



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE INFORMÁTICA Y ELECTRÓNICA
ESCUELA DE INGENIERÍA EN ELECTRÓNICA,
TELECOMUNICACIONES Y REDES

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD
MEDIANTE VIDEO VIGILANCIA INALÁMBRICO USANDO
CÁMARAS IP PARA LA FIE.

TRABAJO DE TITULACIÓN: PROPUESTA TECNOLÓGICA

Trabajo de titulación presentado para optar al grado académico de:
INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y
REDES

AUTOR: BRAULIO WLADIMIR SARABIA BUÑAY

TUTOR: ING. PAUL DAVID MORENO AVILÉS

Riobamba – Ecuador

2018

©2018, Braulio Wladimir Sarabia Buñay

Se autoriza la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento, siempre y cuando se reconozca el Derecho de Autor

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE INFORMATICA Y ELECTRÓNICA
ESCUELA DE INGENIERIA EN ELECTRONICA TELECOMUNICACIONES
Y REDES

El Tribunal de Tesis certifica que: El trabajo de investigación: DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD MEDIANTE VIDEO VIGILANCIA INALAMBRICO USANDO CAMARAS IP PARA LA FIE, de responsabilidad del Señor Braulio Wladimir Sarabia Buñay, ha sido minuciosamente revisado por los Miembros del Tribunal de Tesis, quedando autorizada su presentación.

Dr. Julio Santillán

VICEDECANO

Ing. Patricio Romero

DIRECTOR DE ESCUELA

Ing. David Moreno

DIRECTOR DE TESIS

Ing. Jorge Yuquilema

MIEMBRO DEL TRIBUNAL

Yo, Braulio Wladimir Sarabia Buñay soy responsable de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la Escuela Superior Politécnica de Chimborazo.

BRAULIO WLADIMIR SARABIA BUÑAY

DEDICATORIA

A mi familia, que han sido mi gran apoyo y motivación para salir adelante, y especialmente quiero agradecer con todo mi corazón a la persona que más amo C A G V, que ha estado a mi lado dándome alientos para poder culminar mi carrera profesional, me ha ayudado y me ha apoyado en todo momento y ha sido mi más grande inspiración, sus palabras de aliento han sido la mayor fortaleza que me han podido brindar en los peores momentos de mi vida. Mil gracias por estar a mi lado brindándome su apoyo incondicional, quiero decirle que siempre podrá contar con mi apoyo, es lo mejor que me paso en la vida. De todo corazón mil gracias.

Braulio.

AGRADECIMIENTO

Agradezco a Dios, a mis padres que nunca dejaron de apoyarme a lo largo de mi vida, gracias por brindarme su apoyo y su comprensión, a todas las personas que de una u otra forma me apoyaron en el transcurso de mi formación académica, especialmente a la persona que amo con todo mi corazón, gracias por estar a mi lado y por apoyarme de una manera excepcional mil gracias, también quiero agradecer al Ingeniero David Moreno, docente que ha sido un gran apoyo e inspiración en mi desarrollo profesional, a todos muchas gracias

Braulio.

TABLA DE CONTENIDOS

INDICE DE TABLAS.....	xi
INDICE DE FIGURAS.....	xii
INDICE DE GRAFICOS.....	xv
RESUMEN.....	xvi
SUMARY	xvii
INTRODUCCIÓN	1
CAPITULO I.....	6
1. MARCO TEORICO.....	6
1.1. Sistemas de video vigilancia.....	6
1.1.1. Sistema de CCTV.....	6
1.1.1.1. Componentes de un sistema de cctv.....	7
1.2. Evolución de la video vigilancia.....	8
1.2.1. Sistemas de CCTV analógicos usando VCR.....	8
1.2.2. Sistemas de CCTV analógicos usando DVR.....	9
1.2.3. Sistemas de CCTV analógicos usando DVR de red.....	10
1.2.4. Sistemas de CCTV analógico usando servidores de video	11
1.3. Sistemas de Video vigilancia IP	12
1.3.1. Que es Video IP	12
1.3.2. Ventajas de la video vigilancia IP respecto a sistemas analógicos	13
1.3.3. Aplicaciones de la video vigilancia IP respecto a sistemas analógicos.....	14
1.4. Elementos de un sistema de video vigilancia IP	15
1.4.1. Cámara IP.....	15
1.4.1.1. Componentes de una cámara IP.....	15
1.4.1.2. Características de una cámara IP.....	16
1.4.1.3. Tipos de cámaras IP	18
1.4.2. Cable UTP.....	19
1.4.2.1. Cable UTP categoría 5 y categoría 6.....	20
1.4.2.2. Diferencias.....	20
1.4.2.3. Interferencia	20
1.4.2.4. Velocidad.....	20
1.4.3. Codificador de video	20

1.4.4.	<i>Grabación y almacenamiento</i>	21
1.4.5.	<i>Software de gestión de video</i>	22
1.5.	<i>Audio</i>	23
1.5.1.	<i>Modos de audio</i>	23
1.5.2.	<i>Compresión de audio</i>	23
1.6.	<i>Video</i>	23
1.6.1.	<i>Compresión de video</i>	24
1.6.2.	<i>Estándares de compresión</i>	24
1.7.	<i>Sincronización de audio y video</i>	24
1.8.	<i>Red inalámbrica</i>	24
1.8.1.	<i>Que es una red inalámbrica</i>	24
1.8.1.1.	<i>Tipos de redes inalámbricas</i>	25
1.8.2.	<i>Tecnologías de una red inalámbrica</i>	26
1.8.2.1.	<i>WI-FI (“Wireless Fidelity”)</i>	26
1.8.2.2.	<i>Infrarrojo</i>	27
1.8.2.3.	<i>Bluetooth</i>	27
1.8.2.4.	<i>Microondas</i>	27
1.8.2.5.	<i>Laser</i>	27
1.8.3.	<i>Arquitectura de una red inalámbrica</i>	27
1.8.3.1.	<i>Diseño de una red inalámbrica</i>	27
1.8.3.2.	<i>Redes con tecnología 802.11</i>	28
1.8.4.	<i>Espectros inalámbricos</i>	28
1.8.5.	<i>Intensidad de la señal</i>	28
1.8.6.	<i>Antenas</i>	29
1.8.7.	<i>Protocolo IP</i>	29
1.8.7.1.	<i>Modelo de referencia OSI</i>	29
1.8.7.2.	<i>Modelo de referencia TCP/IP</i>	30
1.8.7.3.	<i>Direccionamiento IP</i>	31
1.8.7.4.	<i>Dirección IPv4</i>	32
1.8.7.5.	<i>Subredes</i>	32
1.8.7.6.	<i>VLANS</i>	32
1.8.8.	<i>Seguridad</i>	32
1.8.9.	<i>Autenticación</i>	33

CAPITULO II	34
2. MARCO METODOLOGICO	34
2.1. Descripción del marco legal	34
<i>2.1.1. Ley de Seguridad Pública y del Estado</i>	<i>34</i>
<i>2.1.2. Norma ISO/IEC 27001</i>	<i>34</i>
<i>2.1.2.1. Ciclo PDCA para el sistema de videovigilancia inalámbrico</i>	<i>36</i>
2.2. Estudio de la situación actual de la FIE.....	37
<i>2.2.1. Descripción de la infraestructura de la FIE.....</i>	<i>37</i>
2.3. Sistema de videovigilancia inalámbrico propuesto para la FIE	39
<i>2.3.1. Requerimientos del sistema de videovigilancia.....</i>	<i>39</i>
<i>2.3.2. Elección de las tecnologías para el sistema de video vigilancia.....</i>	<i>40</i>
<i>2.3.2.1. Selección del medio de transmisión.....</i>	<i>40</i>
<i>2.3.2.2. Selección de las cámaras IP</i>	<i>40</i>
<i>2.3.2.3. Selección del medio de monitoreo y almacenamiento</i>	<i>41</i>
2.4. Interferencia en las redes inalámbricas existentes en el edificio de la FIE.....	41
<i>2.4.1. Análisis de las redes inalámbricas existentes en el edificio</i>	<i>42</i>
<i>2.4.1.1. Lista de redes WIFI al alcance y numero de dispositivos conectados</i>	<i>43</i>
<i>2.4.1.2. Niveles de las señales</i>	<i>44</i>
<i>2.4.1.3. Canales en que las redes están transmitiéndola señal</i>	<i>45</i>
<i>2.4.2. Principales redes inalámbricas existentes en el edificio de la FIE.....</i>	<i>45</i>
<i>2.4.2.1. Lista de las principales redes WIFI.....</i>	<i>46</i>
<i>2.4.2.2. Análisis y estudio de cada red</i>	<i>47</i>
<i>2.4.2.3. Elección de la mejor red WIFI</i>	<i>50</i>
<i>2.4.3. Red inalámbrica para el sistema de seguridad</i>	<i>51</i>
<i>2.4.3.1. Análisis de la red inalámbrica Hikvision</i>	<i>52</i>
CAPITULO III.....	54
3. MARCO DE RESULTADOS	54
3.1. Diseño del sistema de video vigilancia	54
<i>3.1.1. Infraestructura y situación actual del edificio de la FIE.....</i>	<i>54</i>
<i>3.1.1.1. Planta baja</i>	<i>55</i>
<i>3.1.1.2. Primer piso</i>	<i>55</i>
<i>3.1.1.3. Segundo piso.....</i>	<i>56</i>
<i>3.1.2. Requerimientos para el diseño e implementación del sistema de video vigilancia ..</i>	<i>56</i>

3.2.	Descripción de los elementos a utilizar para el sistema de video vigilancia	56
3.2.1.	Cámaras	57
3.2.1.1.	<i>Cámara IP domo DS-2CD1121-i</i>	57
3.2.1.2.	<i>Cámara IP bullet DS-2CD1021-i</i>	58
3.2.2.	Servidor y medio de almacenamiento	59
3.2.2.1.	<i>NVR Ds7608ni-e2/8p</i>	59
3.2.2.2.	<i>Disco Duro Western Digital 1TB</i>	60
3.2.2.3.	<i>Software gestión de almacenamiento</i>	61
3.2.3.	Monitor	62
3.2.4.	Protocolos	63
3.2.5.	Acceso remoto y visualización	64
3.2.6.	Alimentación eléctrica	69
3.3.	Lugar estratégico para la ubicación de los equipos	70
3.3.1.	Ubicación de las cámaras	70
3.3.1.1.	<i>Segundo Piso</i>	71
3.3.1.2.	<i>Primer Piso</i>	71
3.3.1.3.	<i>Planta Baja</i>	71
3.3.1.4.	<i>Afuera del edificio</i>	71
3.3.2.	<i>Ubicación de la central de monitoreo</i>	72
3.4.	Diseño físico del sistema de video vigilancia	73
3.5.	Diseño lógico del sistema de video vigilancia	74
3.6.	Implementación del sistema de video vigilancia	76
3.6.1.	Tendido de cables para la alimentación eléctrica	76
3.6.2.	Instalación y visualización de cada cámara IP	77
3.6.2.1.	<i>Segundo Piso</i>	77
3.6.2.2.	<i>Primer Piso</i>	79
3.6.2.3.	<i>Planta Baja</i>	81
3.6.2.4.	<i>Afuera del edificio</i>	83
3.6.3.	Instalación y visualización del servidor NVR	85
3.6.4.	Instalación de las canaletas	86
3.6.5.	Instalación del logotipo de grabación	88
3.7.	Configuración de los equipos	89
3.7.1.	Configuración del NVR a la plataforma Hik-Connect	89
3.7.2.	Configuración del NVR	92

