dentro del enrutador.*

2.15.2 Tipos de Enrutamiento

Tanto los enrutadores como los anfitriones guardan una tabla de enrutamiento. El daemon de enrutamiento de cada sistema actualiza la tabla con todas las rutas conocidas. El núcleo del sistema lee la tabla de enrutamiento antes de reenviar paquetes a la red local. La tabla de enrutamiento enumera las direcciones IP de las redes que conoce el sistema, incluida la red local predeterminada del sistema. La tabla también enumera la dirección IP de un sistema de portal para cada red conocida. El portal es un sistema que puede recibir paquetes de salida y reenviarlos un salto más allá de la red local.

2.15.2.1 Enrutamiento Estático

Hosts y redes de tamaño reducido que obtienen las rutas de un enrutador predeterminado, y enrutadores predeterminados que sólo necesitan conocer uno o dos enrutadores.

2.15.2.1.1Determinación de Enrutamiento

La información de enrutamiento que él en caminador aprende desde sus fuentes de enrutamiento se coloca en su propia tabla de enrutamiento. El en caminador se vale de esta tabla para determinar los puertos de salida que debe utilizar para retransmitir un paquete hasta su destino. La tabla de enrutamiento es la fuente principal de información del enrutador acerca de las redes. Si la red de destino está conectada directamente, el enrutador ya sabrá el puerto que debe usar para reenviar los paquetes. Si las redes de destino no están conectadas directamente, el en caminador debe aprender y calcular la ruta más óptima a usar para reenviar paquetes a dichas redes. La tabla de enrutamiento se constituye mediante uno de estos dos métodos o ambos:

- *Manualmente, por el administrador de la red.*

- *A través de procesos dinámicos que se ejecutan en la red.*

2.15.2.1.2Rutas Estáticas

Las rutas estáticas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso de enrutamiento según los parámetros del administrador.

Las rutas estáticas por defecto especifican una puerta de enlace de último recurso, a la que el enrutador debe enviar un paquete destinado a una red que no aparece en su tabla de enrutamiento, es decir, se desconoce.

Las rutas estáticas se utilizan habitualmente en enrutamientos desde una red hasta una red de conexión única, ya que no existe más que una ruta de entrada y salida en una red de conexión única, evitando de este modo la sobrecarga de tráfico que genera un protocolo de enrutamiento.

2.15.3 Enrutamiento Dinámico

El enrutamiento dinámico le permite a los en caminadores ajustar, en tiempo real, los caminos utilizados para transmitir paquetes IP. Cada protocolo posee sus propios métodos para definir rutas (camino más corto, utilizar rutas publicadas por pares, etc.).

2.15.4 Encaminadores Inalámbricos

A pesar de que tradicionalmente los en caminadores solían tratar con redes fijas (Ethernet, ADSL, RDSI...), en los últimos tiempos han comenzado a aparecer en caminadores que permiten realizar una interfaz entre redes fijas y móviles (Wi-Fi, GPRS, Edge, UMTS, Fritz!Box, WiMAX...) Un en caminador inalámbrico comparte el mismo principio que un en caminador tradicional. La diferencia es que este permite

la conexión de dispositivos inalámbricos a las redes a las que él en caminador está conectado mediante conexiones por cable. La diferencia existente entre este tipo de en caminadores viene dada por la potencia que alcanzan, las frecuencias y los protocolos en los que trabajan.

2.15.5 Enrutador con Conexiones LAN

Los equipos que actualmente se le suelen vender al cliente como enrutadores no son simplemente eso sino que son los llamados Equipos locales del cliente (CPE). Los CPE están formados por un módem, un enrutador, un conmutador y opcionalmente un punto de acceso WiFi.

2.16 Generalidades de Redes de Comunicación

2.16.1Ondas de Radio

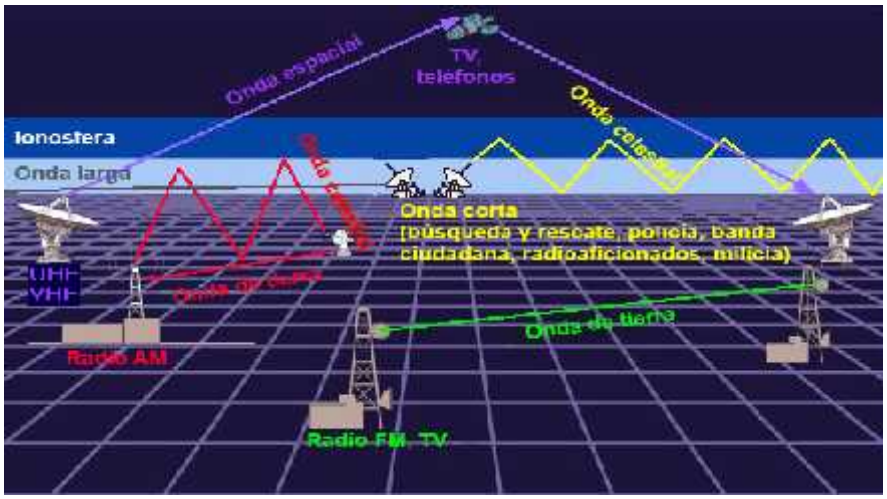

FIGURA 12 : Ondas de Radio

Fuente:https://www.windows2universe.org/physical_science/magnetism/em_radio_waves.html&lang=sp

Las ondas de radio son un tipo de radiación electromagnética. Una onda de radio tiene una longitud de onda mayor que la luz visible. Las ondas de radio se usan extensamente en las comunicaciones.

Las ondas de radio tienen longitudes que van de tan sólo unos cuantos milímetros (décimas de pulgadas), y pueden llegar a ser tan extensas que alcanzan cientos de kilómetros (cientos de millas). En comparación, la luz visible tiene longitudes de onda en el rango de 400 a 700 nanómetros, aproximadamente 5 000 menos que la longitud de onda de las ondas de radio. Las ondas de radio oscilan en frecuencias entre unos cuantos kilo Hertz (kHz o miles de Hertz) y unos cuantos Tera Hertz. La radiación "infrarroja lejana", sigue las ondas de radio en el espectro electromagnético, los lejanos tienen un poco más de energía y menor longitud de onda que las de radio.

Las microondas, que usamos para cocinar y en las comunicaciones, son longitudes de onda de radio cortas, desde unos cuantos milímetros a cientos de milímetros (décimas a decenas de pulgadas).

Varias frecuencias de ondas de radio se usan para la televisión y emisiones de radio FM y AM, comunicaciones militares, teléfonos celulares, radioaficionados, redes inalámbricas de computadoras, y otras numerosas aplicaciones de comunicaciones.

La mayoría de las ondas de radio pasan libremente a través de la atmósfera de la Tierra. Sin embargo, algunas frecuencias pueden ser reflejadas o absorbidas por las partículas cargadas de la ionosfera.

2.16.2 Espectro Electromagnético

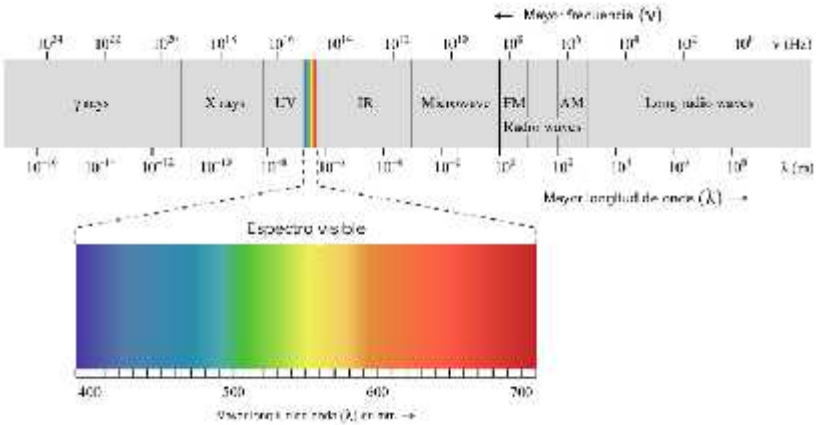

FIGURA 13 : Espectro Electromagnetico

Fuente:https://es.khanacademy.org/science/ap-chemistry/electronic-structure-of-atoms-ap/bohr-model-hydrogen-ap/a/light-and-the-electromagnetic-spectrum

Podemos clasificar y ordenar las ondas electromagnéticas de acuerdo a sus diferentes, longitudes de onda y frecuencias; llamamos a esta clasificación "el espectro electromagnético". La tabla siguiente muestra este espectro, que consiste de todos las clases de radiación electromagnética que existen en nuestro universo.

El espectro electromagnético se compone de todas las clases de radiación en el universo. Los rayos gamma tienen la frecuencia más alta, mientras que las ondas de radio tienen la frecuencia más baja. La luz visible está aproximadamente a la mitad del espectro, y comprende una fracción muy pequeña de este.

Como podemos ver, el espectro visible es decir, la luz que podemos ver con nuestros ojos es tan solo una pequeña fracción de las diferentes clases de radiación que existen. A la derecha del espectro visible, encontramos las clases de energía que son menores en frecuencia (y por lo tanto mayores en longitud de onda) que la luz visible. Estas clases

de energía incluyen los rayos infrarrojos (IR) (ondas de calor emitidas por los cuerpos térmicos), las microondas y las ondas de radio.

Estos tipos de radiación nos rodean constantemente; no son dañinos, pues sus frecuencias son muy bajas. Como veremos en la sección siguiente, "El fotón", las ondas de baja frecuencia tienen poca energía, y por lo tanto no son peligrosas para nuestra salud.

2.17Tipos de Cámaras

Basadas en estándares abiertos, las cámaras han evolucionado para adaptarse a distintas necesidades y ámbitos de uso. Según su diseño y propósito.

2.17.1 Cámaras Fijas

Corresponde a un diseño clásico de cámara de vigilancia. Su orientación es fija y carece de partes móviles, por lo que es la opción más económica. Las cámaras de seguridad de este tipo suelen venir protegidas en un confinamiento rígido resistente, lo que la hace menos vulnerables al vandalismo y a las inclemencias del tiempo.

Es la opción más habitual en exteriores. Su visibilidad persigue un efecto disuasorio, existe un gran cantidad de modelos en muchos tamaños, con lentes vari focales e intercambiables para mayor flexibilidad.

FIGURA 14: Cámaras Fijas

Fuente:https://www.ventasdeseguridad.com/2021031612588/productos/cctv/camaras-fijas-ip.html

2.17.2 Cámaras de Cúpula Fijas

Son cámaras fijas cuyo objetivo está protegido por una cúpula transparente, pero que oculta su interior, el diseño con cúpula busca discreción, a la vez que oculta la verdadera orientación del objetivo y protege a este contra la redirección y el desenfoque.

FIGURA 15: Cámara Ip fija con cúpula

Fuente:https://www.archiexpo.es/prod/axis-communications/product-1782-1385015.html

2.17.3 Cámaras IP PTZ

Una cámara PTZ ofrece las mismas características que cualquier cámara de video con capacidad de orientación zoom la cámara dispone de dos servos, uno para controlar el movimiento horizontal (pan) y otro para el cabeceo (tilt).

Tanto las funciones de orientación como de zoom de cámara pueden programarse en una secuencia automática, o ser controlados remotamente por un controlador humano o de inteligencia artificial.

Son las cámaras preferibles para cubrir un amplio panorama visual o garantizar la identificación no obstante, la cámara puede dejar puntos ciegos momentáneos que pueden ser aprovechados para la infiltración.

2.17.3.1 Características

- *Protocolo de video de alta velocidad.*
- *Lente de alta sensibilidad 1/4 "Sensor CMOS.*
- *Utiliza compresión MJPEG y formato de video VGA / QVGA para que pueda elegir.*
- *Audio bidireccional y micrófono de alta sensibilidad.*
- *Multinivel de gestión de usuarios y la definición de las contraseñas.*
- *Permite configuración inalámbrica (WiFi /802.11/b/g).*
- *Detección de movimiento que permite configurar envío de imagen vía e-mail.*
- *Función PT, rotación de 270° e inclinación de 90°.*
- *Compatible con UPnP.*
- *Visualización compatible con iPhone/ iPad / 3G Phone / Smartphone.*
- *Alcance de visualización nocturna: 15 metros.*

- *Voltaje de alimentación: Adaptador de 110 VAC a 5 VDC / 2.5ª.*
- *Consumo de potencia: 5 watts.*
- *Temperatura de operación: -10º – 60º C.*
- *Humedad: 0% - 90 % RH.*

2.17.3.2Requerimientos mínimos de Visualización

a) *CPU 2.0 GHz.*
b) *Memoria RAM: 512 MB.*
c) *Tarjeta de video: 64 MB.*
d) *Systems operative: Microsoft Windows XP Windows7.*

2.17.4 Cámaras IP PTZ con Cúpula

Las cámaras PTZ se pueden encapsular, al igual que las fijas, en una cúpula de ocultación, este tipo de cámara posee todas las ventajas y funcionalidades. La mayoría de modelos permiten un campo visual completo y continuo, con 360º horizontales y 160º de cabeceo.

FIGURA 16: Cámara PTZ con Cupula

Fuente:https://www.amazon.com/-/es/vigilancia-seguridad-impermeable-detecci%C3%B3n-movimiento/dp/B07R6MV62P

2.17.5 Cámaras IP Térmicas

Las cámaras térmicas, a diferencia de las convencionales, registran las frecuencias de luz infrarrojas, fuera del espectro de la luz visible por el ojo humano. Por tanto, una cámara IP termal, crea imágenes basadas en el calor que irradia cualquier objeto, vehículo, animal o persona.

La principal ventaja de estas cámaras radica en la posibilidad de detectar casi cualquier objeto en condiciones de oscuridad total o atmósfera turbia. Desafortunadamente, la capacidad de identificación de perfiles de objetos o personas con este tipo de cámaras no ha sido ampliamente desarrollada.

FIGURA 17: Cámara IP Termica

Fuente: https://www.axis.com/es-es/products/axis-q87-series

2.17.6 Visión Térmica

El infrarrojo lejano, o termal, generalmente no se considera visión nocturna porque se construye con los mecanismos substancialmente diferentes de los métodos usados para detectar la luz visible.

Es posible construir un dispositivo de la proyección de imagen con energía de microondas, sonido, o cualquier otra señal que sea reflejada o irradiada por los objetos y pueda ser enfocada y ser detectada, pero éstos también generalmente no se consideran

visión nocturna.

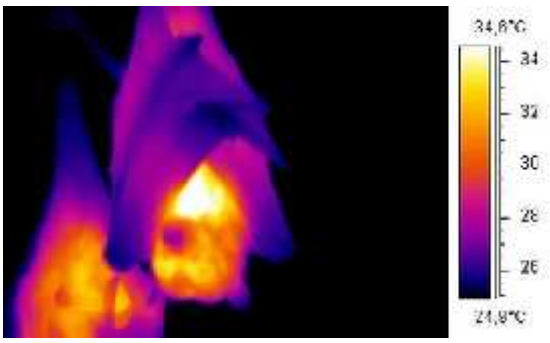

FIGURA 18 : Vision Termica

Fuente: https://es.wikipedia.org/wiki/Visi%C3%B3n_nocturna

2.17.7 Cámaras de Visión Nocturna

Las cámaras de visión nocturna se basan en amplificar la intensidad o captar longitudes de onda no visibles por el ojo humano pero sí por otros sensores.

2.18Estándares de la Industria

Previamente se han mencionado y descrito algunos de los estándares que utiliza la vigilancia IP a diferentes niveles y en distintas funciones. No obstante, la definición de un único canon para todo el conjunto es la cuestión que más está demorando, aunque esté resultando crítica para el conjunto del sector.

2.18.1 Diferencias Históricas entre Estándares

Como se puede deducir, OVIF representa a los principales fabricantes del sector, mientras que PSIA aglutina a las empresas con menor cuota de mercado. Los intereses de cada alianza son opuestos y pugnan por imponer fácticamente sus intereses.

***ONVIF**: Representa a las siete compañías incluyendo Axis y Sony que comparten la mitad del mercado de cámaras IP. Su objetivo ha sido retrasar al máximo la adopción de estándares, dado que su situación de poder en el mercado se mantiene gracias a las barreras tecnológicas.*

***PSIA**: Representa a las compañías con menor cuotadel mercado, lideradas por Honeywell, Panasonic, Pelco, GESecurity, DvTel, IQinVision, Verint. En conjunto, no son más que una fracción del volumen de Sony y Axis. Algunas de estas compañías están especialmente interesadas en la estandarización para poder acceder en el mercado de equipamiento y servicios asociados, no de cámaras.*

2.19 VENTAJAS

2.19.1VigilanciaIP

La vigilancia digital permite la integrar una gran cantidad de subsistemas y servicios asociados a la Vigilancia de video, constituyendo una red, de seguridad o servicios, interactiva, mucho más completa y menos costosa que la que se podría implementar utilizando sistemas de video analógicos. Entre los servicios y posibilidades que se pueden desarrollar sobre redes IP cabe destacar:

- ***No necesita cables***

La ausencia de cableado facilita la instalación de las cámaras y abarata el coste, pudiendo invertir en mejora de la tecnología de las cámaras.

- ***Acceso desde cualquier lugar***

Se puede acceder a las imágenes o grabaciones desde cualquier parte, independientemente de que se esté en el edificio o fuera de él.

- ***Sistema totalmente configurable***

El sistema de grabación es totalmente escalable y modificable según las necesidades. Con solo cambiar el soporte de la cámara IP obtendremos una nueva zona de visionado.

- ***Opciones tecnológicas avanzadas***

Las cámaras IP más modernas pueden contar con avances tecnológicos que incrementan la seguridad y pueden disminuir los costes con sistemas como la grabación de personas no identificadas o la activación por movimiento.

- ***Integración con sistemas externos***

Como alarmas, personal de vigilancia remota, o usos periciales de las imágenes grabadas.

- ***Numero de cámaras casi ilimitado***

Según el ancho de banda que tengamos se podrán instalar tantas cámaras como nos admita el sistema

- ***Manejo remoto de las cámaras***

Las cámaras se pueden mover (cámaras motorizadas) hacer zoom o iniciar o parar la grabación de forma remota.

- ***Facilidad de manejo***

Las cámaras Ip cuentan con aplicaciones de fácil uso que las convierten en una solución ideal para vigilar nuestras casas, negocios o zonas comunes de nuestras viviendas.

Actualmente se están usando en viviendas particulares para el control de niños pequeños y empleados del hogar. Hay que tener muy en cuenta las leyes vigentes si las cámaras se van a utilizar para grabar imágenes en las que aparezcan otras personas ajenas al hogar.

- ***Vigilancia económica y escalable***

Una red de cámaras IP se puede montar por un precio bastante económico, según las prestaciones que necesitemos.

El sistema se puede ir ampliando poco a poco con facilidad por lo que no hace falta hacer una gran inversión inicial para acabar teniendo un sistema completo de vigilancia. Podemos ir ampliando el sistema con cámaras y sistemas de grabación y control según nuestras necesidades y capacidad económica.

2.20Desventajas de la Vigilancia IP

- *Su efectividad depende del servicio de Internet.*
- *Son vulnerables a sabotajes, bastaría con un inhibidor de frecuencias para inhabilitar la señal, si se pierde la señal de Internet quedan inutilizadas.*
- *Al estar conectadas a Internet, pueden ser hackeadas, como cualquier dispositivo conectado.*

2.21 DVR H.264

Es un aparato de gestión de vídeo para controlar la grabación y el archivo de vídeos que provienen de cámaras de video vigilancia *en uno o más discos duros. Existen varias topologías de DVR en el mercado que son diferentes entre ellas no sólo por las características ligadas al número de ingresos de vídeo o a los beneficios, sino también por la capacidad de transmitir las imágenes a través de una red LAN o Internet.*

A cualquiera de las categorías a las que pertenezcan, todos los dispositivos DVR para la gestión de vídeo centralizada basan su actividad en dos funciones primordiales.

a) *La digitalización del vídeo.*
b) *La compresión del vídeo.*

FIGURA 19 : DVR H264

Fuente: https://es.made-in-china.com/co_veleysecurity/product_H264-Realtime-DVR-Ahd-Video-Recorder-CCTV-HDMI-DVR-Recorder_rihhhunsg.html

El tipo de algoritmo de compresión que se utiliza es el parámetro fundamental para la elección de un DVR, porque es determinante para que el resultado esté en línea con las expectativas. Los códec de vídeo son aparatos que implementan los modelos matemáticos utilizados para codificar y descodificar las imágenes y son indispensables para la compresión de los flujos de vídeo que por su propia naturaleza, contienen una gran cantidad de información que debe trasmitirse mucho más con respecto al audio.