3.7.3.	<i>Configuración de las cámaras IP</i>	93
3.7.3.1.	<i>Detección de las Direcciones IP para cada cámara</i>	93
3.7.3.2.	<i>Configuración de cámaras IP tipo Domo y tipo Bala</i>	94
3.7.4.	<i>Conexión entre el NVR y las cámaras IP</i>	96
3.7.5.	<i>Configuración de la alimentación eléctrica por medio de PoE</i>	97
3.7.6.	<i>Configuración para la grabación de los videos</i>	97
3.8.	Calculo del almacenamiento para nuestro sistema de video vigilancia	99
3.8.1.	<i>Ancho de banda del sistema</i>	99
3.8.2.	<i>Calculo del almacenamiento</i>	99
3.9.	Pruebas de funcionamiento	101
3.10.	Costos	104
3.10.1.	<i>Costos Directos</i>	104
3.10.2.	<i>Costos indirectos</i>	104
3.10.3.	<i>Costos totales</i>	104
	CONCLUSIONES	105
	RECOMENDACIONES	106
	GLOSARIO	1
	BIBLIOGRAFIA	- 2 -
	ANEXOS	- 5 -

INDICE DE TABLAS

Tabla 1-2: Tabla comparativa para determinar la señal WIFI con mejor calidad.....	51
Tabla 1-3: Longitud del cable desde las cámaras IP hasta el NVR.....	74
Tabla 2-3: Longitud del cable desde el rack de servidores hasta el NVR.....	74
Tabla 3-3: Costos directos del sistema de video vigilancia	104
Tabla 4-3: Costos indirectos del sistema de video vigilancia	104
Tabla 5-3: Costos totales del sistema de video vigilancia.....	104

INDICE DE FIGURAS

Figura 1-1: Sistemas de CCTV analógico usando VCR.....	9
Figura 1-2: Sistema de CCTV analógico usando DVR	10
Figura 1-3: Sistema de CCTV analógico usando DVR de Red	11
Figura 1-4: Sistema de cctv analógico usando servidores de video.....	11
Figura 1-5: Sistema de video vigilancia IP	13
Figura 1-6: Componentes de una cámara IP	15
Figura 1-7: Sensibilidad de luz	17
Figura 1-8: Resolución de una imagen	17
Figura 1-9: Tipos de cámaras IP	19
Figura 1-10: Codificador de video.....	21
Figura 1-11: Red Inalámbrica	25
Figura 1-12: Tipos de redes inalámbricas.....	25
Figura 1-13: Capas del modelo OSI	30
Figura 1-14: Capas del modelo TCP/IP	31
Figura 2-1: Ciclo de Demming	35
Figura 2-2: Ciclo PDCA de la norma ISO/IEC 27001 aplicada al presente trabajo	36
Figura 2-3: Vista frontal del edificio de la FIE.....	38
Figura 2-4: Vista interior del edificio de la FIE.....	38
Figura 2-5: Software Acrylic	42
Figura 2-6: Lista de redes wifi.....	43
Figura 2-7: Redes principales WIFI existentes en el edificio FIE	46
Figura 2-8: Lista de las redes específicas	46
Figura 2-9: Red Wifi principal en el edificio de la FIE	52
Figura 3-1: Cámara IP DS-2CD1121-i tipo Domo	57
Figura 3-2: Cámara IP DS-2CD1021-i tipo Bullet	58
Figura 3-3: NVR IP DS7608ni-e2/8p	60
Figura 3-4: Disco Duro Western Digital 1TB.....	61
Figura 3-5: Software gestión de video Ivms-4200.....	62
Figura 3-6: Monitor Flatron L177WSB.....	63
Figura 3-7: Instalación del Software IVMS 4200.....	64
Figura 3-8: Instalación del Software IVMS 4200.....	65
Figura 3-9: Registro en Software IVMS 4200.....	65
Figura 3-10: Ejecución del Software IVMS 4200	66
Figura 3-11: Ejecución del Software IVMS 4200	66

Figura 3-12: Registro del dispositivo NVR	67
Figura 3-13: Registro del dispositivo NVR	68
Figura 3-14: Numero de cámaras añadidas.....	68
Figura 3-15: Software y cámaras en funcionamiento	69
Figura 3-16: Central de monitoreo.....	72
Figura 3-17: Diseño físico del sistema de video vigilancia	73
Figura 3-18: Diseño lógico del sistema de video vigilancia	75
Figura 3-19: Tendido de cable para alimentación eléctrica	76
Figura 3-20: Instalación de la cámara 1, segundo piso.....	77
Figura 3-21: Visualización de la cámara 1, segundo piso	77
Figura 3-22: Instalación de la cámara 2, segundo piso.....	78
Figura 3-23: Visualización de la cámara 2, segundo piso	78
Figura 3-24: Instalación de la cámara 3, primer piso.....	79
Figura 3-25: Visualización de la cámara 3, primer piso	79
Figura 3-26: Instalación de la cámara 4, primer piso.....	80
Figura 3-27: Visualización de la cámara 4, primer piso	80
Figura 3-28: Instalación de la cámara 5, planta baja	81
Figura 3-29: Visualización de la cámara 5, planta baja	81
Figura 3-30: Instalación de la cámara 6, planta baja	82
Figura 3-31: Visualización de la cámara 6, planta baja	82
Figura 3-32: Instalación de la cámara 7, puerta principal FIE.....	83
Figura 3-33: Visualización de la cámara 7, puerta principal FIE	83
Figura 3-34: Instalación de la cámara 8, parqueadero	84
Figura 3-35: Visualización de la cámara 8, parqueadero.....	84
Figura 3-36: Central de monitoreo.....	85
Figura 3-37: Visualización del sistema de videovigilancia	85
Figura 3-38: Instalación de las canaletas 2 piso.....	86
Figura 3-39: Instalación de las canaletas 1 piso.....	86
Figura 3-40: Instalación de las canaletas planta baja.....	87
Figura 3-41: Instalación de las canaletas exterior del edificio.....	87
Figura 3-42: Logotipo de seguridad de nuestro sistema de videovigilancia.....	88
Figura 3-43: Ventana principal Hikvision	89
Figura 3-44: Registro en Hikvision	90
Figura 3-45: Vinculo para añadir dispositivo	90
Figura 3-46: Registro del dispositivo NVR	91
Figura 3-47: Vista del dispositivo en línea	91
Figura 3-48: Configuración general del Sistema de videovigilancia	92

Figura 3-49: Configuración del NVR a la LAN	92
Figura 3-50: Acceso a la plataforma, dispositivo en línea.....	93
Figura 3-51: Configuración de cada cámara IP	94
Figura 3-52: Ajustes de imagen de cada cámara IP	94
Figura 3-53: Detección de movimiento de cada cámara IP	95
Figura 3-54: Configuración general de las cámaras IP	95
Figura 3-55: Funcionamiento del sistema de videovigilancia	96
Figura 3-56: Alimentación eléctrica de las cámaras, por medio del protocolo PoE.....	97
Figura 3-57: Tipo de grabación del video.....	98
Figura 3-58: Parámetros generales de grabación del video	98
Figura 3-59: Capacidad de almacenamiento de nuestro sistema de video vigilancia	100
Figura 3-60: Sistema de video vigilancia, visto desde NVR	101
Figura 3-61: Videos almacenados y grabados	102
Figura 3-62: Sistema de video vigilancia, visto desde IVMS-4200	103

INDICE DE GRAFICOS

Grafico 2-1: Intensidad de la señal	44
Grafico 2-2: Rango de frecuencia y número de canales	45
Grafico 2-3: Intensidad de la señal FIE	47
Grafico 2-4: Canal y rango de frecuencias de la señal FIE.....	47
Grafico 2-5: Intensidad de la señal ESPOCH-WIFI-P2.....	48
Grafico 2-6: Canal y rango de frecuencias de la señal ESPOCH-WIFI-P2	49
Grafico 2-7: Intensidad de la señal ESPOCH-FIE-DOCENTES.....	49
Grafico 2-8: Canal y rango de frecuencias de la señal ESPOCH-FIE-DOCENTES	50
Grafico 2-9: Intensidad de la señal HIKVISION	52
Grafico 2-10: Canal y rango de frecuencias de la señal HIKVISION	53

RESUMEN

La finalidad de este trabajo de titulación fue implementar un sistema de seguridad mediante videovigilancia en cual permita realizar un control y supervisión con transmisión de video en alta definición para la Facultad de Informática y Electrónica de la Escuela Superior Politécnica de Chimborazo. El sistema que se utilizó está basado en (IP) protocolos de internet el cual proporciona los medios necesarios para la transmisión de datos llamados datagramas desde el origen al destino, se realizó un estudio de la infraestructura de la FIE con el propósito de determinar los lugares más estratégicos para la ubicación de todos los equipos que cuenta este sistema de videovigilancia, para la alimentación eléctrica de las cámaras se utilizó el protocolo (PoE) Power Over Ethernet. Para la elección de cada componente de este sistema se realizó un análisis de características, mejores prestaciones, eficiencia y con los estándares más altos, tanto de las cámaras, grabador de video en red (NVR) y medios de comunicación; siendo el medio no guiado o inalámbrico el medio de transmisión y por el cual se podrá realizar un control de acceso remoto y con la ayuda del software IVMS-4200 se podrá tener una visualización de todas las cámaras en tiempo real. Una vez que se realizaron todos los aspectos antes mencionados se procedió a la implementación de cada componente del sistema de seguridad, dicha implementación se realizó sin modificar ni llegar a dañar las instalaciones del edificio ya que se mantuvo la estética del edificio; dotando al edificio con un total de 8 cámaras IP. Se concluyó que el sistema de seguridad mediante videovigilancia está en correcto funcionamiento y con el propósito de no violar la privacidad y que las personas estén informadas de esta seguridad se colocó dos logotipos con la imagen de área vigilada en las dos entradas al edificio de la FIE, se recomienda entregar las claves y accesos a una sola persona.

Palabras claves: <TECNOLOGÍAS Y CIENCIAS DE LA INGENIERÍA>, <INGENIERÍA ELECTRÓNICA>, <PROTOCOLO DE INTERNET (IP)>, <VIDEOVIGILANCIA>, <POWER OVER ETHERNET (PoE)>, <TELECOMUNICACIONES Y REDES>, <MEDIO NO GUIADO>, <GRABADOR DE VIDEO EN RED (NVR)>

SUMMARY

The purpose of this research was to implement a security system by means of video surveillance in which it allows to carry out a control and supervision with high definition video transmission for the Faculty of Information Technology and Electronics of the Polytechnic School of Chimborazo. The system that was used is based on (IP) internet protocols which provide the necessary means for the transmission of data called datagrams from the origin to the destination, a study was made of the infrastructure of the FIE with the purpose of determining the more strategic places for the location of all the equipment that this video surveillance system has, for the power supply of the cameras, the Power Over Ethernet protocol (PoE) was used. For the choice of each component of this system, an analysis of characteristics, better performance, efficiency and the highest standards was performed, both for cameras, network video recorder (NVR) and media; the non-guided or wireless medium is the means of transmission and through which remote access control can be performed and with the help of the IVMS-4200 software it will be possible to have a visualization of all the cameras in real time. Once all the aforementioned aspects were carried out, each component of the security system was implemented, this implementation was carried out without modifying or even damaging the building's facilities, since the aesthetics of the building were maintained; endowing the building with a total of 8 IP cameras. It was concluded that the security system by video surveillance is in correct operation and with the purpose of not violating the privacy and that people are informed of this security, two logos with the image of the monitored area in the two entrances to the FIE building were placed, it is recommended to give the keys and access to only one person.

Keywords: <TECHNOLOGIES AND ENGINEERING SCIENCES>, <ELECTRONIC ENGINEERING>, <INTERNET PROTOCOL (IP)>, <VIDEO SURVEILLANCE>, <POWER OVER ETHERNET (PoE)>, <TELECOMMUNICATIONS AND NETWORKS>, <UNDIRECTED ENVIRONMENT> <NETWORK VIDEO RECORDER (NVR)>

INTRODUCCIÓN

En los últimos años se ha producido un notable avance de la tecnología en cuanto al desarrollo de los sistemas de seguridad de videovigilancia se trata, dando como resultado una disminución a gran escala tanto de robos o atracos ya sea de locales comerciales, oficinas o instituciones, mediante el desarrollo e implementación de estos sistemas el nivel de la delincuencia se ha ido reduciendo.

Por la gran demanda que presentan estos sistemas de videovigilancia y debido a que las personas en su gran mayoría requieren los servicios de estos sistemas de seguridad, ya sean empresas o negocios comerciales y hasta instituciones públicas, con la finalidad de mantener un correcto funcionamiento y así poder proteger tanto su negocio y a las personas que laboran dentro de su negocio o institución, por esta y más razones los sistemas de seguridad van evolucionando con el transcurso del tiempo y van a la par con la evolución de la tecnología.

En el presente documento se realizó un estudio de las características y ventajas de un sistema de seguridad mediante videovigilancia, así como también de los puntos que pueden ser considerados de fácil acceso, las zonas donde se ubicaran las cámaras, a demás se realizó un estudio de los efectos de la interferencia producida por las redes de datos existentes. Para este estudio lo que se deberá analizar principalmente es la infraestructura de la Facultad de Informática y Electrónica.

Para el análisis posterior y con los datos obtenidos del estudio de la infraestructura podremos obtener el alcance de las cámaras de seguridad y con la ayuda de una calculadora en línea y datos manuales se podrá también calcular el rendimiento de toda la red de videovigilancia como por ejemplo el almacenamiento y finalmente con los datos obtenidos se procederá a implementar el sistema de seguridad mediante videovigilancia en la FIE.

Antecedentes

Antiguamente los sistemas de seguridad solo se los podía encontrar o instalar en lugares específicos, con la finalidad de resguardar robos o atracos, con el pasar del tiempo los sistemas de seguridad evolucionaron debido a la necesidad de una mayor seguridad, es por esta razón que estos sistemas son muy importantes ya que a más de brindar seguridad, y con la ayuda de estos sistemas de vigilancia los usuarios podrán sentirse más protegidos y a su vez su empresa u oficina podrán estar más seguras y confortables.

En la actualidad la seguridad se ha convertido en un tema muy importante a considerar para toda la sociedad en general, ya que permite salvaguardar la vida de las personas y mantener vigilados los bienes materiales ya sea de un negocio, empresa o institución, logrando así mantener la continuidad de estos. Esto hace que el hombre tome como una necesidad primaria el tema de seguridad.

El uso de las cámaras de seguridad comenzó como un elemento de seguridad de la preparación militar. El primer uso documentado de circuito cerrado de televisión CCTV se produjo en el año 1942 por parte del ejército alemán. Los primeros sistemas se componían únicamente de cámaras en blanco y negro conectadas a monitores y eran importantes para la observación de ensayos de misiles V2 en la preparación de los ataques militares de larga distancia.

Posteriormente aparecieron los generadores de cuadrantes con el fin de poder visualizar varias cámaras a la vez en el mismo monitor. A los primeros grabadores con grabación en cinta de video le siguieron los de grabación en disco digital. Paralelamente las cámaras también evolucionaron, dejando de lado las de b/w y centrándose en las de color, mejorando sensiblemente las resoluciones. (Reina, 2016)

Un sistema de seguridad debe ser instalado de una forma segura y que no brinde falsas alarmas de lo contrario podría ser ignorado. Antes de proceder al diseño y posteriormente a su instalación se debe tener en cuenta consideraciones como los objetos, equipos y las personas que vamos a proteger, así como también el presupuesto total del sistema de seguridad.

Mediante la realización e implementación de este proyecto se pretende resolver estas y otras inquietudes que se puedan presentar en el transcurso de su ejecución, previo al diseño y a su implementación se dará a conocer el tipo de cámaras IP que se va a utilizar, así como también los diferentes recursos e instrumentos a utilizar con sus respectivas características y su correcto funcionamiento.

Con la ejecución e implementación de este proyecto se pretende brindar seguridad principalmente al edificio de la FIE, ya que mediante este sistema se podrá controlar el uso adecuado de las instalaciones y de los equipos, así como también se podrá vigilar la parte interior y exterior de la facultad.

Formulación del problema

¿Es necesario diseñar e implementar un sistema de seguridad mediante video vigilancia inalámbrica para monitorear la FACULTAD DE INFORMATICA Y ELECTRONICA?

Sistematización del problema

¿Qué zonas de la Facultad de Informática y Electrónica pueden ser consideradas de fácil acceso?

¿Cuáles son las principales ventajas de este sistema de seguridad mediante video vigilancia inalámbrica?

¿Qué ventajas presenta el sistema de seguridad mediante video vigilancia frente a un sistema tradicional de CCTV?

¿Qué tipo de equipos se requieren para la instalación de este sistema de seguridad?

¿Cuáles son los lugares o áreas específicos para la ubicación de las cámaras IP?

¿Qué resultados se obtendrán a partir de la instalación del sistema de seguridad mediante video vigilancia?

Justificación teórica

La implementación de este proyecto busca, mediante la aplicación de la teoría y de los conceptos básicos de seguridad, configuración e instalación, encontrar explicaciones coherentes a situaciones internas (pérdida de información física, pérdida y daño físico de los equipos), situaciones externas (daño y mal uso de los espacios físicos de la institución, pérdida de bienes materiales tanto de maestros y estudiantes) que afectan en la enseñanza por parte de los maestros, en el aprendizaje de los estudiantes y en la seguridad de los mismos.

Lo expuesto anteriormente permitirá contrastar diferentes conceptos sobre la seguridad, logrando así evitar robos o atracos y convirtiendo en una realidad la ilusión de tener nuestra facultad más segura y confortable.

Justificación aplicativa

Este proyecto busca implementar un sistema de seguridad mediante video vigilancia inalámbrico que permita monitorear y visualizar en tiempo real todos los sucesos que pueden ocurrir en el transcurso del día.

Para la instalación de este proyecto se utilizará un Kit de cámaras IP con su respectivo NVR (Grabador de Video de Red) que se instala en una computadora y administra nuestras cámaras IP, además permitirá grabar y administrar imágenes ya digitales las cuales son enviadas desde las cámaras IP a través de una red

Este proyecto tiene la finalidad de mejorar el nivel de seguridad tanto de los estudiantes y de las instalaciones de la FIE, ya sea en la parte interior o exterior de la misma evitando así robos o atracos en nuestra facultad.

Objetivos

Objetivo General

Implementar un sistema de seguridad mediante video vigilancia inalámbrico usando cámaras IP para la FIE

Objetivos Específicos

- Analizar las principales características, ventajas y limitaciones del sistema de video vigilancia.
- Analizar los efectos de la interferencia producida por las redes de datos inalámbricas existentes.
- Estudiar las zonas de la FIE para que no existan puntos ciegos
- Determinar las áreas específicas para la ubicación de las cámaras
- Diseñar e implementar el sistema de seguridad mediante video vigilancia considerando los puntos de acceso no autorizado de la FIE.
- Especificar los mecanismos y los protocolos que se utilizarán para mantener la seguridad de la información.
- Determinar el rendimiento de la red de video vigilancia y su alcance

CAPITULO I

1. MARCO TEORICO

1.1. Sistemas de video vigilancia

La videovigilancia entre muchas funcionalidades permite grabar las imágenes que las cámaras capturan, así como también visualizar en tiempo real todo lo que está sucediendo en el lugar donde se encuentran instaladas. Estos sistemas son muy útiles tanto para empresas, negocios e instituciones ya que permiten mantener vigilado el lugar, evitando así robos o atracos dando como resultado una disminución notable en el nivel de inseguridad.

1.1.1. Sistema de CCTV

Un sistema cctv también conocido como Circuito Cerrado de Televisión, tiene como principal objetivo el control y la supervisión de las actividades que se están realizando dentro de un determinado lugar donde se encuentran instalado este sistema. Este sistema se considera cerrado ya que permite un acceso restringido del contenido de las imágenes solo a usuarios registrados.

Este sistema de cctv puede estar compuesto de una o varias cámaras de vigilancia, conectadas a uno o más monitores o televisores, los cuales reproducen las imágenes capturadas, estas imágenes pueden ser, simultáneamente, almacenadas en medios analógicos o digitales, según lo que requiera el usuario. Dichas cámaras se encuentran fijas en un determinado lugar y pueden estar contraladas remotamente desde una sala de control, donde se puede realizar la configuración requerida por el usuario.

Estos sistemas incluyen visión nocturna, operaciones asistidas por ordenador y detección de movimiento, que facilita al sistema ponerse en estado de alerta cuando algo se mueve delante de las cámaras. (García, 2010)

1.1.1.1. Componentes de un sistema de cctv

Entre los principales componentes de un sistema de circuito cerrado están:

Cámara. - Este es el principal componente del circuito cerrado ya que la cámara es el punto de generación de video de este sistema, existe una gran variedad de cámaras con especificaciones y características distintas que son:

- Blanco y negro, color y duales
- Temperatura de funcionamiento
- Resistencia a la intemperie
- Iluminación
- Condiciones ambientales
- Resolución
- Sistema de formato
- Voltaje de alimentación
- Dimensiones
- Tipo de lentes

Lentes. - Este componente viene en forma separa de la cámara, pero tiene un conector de rosca para que se pueda ensamblar en la cámara según sean los requerimientos del sistema, las especificaciones del lente varían según:

- Distancia del objeto
- Angulo mínimo de observación
- Vari focal o fijo
- Intensidad de luz

Monitor. -Mediante este componente podemos visualizar la imagen creada y transmitida por la cámara analógica, es muy importante tener en cuenta que un sistema de circuito cerrado de televisión requiere que el sistema esté en funcionamiento las 24 horas sin tener perdida en la calidad de la imagen.

Grabadoras. -Con la ayuda de estas grabadoras aparte de poder visualizar áreas específicas, me permiten analizar y realizar copias de seguridad de las grabaciones si el usuario lo desea. Las

grabadoras solían ser de cinta, pero con el avance de la tecnología y la llegada de los sistemas IP estas grabaciones se las realiza en discos duros, Pc o en grabadores digitales autónomos.

Matriz de video. - La funcionalidad de este dispositivo hace más cómoda la visualización de las distintas cámaras, pues permite monitorear y conmutar muchas cámaras a un monitor o múltiples monitores de salida, debido a esto se puede desplegar cualquier imagen de las cámaras de entrada en cualquier monitor de salida, esto puede ser de manera intermitente o en secuencia preprogramada, Dicha matriz puede actuar como una interfaz entre las cámaras, los monitores y el puesto de control.