En consecuencia, para el archivo de estos datos en un disco duro o su trasmisión a través de un Network, se necesita una notable compresión de datos. Para comprimir un vídeo, un dispositivo necesita mucha memoria y un procesador potente. Se han realizado muchas investigaciones, orientadas a optimizar la compresión de vídeo para limitar al máximo la pérdida de calidad.

Existen muchos códec en el mercado, pero los más usados son el MJPEG, el MPEG-4 y el H.264 la grabación digital se realiza a través del disco duro que dependiendo de los modelos, puede ser extraíble o no.

El número de los HD que se pueden introducir en un DVR pueden ser de 1 a 8, garantizando así muchas horas y días de grabación los aparatos con más prestaciones por canal de vídeo con un alto factor de calidad.

La visualización en directo, es decir, en tiempo real, de los flujos de vídeo se expresa en metros cuadrados por segundo (fps). Se considera tiempo real una visualización a 25 fps, la función de grabación (play back) es necesaria para la reproducción de acontecimientos diferentes.

La búsqueda normalmente se realizara a través de menús que permiten retomar los acontecimientos por fecha y hora o por topología de alarma (movimiento, sensor, etc.) La copia en soportes externos desde el disco duro del DVR (respaldo) de eventos grabados, es necesaria cuando las informaciones inherentes de un acontecimiento concreto tienen que ser duplicadas.

Los equipos denominados NVR (Network Video Recorder) se utilizan en aplicaciones de video vigilancia. Se trata de equipos de una gran capacidad de elaboración y memoria, conectados generalmente a una red LAN con cámaras analógicas, con la posibilidad de conectar también monitores (características a menudo presentes en los DVR).

En síntesis, su función es la de servidor de imágenes de vídeo, que puede memorizar una gran cantidad de flujos de vídeo procedentes de la LAN y de ponerlos a disposición (a tiempo real o en diferido) de otras unidades conectadas a la misma LAN o a internet.

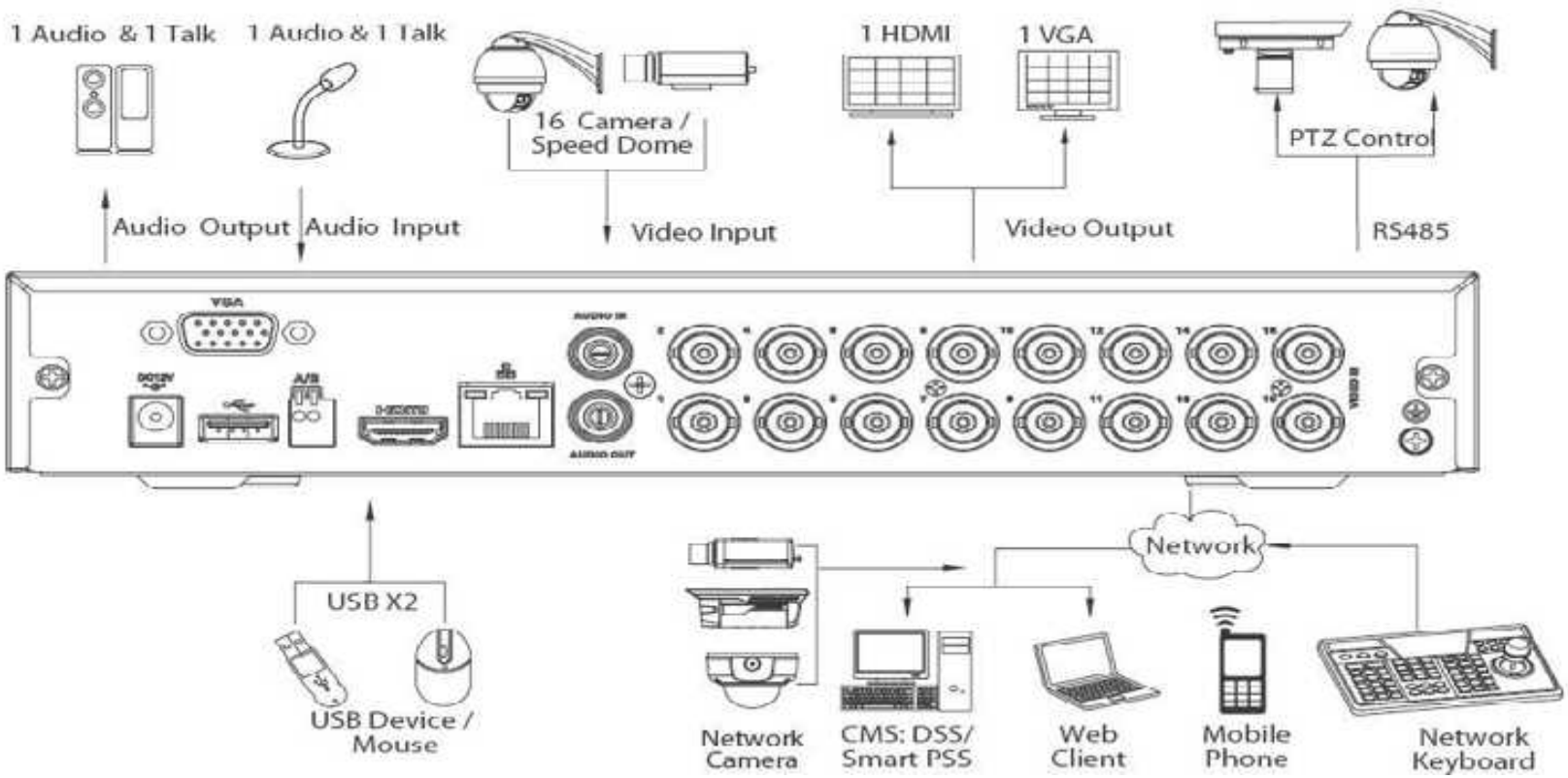

FIGURA 20: Equipo Completo

Fuente:https://www.tecnoseguro.com/faqs/cctv/dvr-que-es-tipos-caracteristicas

El monitor es un dispositivo de salida para el ordenador que muestra en su pantalla los resultados de las operaciones realizadas en él. Al monitor se lo conoce comúnmente como pantalla de la computadora y es un periférico que se conecta a la computadora para poder visualizar las acciones y procesos que se ejecutan.

Un monitor dispone de varios puntos que deben ser considerados para su distinción en términos de usabilidad y calidad.

2.21.1 Características de un DVR

- *Compresión H.264.*
- *Función de detección de movimiento.*
- *Función de máscara para áreas de privacidad.*
- *Función de alarma por bloqueo en las cámaras.*
- *Función de alarma por pérdida en señal del video.*
- *Funciones de Visualización y Reproducción.*
- *Soporta avance rápido, lento, cuadro a cuadro, etc.*
- *Muestra el estado local de la grabación.*
- *Soporta Mouse USB para operar la DVR (incluido).*
- *Control Remoto Inalámbrico Incluido.*
- *Soporta múltiples tipos de grabación, incluyendo tiempo real, grabación manual, alarma externa, video sensor y alarma.*
- *Soporta grabación cíclica (sobre escritura) y no cíclica.*
- *Soporta memorias USB, Discos Duros USB y USB-CDRW (para extraer Grabación.).*
- *No incluye disco duro.*
- *Aprobaciones: FCC, UL, CE, CB, CCC, SGS.*

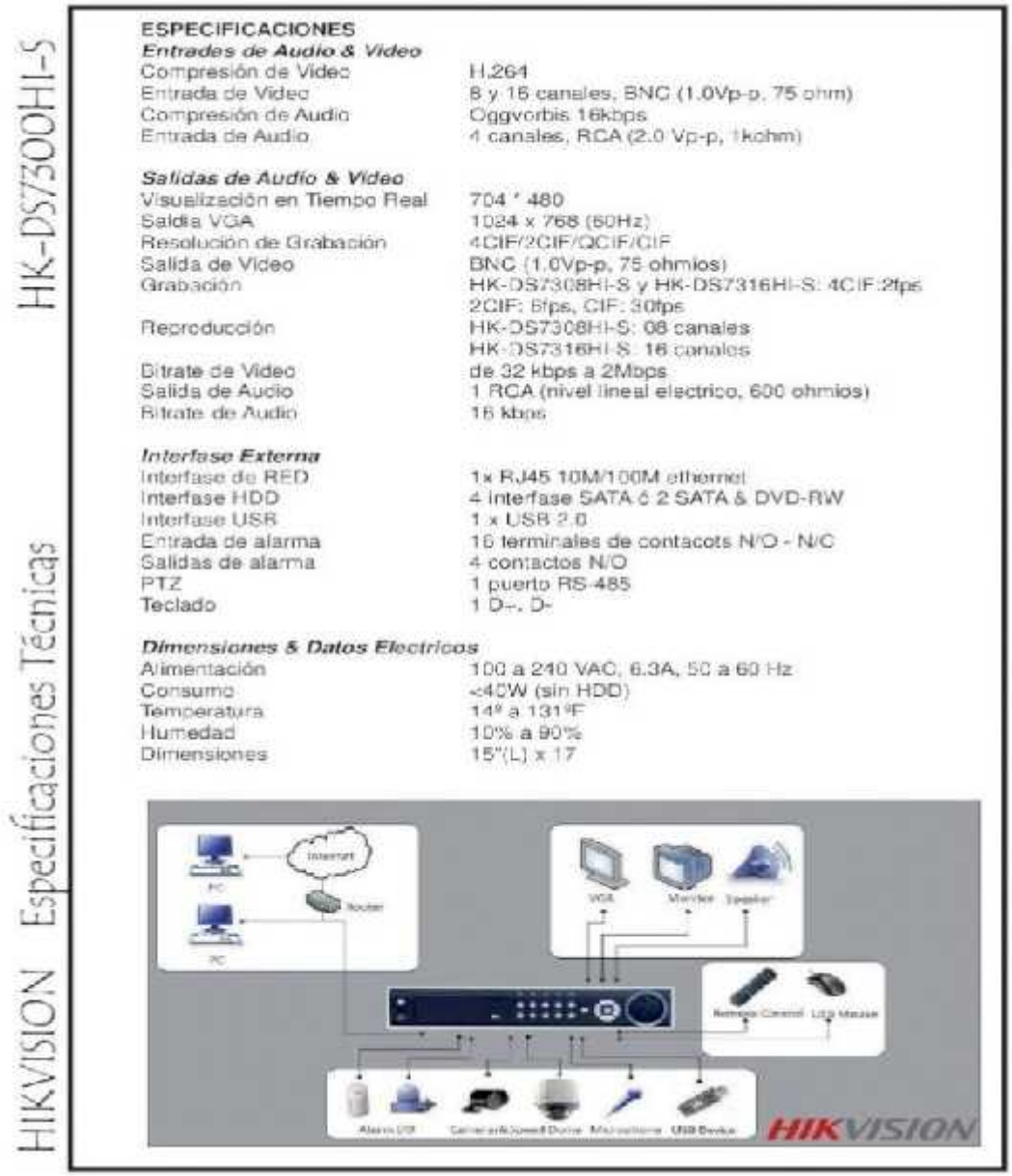

FIGURA 21: Especificaciones

Fuente: https://pdfslide.net/documents/dvr-h264-de-8-240-fps-y-16-480-fps-canalesvr-hikvision-transmisor-digital.html