Líneas de transmisión. -La finalidad de las líneas de transmisión es hacer que la señal de video que sale de las cámaras llegue en las mejores condiciones posibles al monitor, estas líneas deben ser capaces de transportar la señal video, puede alcanzar frecuencias de 8 MHz, con un mínimo de pérdidas. El método de transmisión ha ido cambiando según la evolución de la tecnología, el más usado es el cable coaxial, antecesor del cable UTP, usado en las modernas redes de videovigilancia IP. (García, 2010)

1.2. Evolución de la video vigilancia

La videovigilancia se define como “Vigilancia a través de un sistema de cámaras, fijas o móviles”. Los sistemas de vigilancia por video existen desde hace más tres décadas, pero han ido evolucionando en los últimos años debido al desarrollo tecnológico, la demanda de mayores niveles de seguridad y el estudio de técnicas de análisis de video.

La evolución de estos sistemas ha sido muy notable, debido a su avance que ha ido a la par con la evolución de la tecnología; desde la aparición de las primeras cámaras analógicas con tubo conectadas a VCR (Video Cassette Recorded) hasta los nuevos sistemas semiautomáticos. (García, 2010)

1.2.1. Sistemas de CCTV analógicos usando VCR

Estos sistemas de video vigilancia están compuestos de; cámaras las cuales deben tener sus especificaciones y características según sean las necesidades del usuario, matrices de video o multiplexores para un mejor manejo y gestión de las cámaras debido a que la información puede mostrarse en solo monitor o en varios monitores.

Las imágenes y toda la información grabada son almacenadas en un VCR. En este sistema los equipamientos incluyen: mecanismos de control de posición de cámara, controladores de señal, grabadores de señal, particionadores de imagen, interfonos para comunicación con la zona vigilada, etc. Cada uno de estos servicios va asociado a un cableado específico, por ejemplo, el del audio. (García, 2010)

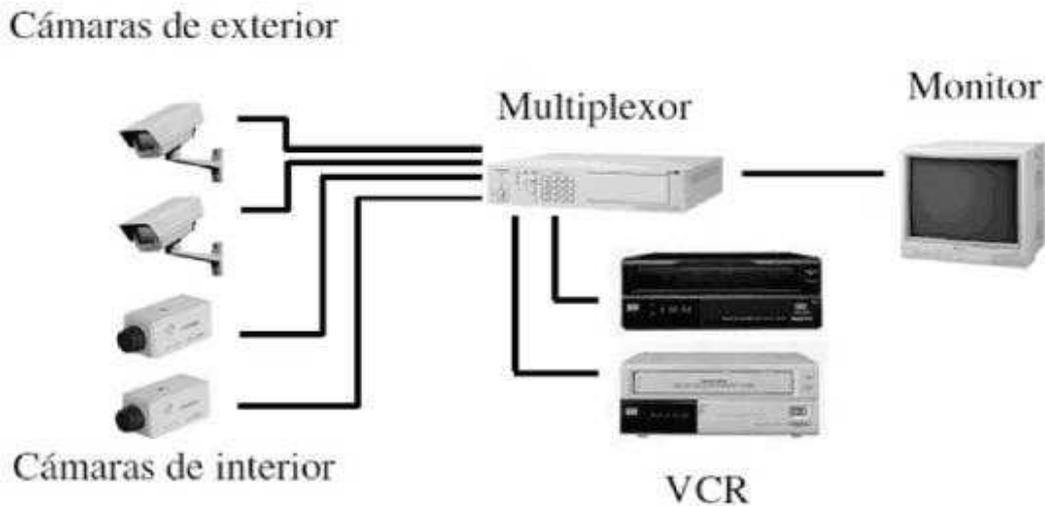


Figura 1-1: Sistemas de CCTV analógico usando VCR
Fuente: F.García, 2010

1.2.2. *Sistemas de CCTV analógicos usando DVR*

La primera revolución digital que tuvo la video vigilancia fue con la aparición del DVR (Digital Video Recorder) a mediados de la década de 1990. El DVR con sus discos duros sustituye el video como soporte de grabación, ya que el video se digitalizaba y se comprimía para poder almacenarlo el máximo número de días posible. Los primeros DVR's su espacio en disco era limitado, por lo que la duración de la grabación era limitada, por esta razón muchos fabricantes desarrollaron algoritmos de compresión de video, el único problema fue que cada fabricante desarrollo su propio algoritmo por lo que resulto un problema ya que no existía una estandarización. Con el paso de los años los costes de espacio en disco duro disminuyeron y los algoritmos de compresión como el MPEG-4 fueron ampliamente aceptados.

La introducción de los DVR presentó ventajas como:

- Mejor calidad de grabación
- Capacidad de buscar rápidamente en una grabación de video
- Desaparición de las cintas y la necesidad de cambiar las cintas

Con la aparición del DVR se redujeron el número de componentes en un cctv, debido a que los DVR's tenían varias entradas de video, por lo general 4,16 o 32, esto quiere decir que se incluían la funcionalidad de los quads o el multiplexor. Estos DVR utilizaban monitores analógicos, que era un aparato de televisión para mostrar imágenes de video, pero con la evolución del video digital se pudo transmitir imágenes a la red de datos, logrando transmitir video digital a largas distancias. (García, 2010)

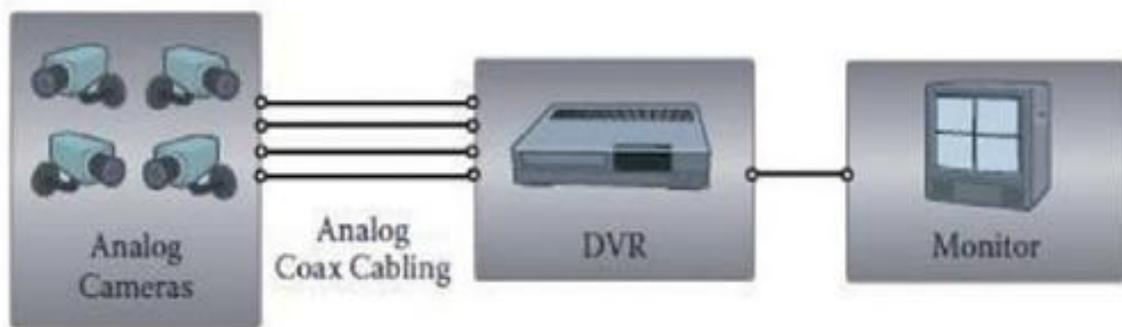


Figura 1-2: Sistema de CCTV analógico usando DVR

Fuente: F. García, 2010

El DVR presento una gran ventaja, debido a la capacidad de monitorizar de forma remota mediante un PC, pero su funcionalidad real no fue efectiva puesto que el ancho de banda con módems telefónicos era demasiado bajo, en el rango de 32 Kbps, esto hacía inviable el envío de video a través de la red ya que las tasas de envío eran muy bajas. (García, 2010)

1.2.3. Sistemas de CCTV analógicos usando DVR de red

Con el pasar del tiempo los DVR evolucionaron, contando con un puerto Ethernet que se utilizaban para conexiones a redes IP, por lo que se denominó DVR de red y permitía la monitorización remota a través de PC's y un control remoto del sistema. Así como el DVR presentaba grandes mejoras respecto al VCR también presentaba muchos inconvenientes, debido a que fue cargado de muchas tareas tales como: digitalización, grabación, compresión de video y funciones de conexión de red, por estas y otras funciones el DVR presentaba falencias y obligaba a que se le de mantenimiento y actualizaciones y en los peores casos buscar repuestos.

Con el pasar del tiempo y debido a que la información que se transmitía era por medio de la red, el DVR presentaba grandes inconvenientes con los virus. Aunque fueron diseñados en máquinas embebidas, el interfaz propietario no permitía la protección mediante antivirus. La protección contra virus es muy difícil de implementar y lo que dificultaba mas era que los DVR no permitían una fácil actualización. (García, 2010)

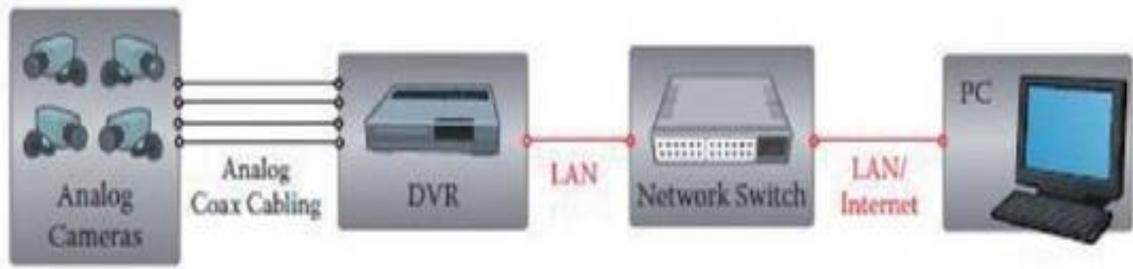


Figura 1-3: Sistema de CCTV analógico usando DVR de Red

Fuente: F. García, 2010

1.2.4. *Sistemas de CCTV analógico usando servidores de video*

Estos sistemas de video IP fueron los primeros y para su constitución se introdujo el codificador o más conocido como servidor de video. La función de un servidor de video es conectarse a cámaras analógicas para digitalizar y comprimir el video captado por ellas, luego envía el video sobre una red IP a través de un conmutador de red a un destinatario (un servidor) que ejecuta el software de gestión de video para la vigilancia y el control. Por esta razón las tareas que antes hacía el DVR se han repartido: el servidor de video digitaliza y comprime la señal y el destinatario (servidor) graba y gestiona, gracias a este reparto de tareas mejora la escalabilidad del sistema. (García, 2010)

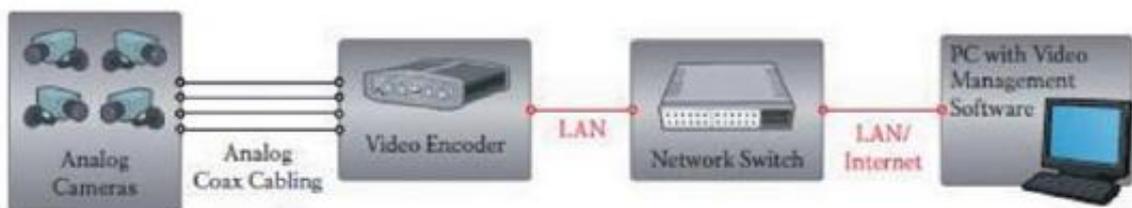


Figura 1-4: Sistema de cctv analógico usando servidores de video

Fuente: F. García, 2010

Este tipo de sistemas presentan ventajas tales como:

- Servidores PC's para la grabación y gestión de videos mediante el uso de la red IP
- Grabación remota
- Escalabilidad
- Sistema expandible

Con la aparición de estos sistemas en el campo de la video vigilancia, es posible utilizar diferentes tipos de NVR y DVR híbrido. Un **NVR** y **DVR híbrido** es un dispositivo propietario con el software de gestión de video preinstalado para la gestión de la señal de video que llega desde los servidores de video o de las cámaras. Cada dispositivo presenta características tales como:

- NVR solo maneja señales entrantes de video en red
- DVR híbrido puede manejar video en red y entradas analógicas en paralelo

Dichos dispositivos se suelen utilizar en pequeños sistemas ya sean de 4 a 16 cámaras, entre principal ventaja esta que todas las funcionalidades de gestión y grabación están disponibles en un solo dispositivo, utilizan plataformas propietarias y debido a esto ser muy costosos ya sea para adquirir, mantener y actualizar el sistema. (García, 2010)

1.3. Sistemas de Video vigilancia IP

Con el transcurso de los años y junto a ellos el avance de la tecnología, los sistemas de cctv van perdiendo influencia en el campo de videovigilancia debido a su infraestructura cableada, en la actualidad la videovigilancia IP (Internet Protocol) se ha posicionado en el mercado por la gran aceptación de los usuarios y por las ventajas que este sistema presenta ya que combina los beneficios que tiene los cctv, permitiendo así tener un control y monitoreo de la información que se tiene en un sistema de videovigilancia IP.