2.21.2 Preparación del Sistema

En primer lugar se debe instalar 2 programas que nos permitirán trabajar de forma correcta:

a) *Drivers ActiveX para Internet Explorer*
b) *Software de Visualización y Configuración de HIKVISION*

2.21.3 Configuración del Router

Para este paso, el usuario deberá tener un conocimiento básico sobre redes, así que la explicación será muy rápida.

La primera es dar una dirección IP dentro de la LAN para el DVR, de forma que el grabador obtenga siempre la misma dirección a pesar del Reset del Router. Como el DVR por default tiene configurado a través de un DHCP, no es necesario configurarlo.

FIGURA 22: DHCP

Fuente:https://edualejo77.files.wordpress.com/2014/01/reserva-dhcp.png

La segunda opción es configurar el DVR para asignar una dirección IP Fija ya sea físicamente en el DVR o a través de la dirección por default en Internet Explorer (192.0.0.4). Se coloca el usuario: admin y contraseña: 12345.

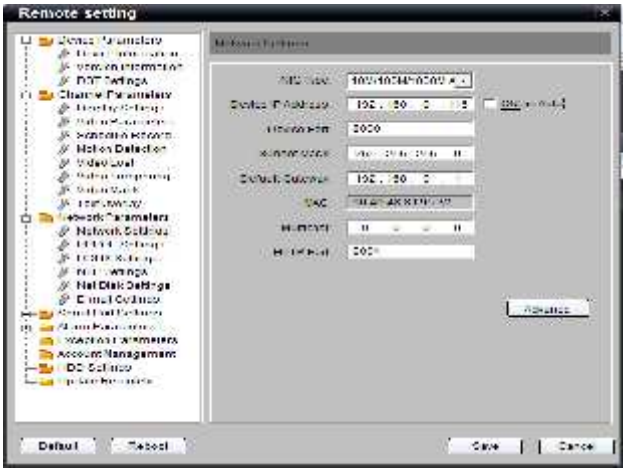

FIGURA 23: Configuración DVR

Fuente:https://edualejo77.files.wordpress.com/2014/01/2.png

En este punto podemos recalcar dos puertos importantes:

2.21.4. PUERTOS

2.21.4.1 Puerto del Dispositivo

Es el puerto por el cual el usuario puede acceder al DVR, a sus configuraciones, a revisar sus características de forma remota. Para este ejemplo tomaremos el puerto 8000.

2.21.4.2 Puerto HTTP

Es el puerto que el DVR utilizará para que sea visualizado a través de cualquier

navegador desde una red local o desde internet. En este caso tomaremos el puerto 8001.

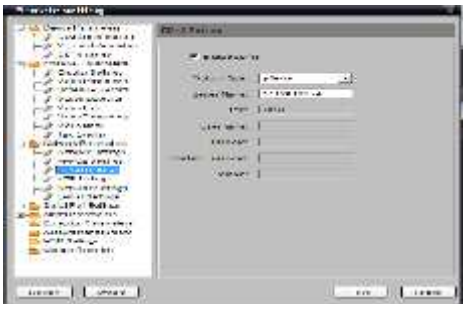

FIGURA 24: Servidor HikVision

Fuente:https://edualejo77.files.wordpress.com/2014/01/3.png

2.21.4.3 Direccionamiento de los Puertos

Es necesario re direccionar los dos puertos (Puerto del Dispositivo y Puerto HTTP) para visualizar de forma remota nuestro DVR a través de internet.

FIGURA 25: Direccionamiento de Puertos

Fuente:https://edualejo77.files.wordpress.com/2014/01/4.png

Un interruptor es un dispositivo en una red de computadoras que eléctricamente y lógicamente conecta juntos otros dispositivos. Los cables múltiples de datos son taponados en un interruptor para permitir comunicación entre dispositivos enlazados en red diferentes.

Los interruptores manejan el flujo de datos a través de una red transmitiendo un paquete admitido por la mayoría de la red sólo para el mismo o más dispositivos para los cuales el paquete es pretendido.

Cada dispositivo enlazado en red conectado para un interruptor puede ser identificado por su dirección de la red, dejando el interruptor regular el flujo de tráfico. Esto maximiza la seguridad y la eficiencia de la red.

Cuando un centro del repetidor es reemplazado con un Ethernet interruptor, la sola colisión abrumadora que el dominio usó por el centro es dividido en más pequeños adelgazando o eliminando la posibilidad y el alcance de colisiones y como consecuencia, aumentando el rendimiento específico potencial.

Un interruptor está más automatizado que un centro del repetidor, lo cual simplemente retransmite paquetes de bits fuera de cada puerto del centro exceptuando el puerto en el cual el paquete fue recibido, incapaz para distinguir depósitos diferentes y logrando una en conjunto eficiencia más bajo de la red.

2.22ProtocoloTCP/IP

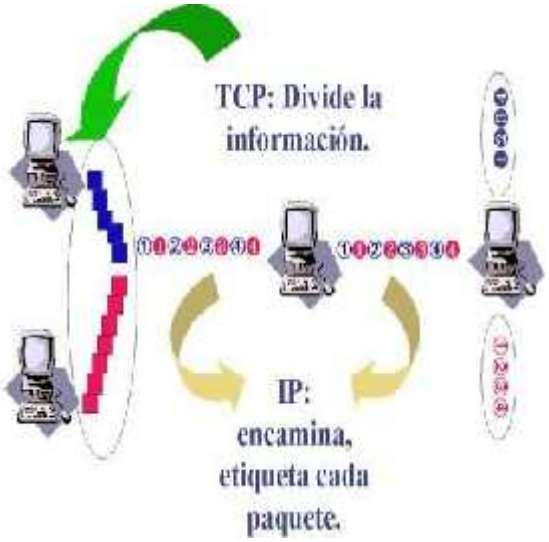

FIGURA 26: Protocolo TCP/IP

Fuente:http://tecnologiaedu.us.es/cursos/29/html/cursos/tema7

El protocolo TCP/IP, es un conjunto de reglas o normas que determinan cómo se realiza el intercambio de datos entre dos ordenadores.

El protocolo TCP se encarga de dividir las informaciones en paquetes de tamaño adecuado, numerar estos paquetes para que puedan volver a unirse en el lugar correcto y añadir cierta información para la transmisión y posterior decodificación del paquete y detectar posibles errores en la transmisión. Por su parte el protocolo IP atiende todas las operaciones relacionadas con el encaminamiento de los paquetes del origen al destino, encargándose de etiquetar cada paquete de información con la dirección apropiada.

Este sistema de comunicación, hace necesario que cada ordenador conectado a Internet tenga una dirección de Internet (IPaddress) única y exclusiva que lo distingue de cualquier otro ordenador en el mundo. Esta dirección o número IP se representa con cuatro números separados por puntos, cada uno de los cuales puede tomar valores entre 0 y 255.

2.22.1 Medios de Transmisión Guiados

Los medios de transmisión guiados están constituidos por cables que se encargan de la conducción (o guiado) de las señales desde un extremo al otro. Las principales características de los medios guiados son el tipo de conductor utilizado, la velocidad máxima de transmisión, las distancias máximas que puede ofrecer entre repetidores, la inmunidad frente a interferencias electromagnéticas, la facilidad de instalación y la capacidad de soportar diferentes tecnologías de nivel de enlace. La velocidad de transmisión depende directamente de la distancia entre los terminales, y desde el medio se utiliza para realizar un enlace punto a punto o un enlace multipunto. Debido a esto, los diferentes medios de transmisión tendrán diferentes velocidades de conexión que se adaptarán a utilizaciones dispares.

Dentro de los medios de transmisión guiados, los más utilizados en el campo de las telecomunicaciones y el ínter conexión de computadoras son tres:

- *Cable de par trenzado*
- *Cable coaxial*
- *Fibra óptica*

Tabla 2 : Medios de Transmission

MEDIODE TRANSMISIÓN	***RAZÓNDEDATOSTOTAL***	***ANCHODEBANDA***	***KM)***
Cable de par trenzado	*4 Mbps*	*3 MHz*	*2 a10*
Cable coaxial	*10Mbps*	*350 MHz*	*1 a10*
Cable de fibra óptica	*2Gbps*	*2 GHz*	*10a100*

2.23 Normas

Estos son algunos de los organismos que rigen las normas que supervisan el desarrollo de procesos y sistemas tecnológicos y de comunicaciones y garantizan los estándares de calidad.

- *TIA: Telecommunications Industry Association.*
- *ANSI: American National Standards Institute.*
- *EIA: Electronic Industries Alliance.*
- *ISO: International Standards Organization.*
- *IEEE: Instituto de Ingenieros Eléctricos y de Electrónica.*

2.23.1 Protección de Datos Personales en Sistemas de Video Vigilancia

Esta guía está dirigida a las personas, compañías u organizaciones que utilizan SV recolectando datos personales, ya sea en calidad de Responsables o Encargados del tratamiento de datos personales, por medio de cámaras, videocámaras, análogas o digitales, cámaras IP o mini-cámaras, circuitos cerrados de televisión (CCTV) y en general, cualquier medio por el cual se realice el tratamiento de imágenes de titulares de datos personales, en especial con necesidad de vigilancia, para orientarlos en el cumplimiento de sus deberes, en materia de protección de datos personales, y a los titulares de la información, para que tengan conocimiento de cómo ejercer sus derechos frente a los primeros, garantizando así el respeto por sus derechos fundamentales a la intimidad, al buen nombre y a la protección de datos personales, consagrados en la Constitución Política a partir del cual se desarrolla el derecho de las personas en Bolivia. Las grabaciones que se realicen dentro del ámbito exclusivamente personal o doméstico, con necesidad periodísticos, o que tengan como calidad la seguridad nacional del Estado.