1.3.1. Que es Video IP

La video vigilancia IP o también llamado video IP es un tipo de comunicación que se realiza a través de redes estas pueden ser cableadas o inalámbricas. La información ya sea audio o video se efectúa por la misma infraestructura de red, una característica muy importante de la red IP es que se usa para alimentación eléctrica a algunos dispositivos como puede ser las cámaras IP mediante la tecnología PoE (Power Over Ethernet), además permite tener una monitorización remota en tiempo real. (García, 2010)

Un sistema de video vigilancia IP consta de:

- Cámaras IP
- Cámaras analógicas
- Servidores de video (adapta la señal de una cámara analógica a la red IP)
- Gestión de video (Servidor de almacenamiento)
- Sala de monitoreo
- Elementos de la red de datos (cables, routers, switches, etc.)



Figura 1-5: Sistema de video vigilancia IP

Fuente: F. García, 2010

1.3.2. Ventajas de la video vigilancia IP respecto a sistemas analógicos

Los sistemas de video vigilancia IP presentan ventajas tales como:

- **Accesibilidad Remota.** - Podemos visualizar el video en vivo y grabado desde cualquier ubicación en red, así como también configurar las cámaras IP y los servidores de video y acceder a ellos de forma remota.
- **Calidad de imagen.** - Tener una alta calidad de la imagen es muy importante para poder observar con claridad un incidente, así como también identificar a las personas u objetos implicados. La cámara de red produce una imagen de alta calidad, así como su

resolución más alta, debido a su tecnología de barrido progresivo y mega píxel, también la calidad de imagen se puede mantener más fácilmente en un sistema de video en red que en un sistema analógico. En un sistema de video vigilancia IP las imágenes se digitalizan una vez y se mantienen en formato digital sin conversiones innecesarias y sin degradación de las imágenes debido a la distancia que recorren por una red.

- **Gestión de eventos y video inteligente.** - Debido a grabaciones innecesarias que no contienen información relevante, se utiliza un software inteligente que incluyen funciones integradas como detección de movimiento por video mientras que para la función de gestión de video se configura mediante la interfaz de usuario del producto de video en red, entre su funcionalidad esta la grabación en uno o varios sitios por motivos de seguridad.
- **Estandarización.** - Todos los productos de video en red basados en estándares abiertos se pueden integrar fácilmente con sistemas de información basados en ordenadores y Ethernet, sistemas de audio o de seguridad y otros dispositivos digitales. Por ejemplo, el video de una cámara de red se puede integrar en un sistema de punto de venta o en un sistema de gestión de edificios.
- **Escalabilidad y flexibilidad.** - La video vigilancia IP puede crecer a la par con las necesidades del usuario, estos sistemas ofrecen una manera de compartir la misma red inalámbrica para la comunicación de datos, también se puede agregar al sistema cualquier cantidad de productos de video en red sin que esto suponga cambios o costosos para la infraestructura de red. (García, 2010)

1.3.3. Aplicaciones de la video vigilancia IP respecto a sistemas analógicos

Entre las principales aplicaciones que tiene la videovigilancia IP tenemos:

- Reconocimiento de matriculas
- Monitorización de tráfico rodado
- Vigilancia en vehículos de transporte publico
- Vigilancia del comportamiento de empleados
- Vigilancia en instituciones educativas, empresas, comercios, hoteles
- Aplicaciones educativas. (García, 2010)

1.4. Elementos de un sistema de video vigilancia IP

1.4.1. Cámara IP

Una cámara IP también conocida como cámara de red, es un dispositivo que capta y transmite una señal de audio y video digital a través de una red IP estándar a otros dispositivos de red, como un pc o teléfono móvil mediante el uso de una dirección IP dedicada. Los usuarios pueden visualizar, almacenar y gestionar video de forma local y remota en tiempo real. (García, 2010)

1.4.1.1. Componentes de una cámara IP

En la siguiente figura se puede observar detalladamente los componentes de una cámara IP.

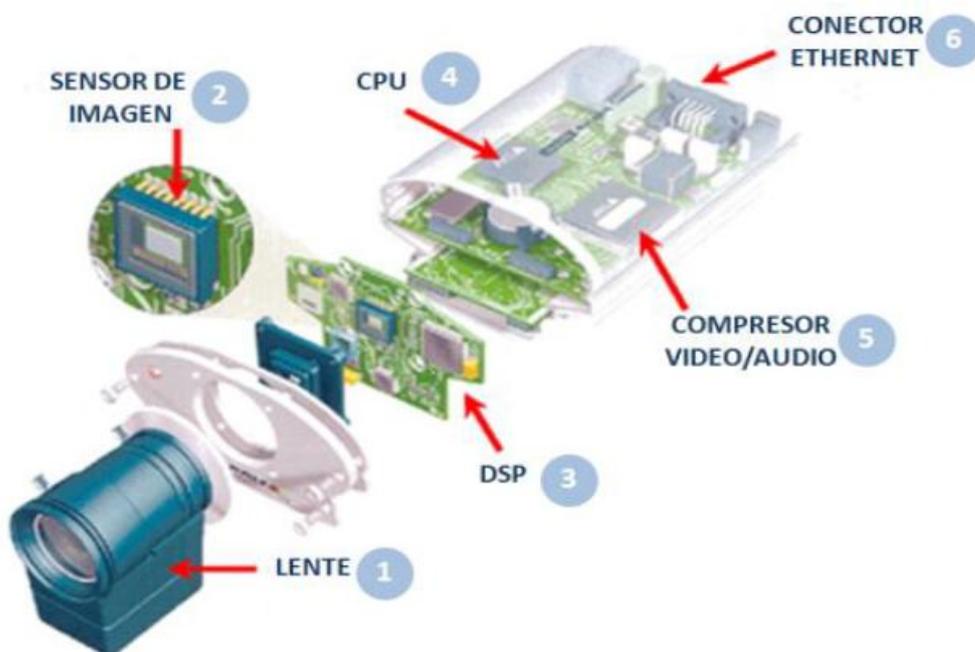


Figura 1-6: Componentes de una cámara IP

Fuente: S. Martí, 2013

- **Lente.-** En video vigilancia las lentes son los ojos de todo el sistema, además es un componente importante de la calidad de la imagen, los lentes pueden ser del tipo: **Fijo** solo tiene un campo de vista disponible por que la distancia focal es fija, **óptica variable** presenta diferentes campos de visibilidad por lo tanto una gama de longitudes focales, se puede ajustar el campo de visión manualmente y las distancias focales son de 3 a 8 milímetros y **zoom** su distancia focal es variable y si se cambia el campo de visión no se necesita volver a centrar la lente, en este tipo de lente la distancia focal puede ser de 6 a 48 milímetros. Las distancias focales grandes permiten visualizar un menor

campo de visión, pero con más detalles, mientras que distancias focales pequeñas permiten visualizar un mayor campo de visión, pero con menos detalles. (Chimborazo, 2015)

- **Sensor de imagen.**-Las cámaras digitales utilizan dos tipos de sensores los CCD (Charge Coupled Device) o CMOS (Complementary Metal Oxide Semiconductor) los cuales están formados en su esencia por semiconductores de metal-óxido (MOS) y están distribuidos en forma de matriz, tienen la función de acumular una carga eléctrica en cada una de las celdas de la matriz conocida como píxeles, la cantidad de luz que incide sobre cada píxel determina la cantidad de carga eléctrica, el tamaño del sensor se mide en diagonal puede ser 1/4", 1/3", 1/2" o 2/3". En el sensor CCD el amplificador es externo y común a todas las células fotoeléctricas mientras que en el sensor CMOS el amplificador está implícito en cada célula,
- **Procesador de imagen.** - Una vez que el sensor digitaliza la imagen este la envía al procesador de imagen para que la procese y envíe a la etapa de compresión, mediante este componente se puede mejorar la calidad de la imagen.
- **CPU.** - La cámara IP tiene un CPU que es un chip basado en Linux, el cual controla y administra las funciones de la cámara, además gestiona los procesos internos como la compresión, envío de imágenes o gestión de alarmas.
- **Etapa de compresión.** - Es una etapa importante para la transmisión de imágenes y videos a través de una red IP, con la finalidad de que la red no llegue a saturarse, entre los métodos de compresión tenemos: **MJPEG** cada fotograma es comprimido a JPEG, **MPEG-4** el primero en usarse en redes IP y también usado en dispositivos móviles y televisión. Y **H.264** este estándar ofrece mayor resolución de video que los dos anteriores, a la misma velocidad de bits y el mismo ancho de banda.
- **Tarjeta Ethernet.** - Ofrece conectividad de red para transmitir las imágenes captadas a través de la red IP. (Martí, 2013)

1.4.1.2. Características de una cámara IP

Para la elección de las cámaras IP es necesario conocer conceptos tales como:

- **Sensibilidad.** -Es la intensidad de luz que incide en una superficie, el valor de lux será menor a mayor sensibilidad y su unidad de medida es el LUX.

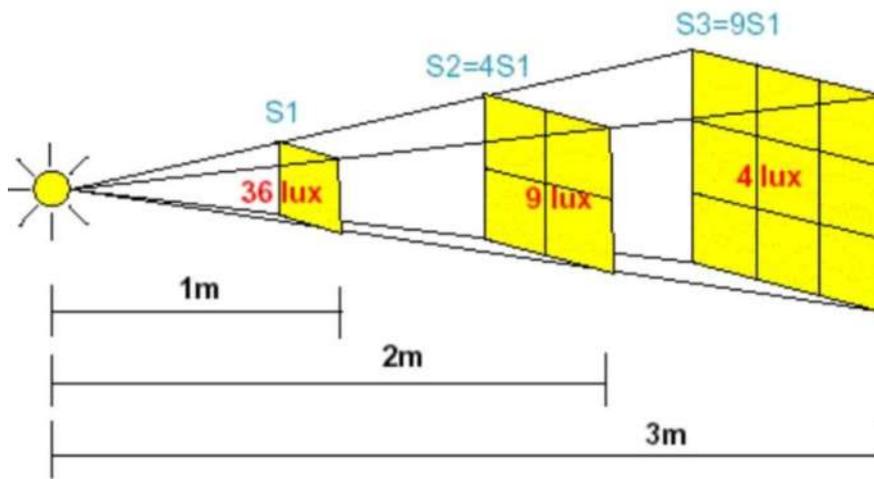


Figura 1-7: Sensibilidad de luz

Fuente: <http://labosigloxxi.blogspot.com/2010/10/ley-inversa-del-cuadrado-de-la.html>

- **Resolución.** - La resolución se mide por sus pixeles horizontales y verticales, a mayor número de pixeles tendrá mayor resolución.