CAPITULO III

3. DESARROLLO DEL PROYECTO

Se hizo una observación en el lugar para dar a conocer la importancia de este proyecto dando a conocer lo que implica su desarrollo. En el cual se requiere implementar unas 4 cámaras para las zonas principales y tener en cuenta un sistema Dvr para estas 4, si se requiere para un futuro colocar más cámaras por motivos de seguridad colocar un sistema Dvr que cumpla con el número que se va requerir para no tener más gastos.

También se provee que desde cualquier smartfone se pueda ver que es lo que está pasando, sin ir al sitio donde se hizo la instalación, facilitando el manejo de este tipo de tecnología.

3.0 Fase de Diseño Lógico

Se utilizará una red privada para el reconocimiento de cada cámara común direccionamiento DHCP que permita obtener su IP automáticamente con la máscara de red por defecto "255.255.255.0".

Datos:

Dirección de red ->200.144.0.10

Primer host utilizable ->200.144.0.1Ultimo
Host utilizable -> 200.144.1.25

Broadcats ->200.144.1.254

Mascara de red ->255.255.255.0

3.0.1 Fase de Diseño Físico

Primero se sitúa dónde quiere que vayan las cámaras para su instalación ya sea en la pared, el techo o ya sea en los postes, se hacen los canales por donde se cableara la red, se sitúa en un cuarto el PC donde no estará alejado del sol y la humedad.

3.0.2 Simulación

Teniendo en cuenta los requerimientos, se procedió con su respectiva simulación en el cual se ha usado Cisco Packet Tracer que es uno de los mejores programas al tratarse de montajes en la red.

Se configuraron dos VLAN, una para las cámaras del primer nivel y segundo nivel, y otra para las cámaras del patio, comedor.

Se configuraron los Reuter y se realizó pruebas.

Se montaron las cámaras donde se conectaron a través del puerto Ethernet al Reuter donde hubo conectividad entre los dispositivos dando así un buen funcionamiento del mismo.

3.1 Funciones del Grabador

Las principales funciones del grabador son: grabación y almacenamiento de las imágenes captadas por las cámaras; control de la motorización y/o zoom de las cámaras; salida para obtener copias seleccionadas de las grabaciones almacenadas (USB, etc.), o grabador de CD; conexión a internet para la visualización, control remoto de todas las funciones y programación de parámetros.
La forma en que se graban las imágenes en configurable por el usuario, e independiente de cada cámara:

a) *Grabación continúa. El grabador está grabando durante todo el tiempo.*
b) *Grabación programada. Sólo se graba en ciertos periodos (hora/día/semana) programados.*
c) *Grabación por eventos. El grabador únicamente graba en los momentos de detección de movimiento o de disparo de alarma.*

3.2 Cálculo de la Capacidad de Almacenamiento del Grabador

Para el cálculo de la capacidad de almacenamiento del disco duro debemos tener en cuenta los siguientes factores:

a) *Número de canales (cámaras) de la instalación*
b) *Resolución de las cámaras (pixeles)*
c) *Número de Frames por segundo (fps)*
d) *Método de compresión - factor de compresión*
e) *Tiempo total de grabación (días)*

3.3 Gestión y Control del Video

En toda instalación de video vigilancia IP es necesario un software específico que realice las funciones de gestión, monitorización, gestión de eventos y configuración de dispositivos. Este software normalmente va incorporado en la compra de un NVR y se instala en cualquier PC o Smartphone de los usuarios autorizados.

Cuando no es así, el software va:

a) Embebido en los mismos elementos de la red (cámaras), para acceder a él basta con teclear la dirección IP del dispositivo en un navegador y se accede al menú que administra toda la configuración de los elementos este sistema sólo es viable si hay pocas cámaras.

b) instalado en el PC que va a controlar, gestionar y grabar las imágenes.

Un sistema de gestión de video puede incluir muchas funcionalidades diferentes, que pueden ser:

- *Grabación de video.*
- *Reproducción de video en directo, admite la posibilidad de ver la imagen de varias cámaras al mismo tiempo.*
- *Reproducción y grabación del audio.*
- *Gestión de eventos, como detección de movimiento y alarmas.*
- *Configuración de las cámaras, tanto de los parámetros básicos como resolución, compresión, frecuencia de imagen… cómo parámetros PTZ.*
- *Funciones de búsqueda y reproducción de videos grabados.*
- *Control de acceso de usuarios.*
- *Aplicaciones de video inteligente como la realización de rondas virtuales.*
- *Mapeo de las cámaras, se crea un mapa gráfico de la instalación vigilada, donde podamos visualizar iconos que representan los diferentes elementos del sistema.*

- *Envío de alertas por email, en el momento de detección de movimiento o activación de alarmas.*

- *Visualización en Smartphone, PDA, o similar.*

3.4Ancho de Banda

Para hacer el cálculo del ancho de banda ocupado por todas las cámaras es necesario conocer los siguientes datos:

a) *Número de canales (cámaras) de la instalación.*
b) *Resolución de cada una de las cámaras (pixeles).*
c) *Número de frames por segundo (fps).*

Para las cámaras ip hay que tener una consideración, especial ya que es necesario saber el ancho de banda con que cuenta el sitio donde se realizara la instalación.

El ancho de banda es el rango de frecuencia que un canal de comunicación permite transmitir, la cantidad de ancho de banda que requiere un sistema de video vigilancia, depende del número de cámaras, fotogramas por segundo, resolución de imagen, tipo de compresión de video y la complejidad de la imagen.

3.5 Cámara Hik Visión

3.5.1 Contenido del Equipo

El equipo se entrega con todo lo necesario para su funcionamiento:

- *1 Cámara inalámbrica de visión nocturna 15m.*
- *1 Soporte metálico para cámara.*
- *1 Antena de 2,4Ghz.*
- *1 Alimentador estabilizado de 12V / 500mAh.*
- *2Años de garantía.*

3.5.2 Características de la Cámara

Esta cámara se caracteriza por visión nocturna y sensor PIR incorporado es un accesorio para ampliación del sistema de grabación en tarjeta SD, el único equipo que cuenta con esa gama que puede enviar de forma inalámbrica la imagen de hasta 4 cámaras al mismo tiempo, sin interferencias de ningún tipo.

Esto es posible gracias a la nueva tecnología inalámbrica digital que incorpora varios niveles de cifrado, haciendo que el envío de la señal de vídeo sea completamente privado, seguro, fiable y estable.

En definitiva, es un sistema de vigilancia inalámbrico digital económica, cómoda, práctica e ideal para mantener supervisados a niños, mayores, trabajadores, y principalmente para atracos de delincuentes.

FIGURA 27: Características de la Cámara

Fuente:https://www.google.com/search?q=caracteristicas+de+la+camara+ip&tbm=isch&ved=2ahUKEwiqp7L42p70AhU9s5UCHQ2dA4AQ2-cCegQIABAA&oq=caracteristicas+de+la+camara+ip&gs_lcp=CgNpbWcQAzIGCAAQCBAeMgQIABAYMgQIABAYOgQIABBDOgUIABCABDoGCAAQBxAeOgQIABAeOgYIABAFEB5QgA1Y9hhgwR1oAHAAeACAAa8BiAHcBJIBAzAuNJgBAKABAaoBC2d3cy13aXotaW1nwAEB&sclient=img&ei=OZmUYeqmOr3m1sQPjbqOgAg&bih=781&biw=1707#imgrc=n7L2cTINJjN8_M&imgdii=126iHqcs-sIpnM

Este tipo de cámara posee varias funciones de una cámara analógica estándar de circuito cerrado, pero proporciona muchas más funcionalidades. De hecho, una cámara de red es una cámara analógica capaz de digitalizar imágenes y transmitirlas por una red.

3.5.3 Sensor de Imagen

El sensor de imagen es el elemento de una cámara digital que capta la luz que compone la cámara. Se trata de un chip formado por millones de componentes sensibles a la luz que al ser expuestos capturan la imagen .El sensor de la imagen es como la película

fotográfica que utiliza la cámara analógica el sensor de imagen está compuesto por millones de pequeños semiconductores de silicio, los cuales captan los fotones (elementos que componen la luz, la electricidad). A mayor intensidad de luz, más carga eléctrica existirá.

Estos fotones desprenden electrones dentro del sensor de imagen, los cuales se transformarán en una serie de valores datos digitales creando un píxel.

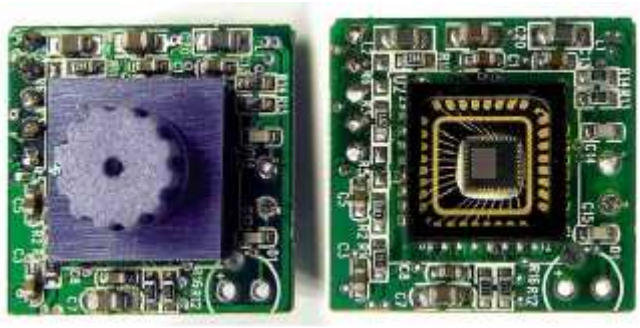

FIGURA 28: Sensor de Imagen

Fuente: https://es.wikipedia.org/wiki/Sensor_de_imagen

3.5.4 Sensor Fotoeléctrico y Procesamiento de Imagen

El sensor de imagen convierte la imagen en una matriz de bits, mediante un proceso fotoeléctrico puede ser de dos tipos: CCD o CMOS. Los sensores CCD se emplean desde hace décadas y siguen siendo más eficaces en entornos de baja luminosidad, ya que son más sensibles. En cambio, los chips CMOS tienen toda su lógica integrada y su bajo coste y volumen los hace más apropiados para aplicaciones generales y de pequeño tamaño.