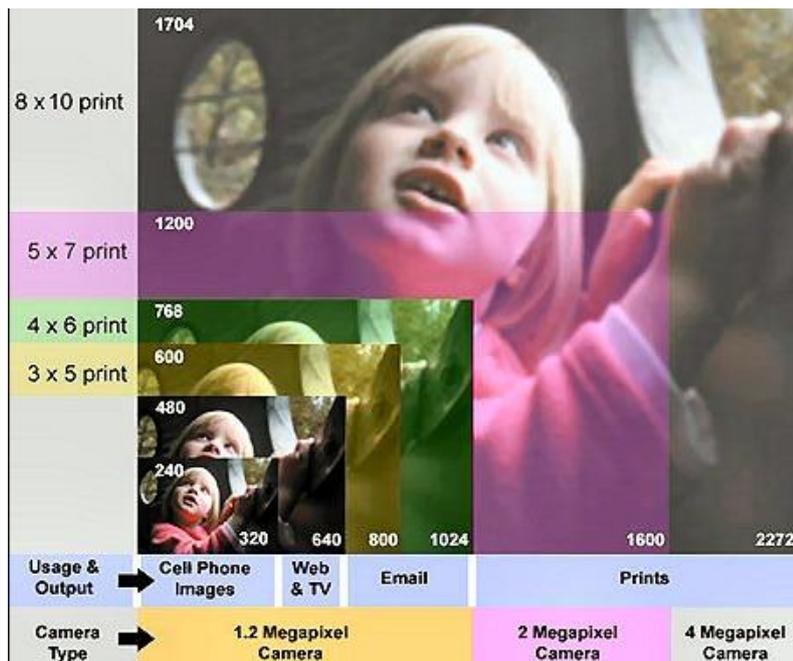


Figura 1-8: Resolución de una imagen

Fuente: <http://es.engadget.com/2007/07/18/especial-sobre-fotografia-y-video-megapixeles/>

- **Conmutación.** - En un sistema de video vigilancia IP las cámaras de día/noche disponen de un sistema para funcionar en color durante el día y conmutan a funcionamiento B/N durante la noche o con poca iluminación, para poder obtener mayor sensibilidad y resolución.

- **Compensación de contra luz (BLC).** - Su función es evitar que las partes de una imagen con poca luz se vean muy oscuras y las partes de mucha luz se vean muy claras.
- **Ajustes de blancos.** - Es muy necesario ya que las cámaras necesitan tener una referencia de cuales el color blanco para así tener una tonalidad correcta para el resto de los colores, entre los ajustes en blanco tenemos: **AWC** es automático y se ajusta solo al momento de la instalación y **ATW** seguimiento automático se hace en cada momento.
- **Control automático de ganancia.** - Se lo utiliza en cámaras que trabajan con bajo nivel de luz, es un circuito electrónico que mantiene la señal de video a un nivel constante.
- **Shutter.** - Permite aumentar la sensibilidad de la cámara y está presente en muchos sensores CCD de las cámaras. (Martí, 2013)

1.4.1.3. Tipos de cámaras IP

Para un sistema de video vigilancia tenemos varios tipos de cámaras IP que podemos utilizar, entre estas tenemos:

- **Cámara IP fija.** -Disponen de un campo de vista fijo y su ángulo también queda fijo una vez colocada, son una buena opción para aplicaciones en las que se desea que la cámara este bien visible, este tipo de cámaras pueden instalarse en carcasas diseñadas ya sea para usos interiores o exteriores.
- **Cámara IP domo fija.** - Este tipo de cámaras es también conocida como mini domo por su discreto diseño, debido a que es una cámara fija preinstalada en una pequeña carcasa domo. Esta cámara puede enfocar el punto seleccionado en cualquier dirección, una de sus ventajas es que es resistente a las manipulaciones. Pero no dispone de objetivos intercambiables y en el caso de disponer la selección de objetivos está limitado debido a su pequeño espacio dentro de la carcasa domo
Su diseño es a prueba de vandalismo y por esto tiene protección IP66, donde: IP es el índice de protección, 6 primer dígito tiene protección contra personas y entrada de polvo, 6 segundo dígito protección contra chorros de agua en cualquier dirección.
- **Cámara IP PTZ (Pan Tilt-Zoom).** - Su utilización está dirigida principalmente para espacios o áreas amplias, debido a que pueden moverse horizontal o verticalmente y disponen de zoom ajustable dentro de un área y puede ser ajustable de forma manual o automática.
- **Cámara IP domo PTZ.** - Este tipo de cámaras permiten cubrir áreas más amplias, permiten mayor flexibilidad en sus movimientos horizontal continuo de 360 grados,

vertical de 180 grados y zoom. Por su diseño resultan de gran ayuda para instalaciones discretas. Su función es de operación continua, ya que la cámara se mueve de una posición predefinida a la siguiente posición predefinida de forma automática, se pueden programar hasta 20 rondas de vigilancia. (Axis Communications, 2009) (García, 2010)



Figura 1-9: Tipos de cámaras IP

Fuente: SARABIA, Braulio. 2018

1.4.2. Cable UTP

También conocido como cable de par trenzado, está constituido de un forro plástico que en su interior se encuentran 8 pares de cables de cobre recubiertos de un material plástico de diferentes colores para diferenciarlos entre sí, básicamente son de dos en dos y en colores combinados como: blanco / azul - azul, blanco / verde – verde, blanco / café – café y blanco / naranja – naranja.

Este conjunto de cables permite la transmisión de información tanto de redes telefónicas y en redes de datos, la manera en la que se encuentran trenzados permite que la eliminación de interferencias electromagnéticas del ambiente y de otros cables que pueden compartir la misma trayectoria. (Informática Moderna, 2008)

1.4.2.1. Cable UTP categoría 5 y categoría 6

Los cables tanto de categoría 5 o 6 disponen de 4 pares de cables que se encuentran en un forro plástico y cada par de cables tienen un código de color con un cable que tiene un aislamiento de color sólido y el otro un aislamiento rayado con el mismo color.

Con la finalidad de reducir la interferencia los cables sólido y rayado del mismo color van trenzados y las vueltas tienden a anular las perturbaciones externas que son las mismas en los dos cables. (Markgraf, 2014)

1.4.2.2. Diferencias

Los cables categoría 6 son nominalmente más gruesos que los cables categoría 5, este cable categoría 6 por su grosor y por las mejoras de torsión ofrece menos pérdidas de inserción, mejor rendimiento de diafonía y una mejor señal al ruido que el cable categoría 5. (Jie, 2014)

1.4.2.3. Interferencia

Los cables de red a más de ser capaces de transmitir datos a alta velocidad, dichos cables deben tener una alta resistencia a las interferencias externas, como ondas electromagnéticas producidas por los microondas, teléfonos, impresoras u otros dispositivos ya que esta interferencia distorsiona la señal que se transmite provocando así los errores. El cable categoría 6 utiliza un mejor aislamiento y más vueltas y por tal razón presenta menor interferencia. (Markgraf, 2014)

1.4.2.4. Velocidad

La velocidad de transmisión depende del tipo y categoría de cable que se está utilizando. El cable categoría 5 presenta una frecuencia de 100 MHz y una velocidad de hasta 100 Mbps y es utilizado para redes Ethernet. El cable categoría 6 presenta una frecuencia de 250 MHz y una velocidad de hasta 1000 Mbps. (Markgraf, 2014)

1.4.3. Codificador de video

En los sistemas de video vigilancia un codificador de video permite migrar un sistema de cctv analógico a un sistema de video en red, de este modo no se pierde la infraestructura montada de un cctv analógico. Una vez realizado este procedimiento, el codificador de video se conecta a la cámara analógica por medio de un cable coaxial para luego convertir la señal analógica en

secuencias de video digitales y así enviarlas a través de una red basada en IP (LAN, WAN o internet).



Figura 1-10: Codificador de video
Fuente: Axis Communications. 2009

Con la introducción de este codificador de video ya no es necesario el NVR o VCR, ya que para grabar y visualizar el video digital se necesita un PC, además se puede acceder remotamente y controlar cualquier cámara de video analógica a través de una red IP. Entre sus ventajas están la gestión de eventos y la función de video inteligente. (Axis Communications. 2009)

1.4.4. Grabación y almacenamiento

En un sistema de video vigilancia la grabación y el almacenamiento es una parte importante debido a la información que se maneja.

Existen varios tipos de almacenamiento entre los más importantes tenemos:

- **Almacenamiento interno en la cámara.** -Una cámara IP tienen una memoria interna (tarjeta SD o memoria USB) la cual permite grabar por un determinado tiempo.
- **Almacenamiento en la PC.** - Este tipo de almacenamiento es para sistemas pequeños, debido a que la grabación se guarda en el disco duro de la PC.
- **Almacenamiento en NVR (Network Video Recorder).** - Principalmente realizado para instalaciones profesionales, debido a que es un grabador de video en red, el cual es parecido a un disco duro, pero con mayor resistencia. Para visualizar las grabaciones se puede conectar al NVR un monitor y con un teclado se puede controlar el movimiento o zoom desde el grabador. Además, el NVR puede conectarse a cualquier parte de la LAN y para poder tener conexión a internet requiere una IP fija. (Martí, 2013)

Así como el almacenamiento, la grabación también tiene su nivel de importancia ya que entre sus funciones están el control de la monitorización o zoom de las cámaras, obtener copias de las grabaciones, conexión a internet y el control remoto de todas las funciones.

Las imágenes pueden ser grabadas en diferentes formas y se configura según las necesidades del usuario:

- **Grabación continua.** -La grabación es en todo momento.
- **Grabación programada.** - La grabación es por periodos según sean programados.
- **Grabación por eventos.** - La grabación empieza cuando detecta algún movimiento.
- **Grabación por eventos y por tiempo.** - La grabación empieza cuando hay movimiento, pero en un tiempo programado. (Martí, 2013)

La capacidad de almacenamiento del grabador está dada por: el número de canales (cámaras) de la instalación, resolución (píxeles), número de frames por segundo (fps), método y factor de compresión, tiempo total de grabación (días) y el porcentaje de alarma (%) que es el total del tiempo que está grabando. (Martí, 2013)

1.4.5. Software de gestión de video

En todo sistema de video vigilancia es de suma importancia tener instalado un software específico el cual permite la gestión, monitorización, gestión de eventos y configuración de dispositivos, este software viene incorporado en el NVR y se lo instala en la PC del usuario autorizado, de ser el caso que no tenga incorporado este software va: **embebido** en los mismos elementos de la red y para acceder solo tenemos que ingresar la dirección IP del dispositivo, solo se lo utiliza en sistemas con pocas cámaras, **instalado en la PC** el cual controla, gestiona y graba las imágenes. (Martí, 2013)

Entre sus funcionalidades están:

- Grabación de video
- Reproducción de video en directo
- Reproducción y grabación de audio
- Gestión de eventos
- Configuración de parámetros de las cámaras
- Funciones de búsqueda de videos
- Control de acceso de usuarios
- Mapeo de cámaras. (Martí, 2013)

1.5. Audio

Una parte muy importante en un sistema de video vigilancia es el audio, ya que permitiría aclarar de forma más eficiente u justa un acto ilícito, pero aún no se ha extendido en el campo de la videovigilancia. A más del campo de visión de la cámara, el audio permite ampliar su cobertura debido a su capacidad que permite cubrir un área de 360 grados. (Axis Communications. 2009)

1.5.1. Modos de audio

- **Simplex.** -El audio solo se envía en una dirección
- **Semiduplex.** - El audio se envía en ambas direcciones, uno a la vez.
- **Full dúplex.** - El audio se envía a y desde el operador simultáneamente. (Axis Communications. 2009)

1.5.2. Compresión de audio

Con la finalidad de tener una transmisión y almacenamiento efectivo, las señales analógicas deben convertirse a audio digital mediante un proceso de muestreo luego deben comprimirse para reducir el tamaño. (Axis Communications. 2009)

- **Frecuencia de muestreo.** - Es el número de muestras por segundo de una señal de audio analógica y se mide en hercios (HZ). Mientras más alta es la frecuencia de muestreo mejor será la calidad de audio.
- **Frecuencia de bits.** - Determina el nivel de compresión, mientras más alto sea el nivel de compresión más baja será la calidad del audio.
- **Códecs de audio.** - Permite mejorar la calidad del audio. (Axis Communications. 2009)

1.6. Video

En los sistemas de video vigilancia los videos que son grabados pueden contener información que no sea de utilidad y que necesita ser eliminada para eso se utiliza la compresión de video.

1.6.1. Compresión de video

Consiste en eliminar datos de la información que son de importancia, con la finalidad de reducir el tamaño del video, pero sin afectar la calidad de la imagen y así poderlo enviar a través de la red y poder almacenarlos. (Axis Communications. 2009)

1.6.2. Estándares de compresión

Entre los estándares de compresión más utilizados tenemos:

- **Motion JPEG.** -Consta de una secuencia de video digital compuesta por una serie de imágenes JPEG individuales, su ventaja es que utiliza imágenes fijas.
- **MPEG-4.**- Es compatible con aplicaciones que tienen un ancho de banda reducido y requieren imágenes de alta calidad.
- **H.264.**- Este estándar puede reducir el tamaño de un archivo de video digital más del 80%. (Axis Communications. 2009) (Chimborazo. 2015)

1.7. Sincronización de audio y video

Esta sincronización se realiza mediante un reproductor multimedia, a través de una red se envían el audio y el video como paquetes individuales, con la finalidad de que el usuario o cliente puede reproducir perfectamente sincronizados tanto el video y el audio. Los formatos que más se utiliza son MPEG-4 o H.264, ya que las transmisiones de audio y video se envían por medio del protocolo RTP (Red Time Protocol) que es un protocolo de transporte en tiempo real y que introduce un código de tiempo en los paquetes de audio y video. (Axis Communications. 2009)

1.8. Red inalámbrica

1.8.1. Que es una red inalámbrica

Es una red en la que distintos dispositivos pueden comunicarse o compartir información sin la necesidad de tener una conexión cableada. Una de las ventajas más notables de las redes inalámbricas es permitir que un usuario se mantenga conectado a la red cuando se desplaza dentro de un área determinada

Una red inalámbrica no utiliza un cableado estándar, ya que se basa en un enlace el cual utiliza ondas electromagnéticas (infrarrojo y radio), las redes se diferencian ya sea por la frecuencia de transmisión, su velocidad y alcance. (CCM. 2017) (Informática Moderna. 2008)

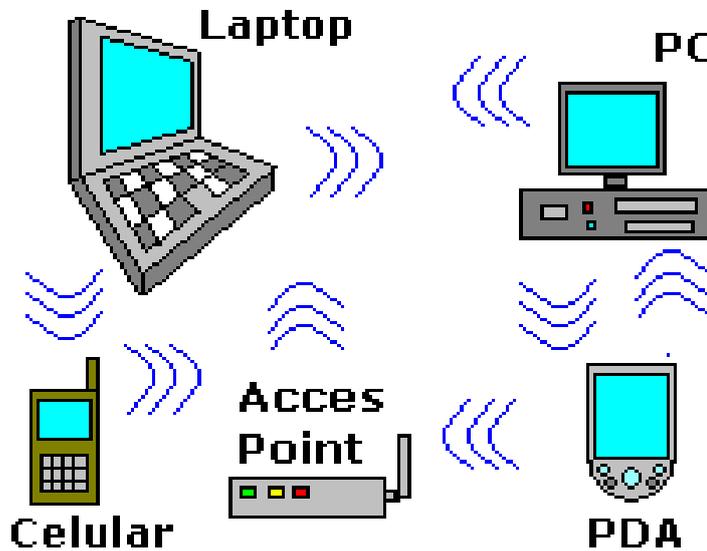


Figura 1-11: Red Inalámbrica
Fuente: InformáticaModerna.2016

1.8.1.1. Tipos de redes inalámbricas

Dependiendo del área geográfica que el usuario se conecta a la red, el cual se denomina área de cobertura. Se clasifican en varias categorías que son:

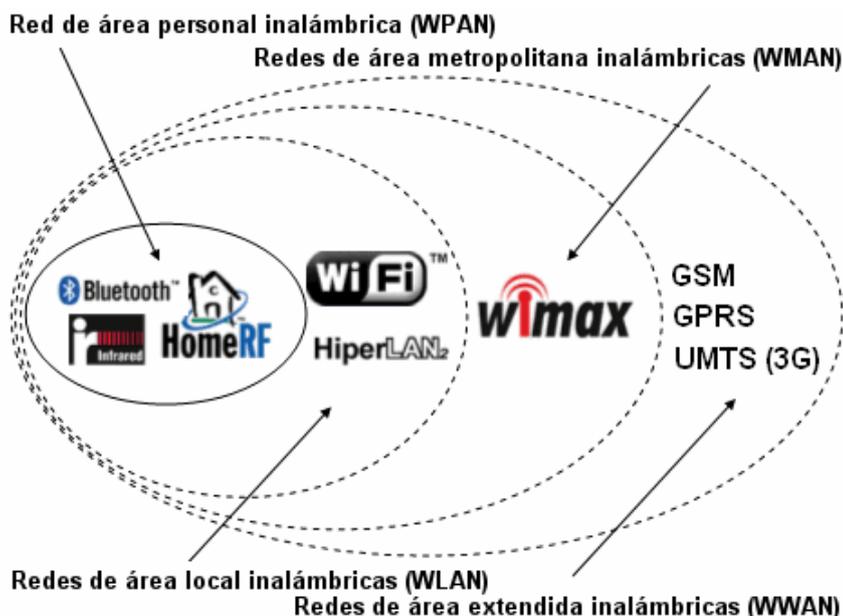


Figura 1-12: Tipos de redes inalámbricas
Fuente: Ccm.2017

- **Redes de área personal (WPAN).** -Son redes de corto alcance, abarcan un área de algunas decenas de metros.
- **Redes de área local (WLAN).** - Estas redes son equivalentes a un área de una red local de una empresa, con alcance aproximadamente de 100 metros.
- **Redes de área metropolitana (WMAN).** - Conocida también como bucle local inalámbrico basadas en el estándar 802.16, su velocidad es de 1 a 10 Mbps con un alcance de 4 a 10 kilómetros.
- **Redes de área extensa (WWAN).** - Su alcance es el más amplio de todas las redes inalámbricas, los teléfonos móviles están conectados a una red de área extensa. (Ccm. 2017)

1.8.2. Tecnologías de una red inalámbrica

Entre las tecnologías actuales para red inalámbrica tenemos:

1.8.2.1. WI-FI (“Wireless Fidelity”)

Sus siglas significan fidelidad sin cables, también conocida como red de área local en la que su transmisión inalámbrica es por medio de ondas de radio con buena calidad de emisión para distancias cortas hasta de 100m, dicha transmisión esta estandarizado por la IEEE. Para su transmisión se necesitan antenas integradas en las tarjetas, el emisor y el receptor no necesariamente deben estar frente a frente ya que estas ondas traspasan obstáculos. (Informática Moderna. 2008)

Entre los estándares principales tenemos:

- **IEEE 802.11b.**- Solo trabaja en la banda de frecuencia de 2.4 GHz compatible con velocidades menores, su velocidad de transmisión es de 11 Mbps.
- **IEEE 802.11g.**- Solo trabaja en la banda de frecuencia de 2.4 GHz y su velocidad de transmisión es de 11, 22 y 54 Mbps.
- **IEEE 802.11n.**- Trabaja en la banda de frecuencia de 2.4 y 5 GHz, su velocidad de transmisión es de 300 Mbps.
- **IEEE 802.11ac.** – Solo trabaja en la banda de frecuencia de 2.5 a 5 GHz, su velocidad de transmisión es de 433 Mbps y 1.3 Gbps. (Informática Moderna. 2008)

1.8.2.2. Infrarrojo

Su transmisión es por medio de ondas de calor a corta distancia hasta 1m y pueden traspasar cristales. No utiliza ningún tipo de antena más bien usa un diodo emisor, debido a esto funciona en línea recta donde el emisor debe estar frente al receptor ya que no traspasa obstáculos.

1.8.2.3. Bluetooth

El método de transmisión es por medio de ondas de radio de corto alcance de 1, 20 y 100 m a la redonda, no necesitan el uso de antenas externas visibles y su velocidad de transmisión es de hasta 1 Mbps.

1.8.2.4. Microondas

Este tipo de transmisión es a gran escala, suelen ser muy costosas. Existen dos tipos satelitales y terrestres.

1.8.2.5. Laser

Estas son tecnologías de muy alta velocidad, su transmisión es por medio de un haz de luz láser emitida por un diodo especial. (Informática Moderna. 2008)

1.8.3. Arquitectura de una red inalámbrica

Según las necesidades del usuario las arquitecturas de las redes pueden ser de diferentes formas, siempre y cuando cumplan con los requerimientos y así poder tener una buena funcionalidad del sistema.

1.8.3.1. Diseño de una red inalámbrica

Las redes pueden ser de forma:

- **Red punto a punto.** -La información se transmite de un punto a otro y usa antenas direccionales para así proporcionar el ancho de banda más alto para el enlace, debido a esto se tiene un alto nivel de seguridad y puede ser ajustable para un mínimo de interferencia.

- **Red punto a multipunto.** -Su información se envía de un punto a varios receptores, utiliza una antena omnidireccional.
- **Red mesh.** -Este tipo de redes se caracterizan ya que varios nodos conectados proporcionan rutas de conexión redundantes e individuales, usa protocolos de enrutamiento especiales para asegurar su transmisión. (Chimborazo. 2015)

1.8.3.2. Redes con tecnología 802.11

Basados en el estándar 802.11 tenemos diferentes formas de red como son:

- **Red ad- hoc.** - Similar a como opera Wifi y debe ser seleccionado como el modo de funcionamiento de la interfaz WLAN, su cobertura entre edificios es de 30 a 50 m y al aire libre hasta 300m
- **Red de infraestructura.** - Por su cobertura que es un área grande utiliza varios puntos de acceso. El movimiento de los usuarios entre celdas inalámbricas se conoce como hand off, en esta red los puntos de accesos se identifican como SSID (Service Set Identifier) y se configura en cada punto de acceso.
- **Frecuencias.** - Una red WLAN opera en el rango de 2.4 o 5 GHz, una desventaja es que en el rango de 2.4 también operan otras tecnologías y en el rango de 5 se necesitan más puntos de acceso. (Chimborazo. 2015)

1.8.4. Espectros inalámbricos

En las redes la comunicación inalámbrica se realiza a diferentes frecuencias de radio que se conoce también como espectro y se mide en hercios (Hz) que es una unidad para ciclos electromagnéticos por segundo, debido a esto se puede realizar una llamada y escuchar la radio al mismo tiempo. (Chimborazo. 2015)

1.8.5. Intensidad de la señal

En los sistemas inalámbricos tenemos muchas maneras para poder medir la intensidad de la señal. Una de las formas es mediante el estándar definido por IEEE 802.11, mediante este estándar la energía es valorada con los circuitos instalados en una tarjeta de red inalámbrica(NIC), este valor numérico es entero y con un rango entre 0 y 255 (valor de 1 byte) llamado RSSI que es el indicador de la intensidad de la señal. (Chimborazo. 2015)

1.8.6. Antenas

En los sistemas inalámbricos las antenas son muy importantes, pueden ser **omnidireccionales** que recepta las ondas electromagnéticas en todas las direcciones y se las utiliza en redes multipunto ya que tienen un área amplia, **direccional** la cual centra las ondas electromagnéticas en una sola dirección así la señal llega a mayor distancia y se las utiliza en aplicaciones punto a punto. (Chimborazo. 2015)

1.8.7. Protocolo IP

Tanto el usuario como la persona que realiza la instalación del sistema de video vigilancia deben conocer que hay una serie de tecnologías de redes se inicia automáticamente y así asegurar que el portátil obtenga una dirección IP con la finalidad de que pueda comunicarse de forma segura a través de una red.