Un micro controlador en la cámara comprueba la exposición, el equilibrio de blancos,

la nitidez de la imagen y todos los aspectos de la imagen. Estas funciones las llevan a cabo el controlador de cámara y el chip de compresión de vídeo.

3.5.5FrameRate

*Es el número de imágenes captadas por segundo existe una relación clara entre la forma de comunicar la cámara con el ordenador y el número de fps así, existen cámaras que se comunican vía puerto paralelo y solamente capturan 3 fps. Las cámaras que usan la conexión USB alcanzan entre 8 y 14 fps. Para monitores panorámicos de 19" o 22" resoluciones de 1680*1050.compresión de vídeo formatos.*

Tras la digitalización de la imagen, se procede a su compresión el formato de compresión de vídeo puede ser m-jpeg, mpeg-4 o h.264/avc.m-jpeg es tradicionalmente más difundido en cámaras web. Cada frame de video o campo entrelazado es comprimido por separado como una imagen jpeg. Originalmente fue desarrollado para aplicaciones multimedia en pc. Aunque ya existen formatos más avanzados que lo han desplazado, sigue siendo el más utilizado en dispositivos portables de captura de vídeo.

El streaming HTTP separa cada imagen en respuestas HTTP individuales a un marcador especificado el servidor, en este caso la cámara, envía los paquetes de datos, la conexión no se cierra mientras el cliente "quiera" recibir más grabaciones y el servidor "quiera" emitirlas.

En cambio, MPEG-4 es transmitido típicamente sobre User Datagram Protocol (UDP), Real time Transporte Protocol (RTP), o Real Time Streaming Protocol (RTSP). UDP no garantiza el envío y ni retransmite los paquetes perdidos. UDP permite envío IP Multicast (IPmc), aunque no esté universalmente soportado.

A partir de 2008 se comenzó a incorporar el formato H.264, que permite ahorrar hasta

un 50% de información respecto a MPEC-4 Part2 y de 80% respecto a MJPEG. No obstante, la falta de estandarización en la industria hace que su difusión no sea más rápida, tanto MPEG-4 como H.264 son formatos patentados por los que se debe pagar, normalmente asociado a las cámaras IP compatibles con estas tecnologías.

Para ilustrar la importancia del formato de compresión, a continuación se muestran las tablas de almacenamiento entre diferentes tipos de compresión en una misma instalación de cuatro cámaras inteligentes, es decir, que sólo filman cuando se produce actividad.

Tabla 3 : Total de Datos Almacenados en 30 Días: 259.2GB

Compresión MPEG-4								
Cámara	*Resolución*	*FpS*	*Tamaño Imagen (KB)*	*Tasa de bits (Kbit/s)*	*MB por Hora*	*Horas de Operación*	*GB/día*	*Total GB en 30días*
1	***CIF***	***15***	***-***	***170***	***76.5***	***8***	***0.612***	***18.36***
2	***4CIF***	***15***	***-***	***400***	***180***	***8***	***1.44***	***43.2***
3	**CIF**	**15**	**-**	**880**	**396**	**12**	**4.752**	**142.56**
4	**CIF**	**5**	**-**	**170**	**76.5**	**24**	**1.836**	**55.08**

Tabla 4 : Total de Datos Almacenados en 30 días: 171.72 GB

Compresión H.264								
Cámara	*Resolución*	*FpS*	*Tamaño Imagen (KB)*	*Tasa de bits (Kbit/s)*	*MB por Hora*	*Horas de Operación*	*GB/día*	*Total GB en 30días*
1	***CIF***	***5***	***-***	***110***	***49.5***	***8***	***0.396***	***11.88***
2	***4CIF***	***15***	***-***	***250***	***112.5***	***8***	***0.9***	***27***
3	***CIF***	***15***	***-***	***600***	***270***	***12***	***3.24***	***97.2***
4	***CIF***	***5***	***-***	***110***	***49.5***	***24***	***1.188***	***35.64***

Tabla 5 : Total de Datos Almacenados en 30 días: 1170.72GB

Compresión M-JPEG								
Cámara	*Resolución*	*FpS*	*Tamaño Imagen (KB)*	*Tasa de bits (Kbit/s)*	*MB por Hora*	*Horas de Operación*	*GB/día*	*Total GB en 30días*
1	***CIF***	***5***	***13***	***-***	***234***	***8***	***1.872***	***56.16***
2	***4CIF***	***15***	***13***	***-***	***702***	***8***	***5.616***	***168.48***
3	***CIF***	***15***	***40***	***-***	***2160***	***12***	***25,92***	***777.6***
4	***CIF***	***5***	***13***	***-***	***234***	***24***	***5,616***	***168.48***

3.5.6 Resolución

Es el número de puntos que capta la cámara, cuanto mayor sea, mayor número de píxeles representados, mayor es la definición y el nivel de detalle de las imágenes presentadas. Se mide en píxeles horizontales pixeles verticales. Tendremos una resolución horizontal y otra vertical, por ejemplo: 800x600, 1024x768, 1280x1024 La segunda cifra indica el número de veces que el haz de electrones ha de recorrer la*

*pantalla hasta completar la representación de la imagen con unas resoluciones de 1680*1050.*

3.5.7 Iluminación Mínima

Esta cámara tiene menor cantidad de luz necesaria para que la cámara produzca una imagen de calidad aprovechable la iluminación mínima se indica en lux que es una medida de iluminancia.

3.5.8Longitud Focal Variable

Tienen la ventaja de brindar varias longitudes focales agrupadas en un solo cuerpo de objetivo, lo cual se consigue mediante el movimiento de ciertos elementos dentro del mismo. Esto los hace más versátiles para el uso diario puesto que no requiere el cambio de objetivo para obtener una longitud focal diferente. Como desventaja, poseen más elementos ópticos, con lo cual existe una mayor probabilidad de aparición de aberraciones y mayor pérdida de luz, lo cual hace que sean menos luminosos que sus contrapartes de focal fija. Por otra parte, son más pesados y frágiles que un objetivo fijo en igual relación de luminosidad.

Existen tres tipos de objetivos de longitud focal variable: Los objetivos los ***multifocales****, los* ***par focales****. En las tres clases de objetivo pueden variar su longitud focal a voluntad del usuario sin embargo la diferencia entre ellas radica en que los par focales mantienen el foco durante el cambio de longitud focal, mientras que en los multifocales y en los vari focales la distancia de enfoque cambia.*

3.5.9Objetivos Multifocales

Son aquellos objetivos que puede adoptar un número limitado de distancias focales, pero nunca una posición intermedia entre ellas. Decimos que el paso de la máxima distancia focal a la mínima distancia focal se hace de forma discreta. Un objetivo multifocal no es un objetivo zoom, haciendo obligatorio el enfoque a cada cambio de distancia focal.

3.5.9.1 Objetivos Par Focales

Son aquellos aumentos en un microscopio no requieren volver a enfocar la muestra cuando los objetivos cambian. Los objetivos del revólver de un microscopio son par focales, es decir, al cambiar de un objetivo de bajos aumentos a uno de más altos aumentos sólo hay que retocar ligeramente el foco con el ajuste micrométrico.

3.5.9.2 Objetivos Vari Focal

Son aquellos objetivos que entre la mínima distancia focal y la máxima distancia focal puede situarse en cualquier posición intermedia pasando de una a una de forma continua multifocales ,par focales y vari focales.

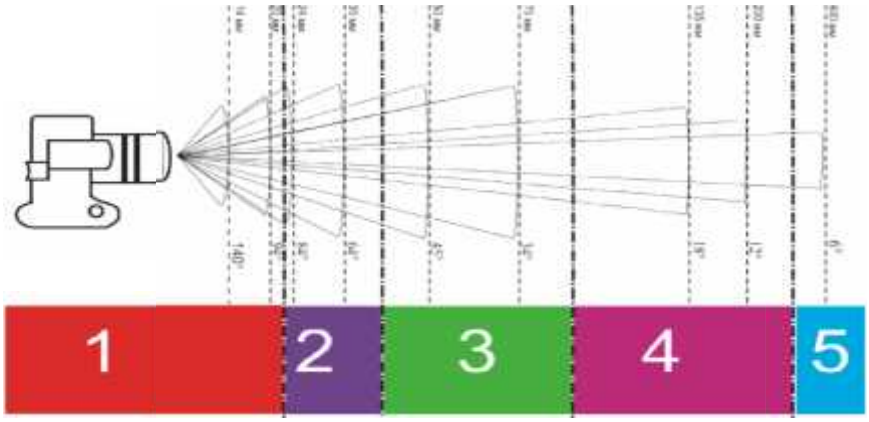

FIGURA 29: 1y 2 multifocales 3 y 4 par focales y 5 vari focal

Fuente: https://es.wikipedia.org/wiki/Objetivo_(fotograf%C3%ADa)

3.5.10 Alcance de Infrarrojos

Si la cámara va a estar colocada en un lugar con poca iluminación o se necesita Vigilancia 24 horas la mejor opción es colocar cámaras con visión nocturna. Estas cámaras graban durante el día a todo color y cuando hay poca iluminación encienden de forma automática sus infrarrojos para seguir grabando en blanco y negro tiene un alcance de 15 metros.

Tabla 6 : Características de la Cámara Visión

Sensor de imagen	*CMOS Color de 1/4"*
Resolución	*640 x 480 píxeles*
Iluminación mínima	*0 Lux IR ON*

Lente	*3,8 mm (66º)*
Alcance de infrarrojos	*15 metros*
Antena	*Omni 3dBi*
Potencia de transmisión	*100 mW*
Distancia de transmission aproximado	*Hasta 100 Metros en condiciones idóneas*
Frecuencia receptor	*ISM 2400-2483.5 MHz*
Detector PIR	*Detector de movimiento incorporado*
Micrófono	*Sí*
Altavoz	*Sí*
Alimentación	*AC 100~240V / DC 12V / 500mA*
Consumo	*270 mA Max*
Dimensiones	*110mm x 75mm x 82mm*
Peso	*555 gr (alimentador incluido)*

3.5.11 Dimensiones

Esta cámara tiene las siguientes dimensiones.

FIGURA 30 : Dimensiones

Fuente:https://www.mscsolarprojectspa.cl/producto/camara-ip-wifi-hd-2-antenas-vision-nocturna-infrarroja-para-exterior-interior-a-prueba-de-agua-app-yoosee/

3.5.12 Requisitos del Ordenador

Las cámaras no necesitan un ordenador para funcionar contienen un hardware y software que hace de servidor web autónomo. Únicamente necesitará un ordenador para su configuración inicial o si desea grabar las imágenes en el disco duro del ordenador. Posteriormente podrá ver las imágenes desde cualquier ordenador o móvil a través de Internet.

Requerimientos de configuración del sistema: *por ejemplo para ver 4 cámaras al mismo tiempo:*

- ***CPU:*** *2.06 GHz o más. Memoria: 256 Mb o más.*
- ***Tarjeta de red:*** *10M o más. Tarjeta gráfica: 64 Mb o más de memoria.*
- ***Sistemas Operativos:*** *Windows 2000, XP, Vista o 7.*

3.5.13 Instalación de Hardware

Luego realizar los siguientes pasos para configurar el hardware de la cámara. Asegurándonos de seguir cada pasó cuidadosamente para asegurar que la cámara opera adecuadamente.

a) *Conectar mediante el cable de red suministrado la cámara y el Router Cable/ADSL.*
b) *Conectar el adaptador de corriente a un enchufe y luego a la cámara en la clavija correspondiente.*
c) *La cámara tarda unos 30 segundos en iniciarse y luego mostrará una dirección IP asignada en el programa IP Camera, cuando la cámara se ha conectado correctamente el LED pasará de parpadear lentamente a parpadear más rápido.*

3.5.14 Instalación de Software CMS H264

La instalación del software es la clave para configurar exitosamente la cámara inalámbrica. Esencialmente este software sirve para ver la cámara asignada inicialmente y poder acceder así a su menú.

La instalación universal del software ***CMS H264*** *es extremadamente simple, simplemente haga clic en el icono y siga paso a paso, haciendo clic en "Next". Al final del proceso de instalación, elija el idioma que prefiera usar.*

FIGURA 31: Instalación de Software CMS H264

Fuente:https://aprendacctv.com/software-gratuito-de-video-vigilancia-monitoreo-de-dvr-h264/

3.5.15 Administrador

Cuando se inicia sesión como administrador, se activa la opción para administrador que nos dará:

- ***Información del dispositivo.-*** *muestra información sobre el ID de dispositivo (MAC única), Versión del firmware, Versión del dispositivo de interfaz de usuario, Alias, status, Condición DDNS.*
- ***Configuración Alias:*** *puede introducir el nombre que desee para identificar la cámara.*
- ***Fecha y Hora:*** *página de configuración de fecha, hora, zona horaria y forma de actualización.*
- ***Configuración de usuarios:*** *dispone de hasta 8 cuentas de usuario en los que puede especificar el nombre de usuario, contraseña y grupo al que pertenece.*
- ***Visitante:*** *sólo se pueden ver las imágenes, activar el audio y grabar las imágenes.*
- ***Operador:*** *se puede controlar la dirección de la cámara y configurar algunos parámetros.*
- ***Administrador:*** *se pueden realizar configuraciones avanzadas de la cámara.*

Los equipos y materiales son:

Tabla 7 : Materiales a Utilizar

Nombre	***Cantidad***	***Valor***
Cámara HIKVISION	*1*	*500Bs*
Router	*1*	*200 Bs*
Cable de red UTP cate. 6	*1 mt*	*600 Bs*
Dvr 4 Canales	*1*	*400 Bs*

Access Point	*1*	*500 Bs*
Cable UTP Cat.6 para exterior Miokee,carrete	*3.5 mt.*	*170 Bs*
RackGabinete5ruParedIdealParaDvrSwitchRouter	*1*	*130 Bs*
Conector de red RJ45 Bolsa 10	*1*	*50 Bs*
Rack: Gabinete De Pared 5ru X51	*1*	*160 Bs*
Monitor Dell18.5E1916hv	*1*	*1000 Bs*
Total		*3610 Bs*

3.5.16Configuración en los Router

ROUTER - MONITOREO

Router>ena

Router#config t

Router (config)#line console 0

Router (config-line)#password villca

Router (config-line)#login

Router (config-line)#exit

Router (config)#hostname ISP

ISP (config)#line vty 0 4

ISP (config-line)#password villca

ISP (config-line)#login

ISP (config-line)#exit

ISP#wr

Building configuration...

[OK]

ISP#exit

User Access Verification

Password:

Password:

ROUTER- ACOGIDA NIÑO JESUS

ISP>ena

ISP#config t

ISP(config)#hostname ISP

ISP(config)#int fa0/0

ISP(config-if)#ip add 200.44.32.1 255.255.255.0

ISP(config-if)#no sh

ISP(config-if)#

ISP(config-if)#^Z

ISP#wr

ISP#

ISP#config t

ISP (config)#int fa0/1

ISP (config-if)#ip add 190.200.0.254 255.255.255.0

ISP (config-if) #no sh

ISP (config-if)#

ISP (config-if)#^Z

ISP#wr

[OK]

ISP#config t

ISP (config-if) #router eigrp

ISP (config-if) #network 190.200.0.0 0.0.0.255

ISP (config-if) #network 200.44.32.0

ISP (config-if) #exit

3.5.17 Simulaciones en Packet Traicer Centro de Acogida Niño Jesús

FIGURA 32 : Centro de Acogida niño Jesús

Fuente: Elaboración Propia

3.5.18 Configuración DHCP

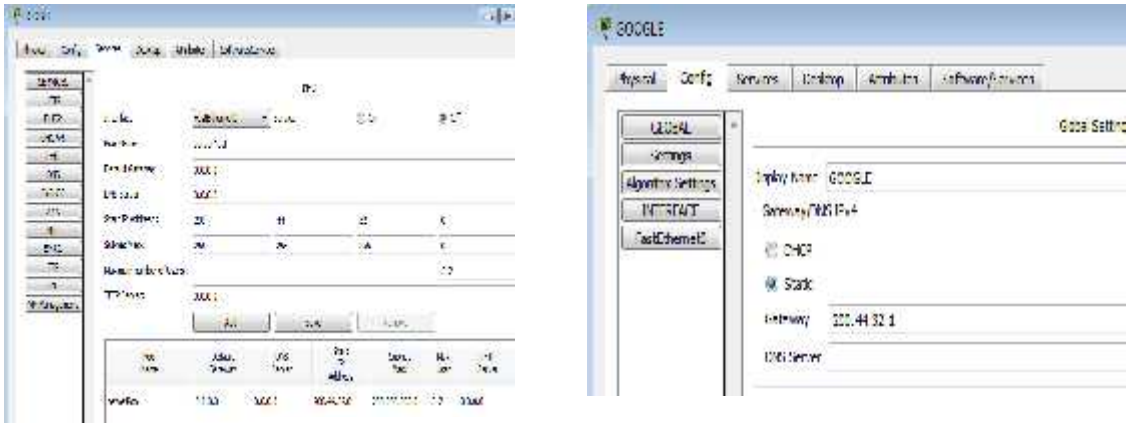

FIGURA 33: Configuración

Fuente: Propia

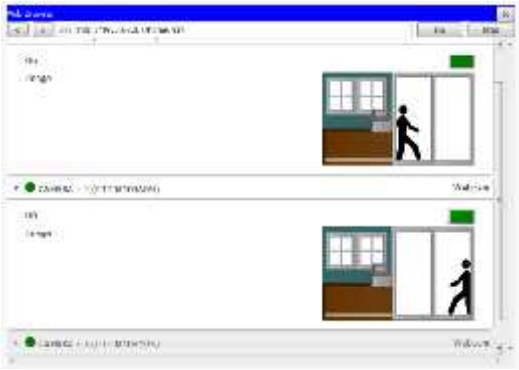

FIGURA 34: Cámara en Funcionamiento

Fuente: Elaboración Propia

3.5.19 Sala de Monitoreo

FIGURA 35 : Sala de Monitoreo

Fuente: Elaboración Propia

3.5.20 Centro de Acogida Niño Jesús

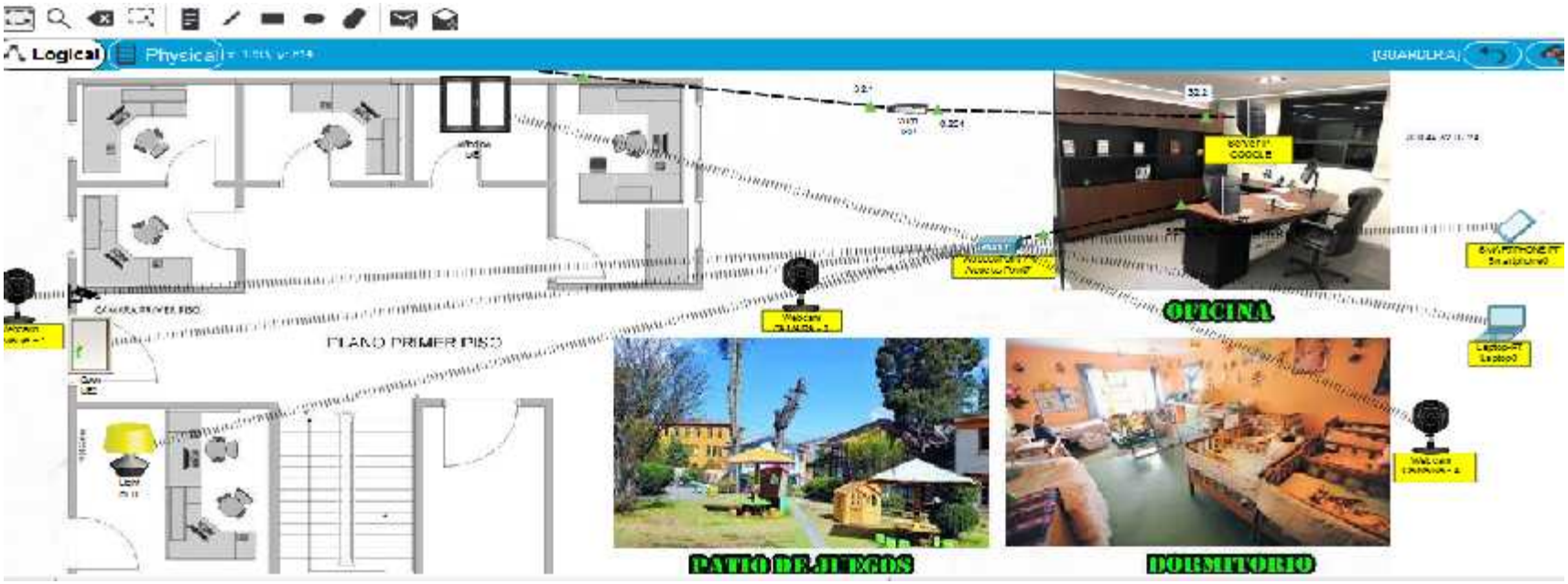

FIGURA 36 : Centro de Acogida Niño Jesús

Fuente: Elaboración Propia

3.5.21 Ingresos con Contraseña para las Cámaras

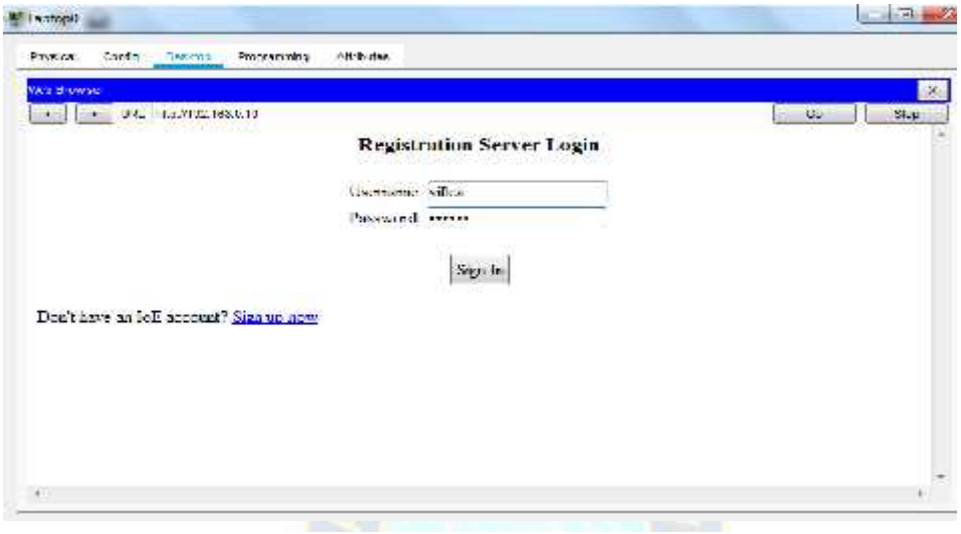

FIGURA 37 : Ingreso con Contraseña

Fuente: Elaboración Propia

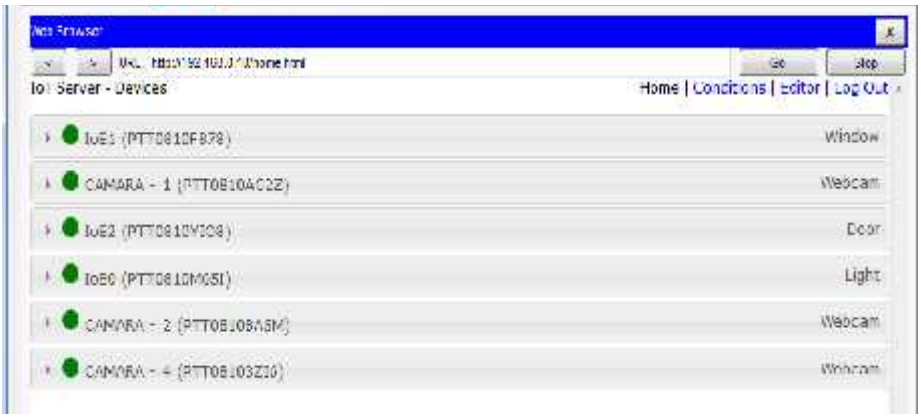

FIGURA 38 : Verificación de las Distintas Cámaras

Fuente: Elaboración Propia

3.5.22 Funcionamientos de las Cámaras

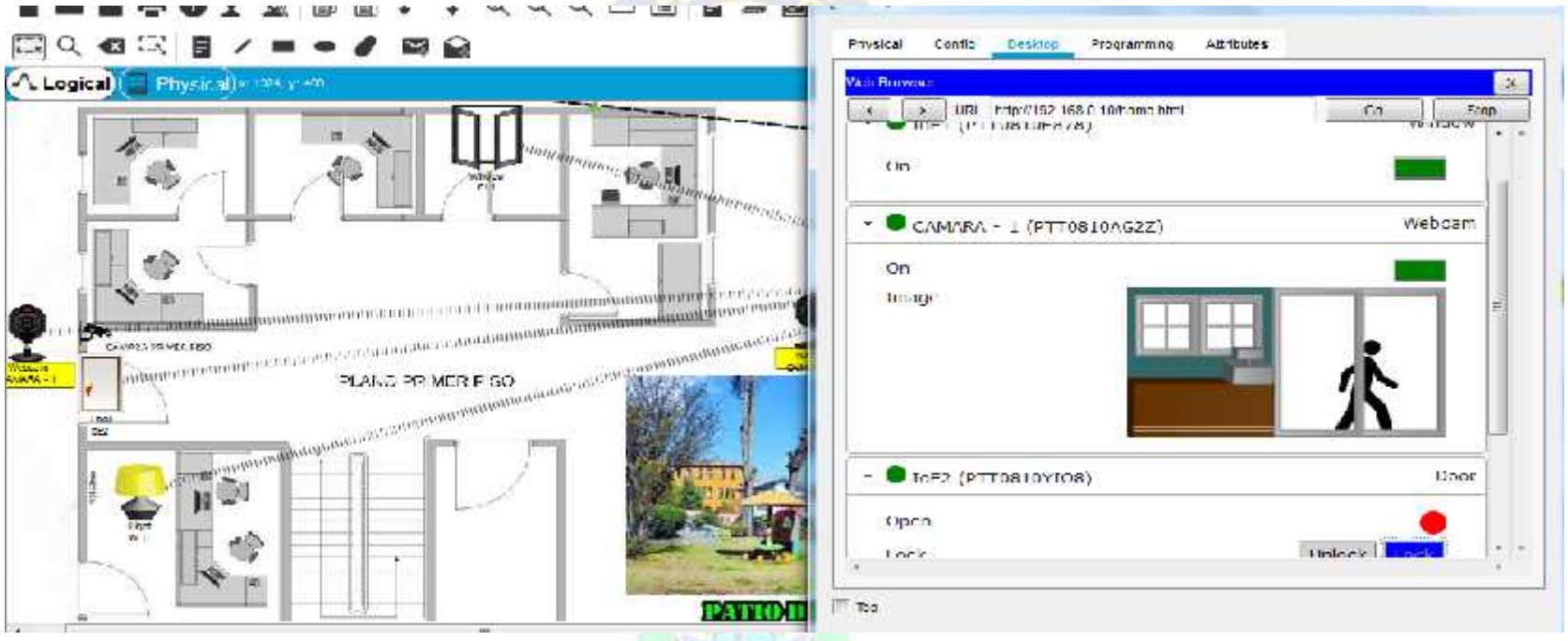

FIGURA 39 : Funcionamiento de las Cámaras

Fuente: Elaboración Propia

3.5.23 Cámara 1 Funcionando

FIGURA 40 : Funcionamiento de la cámara 1

Fuente: Elaboración Propia

CAPITULO IV

4. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- *Al ir desarrollando este proyecto se aprende bastante sobre los sistemas de redes tanto en la configuración y simulación.*
- *Dependiendo del uso que se le puede dar las redes inalámbricas puede ser una gran ventaja para la seguridad en dónde se esté manejando.*
- *Se buscó la información de diferentes fuentes y paginas para la realización de este proyecto.*
- *Se diseñó cumpliendo con los requerimientos de las instalaciones del centro de Acogida Niño Jesús*
- *Se logró realizar la simulación de la red con cámaras ip inalámbricas para los predios del centro de acogida niño Jesús*
- *Este proyecto puede ser implementado tanto en colegios, universidades o hasta en las mismas viviendas ya que su instalación es de manera inalámbrica.*

4.2 Bibliografía

1.- GUERRERO, JULIO MUÑOZ. 2016.*SISTEMAS DE SEGURIDAD. s.l. : PARANINFO, 2016.*

2.- Madrid), Jose Maria Merchan(Inginiero de telecomunicaciones por la universidad de. 2012 (1ra Edicion).*DISEÑO E INSTALACION DE SISTEMAS DE VIDEOVIGILANCIA CCTV DIGITALES. MADRID : s.n., 2012 (1ra Edicion). 512.*

3.*- Cisco. (2009). MANUAL DE ADMINISTRACION DE ROUTERS Y SWITCHES.*

4.3 Páginas Web

- *http://www.axxonsoft.com/sp/products/axxon_next/installation/*
- *http://zoominformatica.com/blog/como-configurar-camara-ip/*
- *http://www.laprensa.hn/mundo/767771-410/muere-beb%C3%A9-tras-ser-violado-en-orfanato-de-bolivia*
- *https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_metropolitana*
- *http://www.trabajosocial.unlp.edu.ar/uploads/docs/switch__routers_y_acces_point__conceptos_generales.pdf*

- *https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/*
- *https://es.wikipedia.org/wiki/Modelo_OSI*
- *https://www.ambit-bst.com/blog/todo-lo-que-debes-saber-de-cisco-packet-tracer*
- *https://argos.red/ventajas-de-las-camaras-ip/*
- *https://www.swann.com/downloads/drivers/DVR_4000/DVR4%268_3000%264000_M34K48CH151112S.pdf*
- *https://laracctv.wordpress.com/conecta-tu-dvr-a-internet/*
- *https://edualejo77.wordpress.com/2014/01/26/manual-para-visualizacion-de-dvrs-hikvision-a-traves-de-internet-con-su-servidor-ddns/*
- *https://repositorio.umsa.bo/xmlui/bitstream/handle/123456789/19031/PG-2160.pdf?sequence=1&isAllowed=y*
- *https://vdocumento.com/seguridad-de-tcp-ip-de-seguridad-de-la-familia-de-protocolos-tcpip-anlisis-de.html*
- *https://red.uao.edu.co/bitstream/handle/10614/9976/T07643.pdf?sequence=1&isAllowed=y*
- https://es.slideshare.net/eduardo_onofre123/topologas-y-componentes-de-una-red-inalmbrica