Este protocolo de internet IP se encuentra en la capa 3 del modelo OSI y en la capa 2 del modelo TCP/IP. Un ISP (proveedor de servicios de internet) puede asignar una dirección IP dinámica o estática. IP es quien ofrece una conexión el cual divide los datos en datagramas IP antes de que se transmita, esto quiere decir que IP no garantiza ni la llegada ni la secuencia del datagrama IP ya que funciona sobre una base sin conexión y se dirigen a un destinatario en formas diferentes y por eso se usa los protocolos de la capa de transporte del modelo OSI o TCP/IP. (Chimborazo. 2015)

1.8.7.1. Modelo de referencia OSI

La Organización Internacional para la Estandarización (ISO) fue quien diseño el modelo de referencia (OSI) que utiliza capas estructuradas para las actividades de la red y consta de 7 capas.

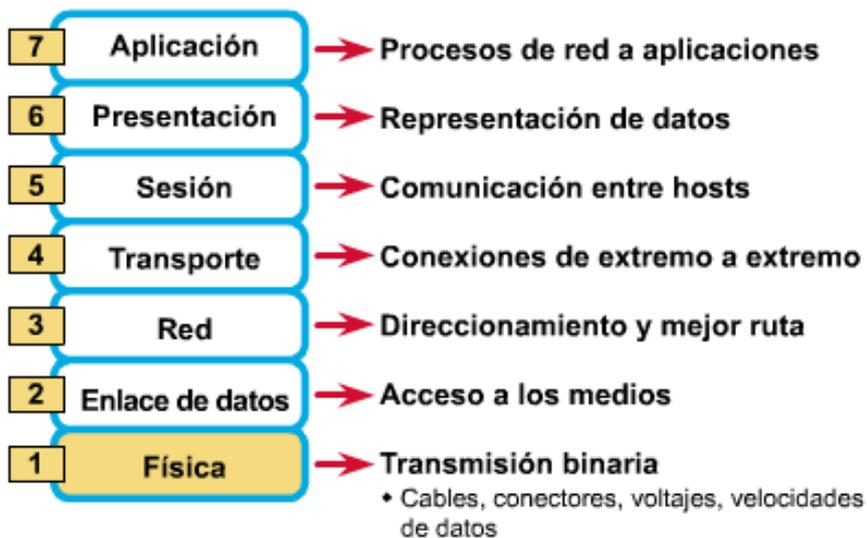


Figura 1-13: Capas del modelo OSI
Fuente: Txdatos.2011

- **Capa Física.** - Define las características del canal y se ocupa de la transmisión de bits a través de un canal de comunicación.
- **Capa de Enlace de datos.** - Ensambla los bits de la capa física en grupos de tramas y así asegura su envío, además verifica y corrige los errores de la capa física.
- **Capa de Red.** - Se asegura que los paquetes lleguen desde su punto de inicio hasta su punto final.
- **Capa de Transporte.** - Esta capa es la encargada de que el mensaje completo llegue a su destino.
- **Capa de Sesión.** - Esta capa establece, mantiene y sincroniza la interacción entre los sistemas y es controladora de diálogos en la red.
- **Capa de Presentación.** - Es la encargada de la sintaxis y la semántica de la información intercambiada entre dos sistemas.
- **Capa de Aplicación.** - Permite a los usuarios acceder a la red. (Txdatos. 2011)

1.8.7.2. Modelo de referencia TCP/IP

Este modelo de referencia TCP/IP junto a la pila del protocolo TCP/IP permiten la comunicación entre dos computadoras de cualquier parte del mundo a casi la velocidad de la luz y consta de 4 capas.

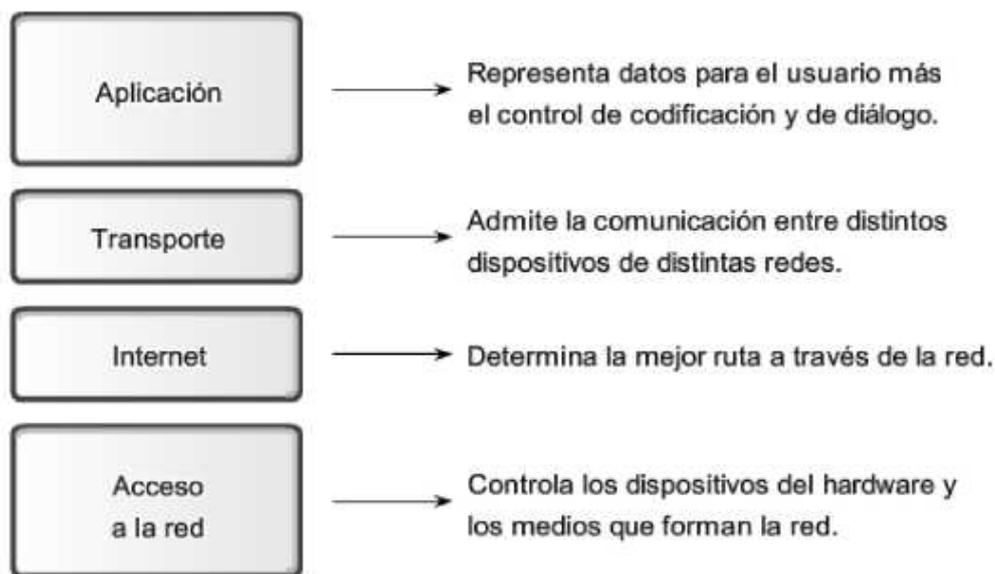


Figura 1-14: Capas del modelo TCP/IP
Fuente: Txdatos.2011

- **Capa de Aplicación.** -Garantiza que los datos estén correctamente empaquetados para su envío a la próxima capa.
- **Capa de Transporte.** - Tiene presente localidad de servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores.
- **Capa de Internet.** - Su propósito es enviar paquetes desde el origen a cualquier parte de la red y que lleguen a su destino sin importar la ruta que eligieron para llegar ahí.
- **Capa de Acceso a la red.** - Se encarga de realizar un enlace físico y luego realizar otro enlace físico. (Txdatos. 2011)

1.8.7.3. Direccionamiento IP

Con este direccionamiento IP podemos identificar en la red un dispositivo, ya que todo dispositivo tiene un único número IP. Una dirección IP consta de 4 números de hasta 3 cifras (192.168.0.15) que están separadas por un punto y varían entre 0 y 255.

Las direcciones IP se clasifican en:

- **Direcciones IP públicas.** - Este tipo de direcciones son las que ofrece el proveedor de acceso a internet y es asignada a cualquier dispositivo que este directamente conectado a internet, pueden ser visibles desde cualquier punto de internet.
- **Direcciones IP privadas.** - Este tipo de direcciones deben ser únicas para cada dispositivo, y pueden ser repetidas siempre y cuando estén en redes diferentes.

Las direcciones IP pueden ser del tipo:

- **Dirección IP Dinámica.-** Estas direcciones son asignadas por medio de DHCP (Dynamic Host Configuration Protocol) la cual tiene una dirección máxima determinada, debido a que un dispositivo que se conecta cada vez a internet tiene un número de dirección diferente.
- **Dirección IP fija o Estática. -** Son asignadas de manera manual por el usuario o por el servidor de la red y siempre van a tener el mismo número.

1.8.7.4. Dirección IPv4

Este tipo de direcciones se expresan por un número binario de 32 bits o que es lo mismo 4 bytes, tienen un número limitado de direcciones únicas (4 294 967 296). (Chimborazo. 2015)

1.8.7.5. Subredes

Mediante la creación de subredes se puede dividir el espacio de direcciones, según sean las necesidades del usuario o a su vez según la agrupación de las cámaras, en este caso se crearía una subred para cada grupo. Si tenemos la dirección 192.168.1.50 con una máscara 255.255.255.0 donde los 2 primeros octetos indican la red y el 3 octeto indica la subred, es importante conocer que al igual que las redes debemos excluir 2 direcciones de cada subred para su identificación. (Chimborazo. 2015)

1.8.7.6. VLANs

Es una red local virtual o LAN virtual es una red de área local en la cual se pueden agrupar un conjunto de equipos de manera lógica. Debido a estas redes virtuales podemos liberar la arquitectura física ya que se define una segmentación lógica basada en el agrupamiento de equipos. (Ccm. 2017)

1.8.8. Seguridad

Dentro del campo de la video vigilancia la seguridad es un término de suma importancia, debido a la información que se maneja y más aún ya que los usuarios necesitan tener confidencialidad de la información tanto que se envía o recibe que es grabada por medio de su sistema y es necesario protegerla. En el tema de seguridad un tipo de seguridad y el más conocido son por medio de autenticación de usuario y contraseña.

1.8.9. Autenticación

El método para mantener segura nuestra información o datos en una red IP se utiliza la autenticación por medio de usuario y contraseña. En este método se realizará la autenticación y autorización, esto quiere decir que el usuario deberá identificarse en la red y en el extremo remoto mediante un nombre de usuario y una contraseña, estos datos serán verificados antes de que se le permita ingresar al sistema. También se puede añadir de seguridad adicional cifrando los datos para evitar que otros usuarios ingresen al sistema de seguridad.

Mediante este sistema evitamos que personas inescrupulosas manipulen la información que se encuentra en la red.

CAPITULO II

2. MARCO METODOLOGICO

2.1. Descripción del marco legal

La ESPOCH y todas sus Facultades, por el mero hecho de ser una institución pública a la que asisten infinidad de personas necesitan el mejor sistema de videovigilancia. Pero se debe conocer el marco legal para saber si se puede o no instalar un sistema de seguridad, con la finalidad de no incurrir con los estatutos de la ley.

2.1.1. *Ley de Seguridad Pública y del Estado*

La Ley de Seguridad Publica y del Estado nace con la finalidad de garantizar el orden, la convivencia y establecer e implementar políticas, planes, estrategias y acciones que garanticen la integridad y seguridad de todas personas evitando así actos ilícitos que van en contra de su seguridad, todo esto encaminando al buen vivir. (Justia Ecuador, 2018)

2.1.2. *Norma ISO/IEC 27001*

Esta Norma tienen como finalidad mantener la seguridad de la información, debido a que las empresas, negocios e instituciones públicos cada vez presentan más riesgos e inseguridades que pueden llegar a dañar de forma permanente su sistema de información, logrando así poner en peligro la continuidad de sus actividades. (Aenor Ecuador, 2016)

La seguridad de la información permite garantizar su confidencialidad, integridad y disponibilidad, evitando así que pueda caer en manos inescrupulosas y se utilice de manera incorrecta

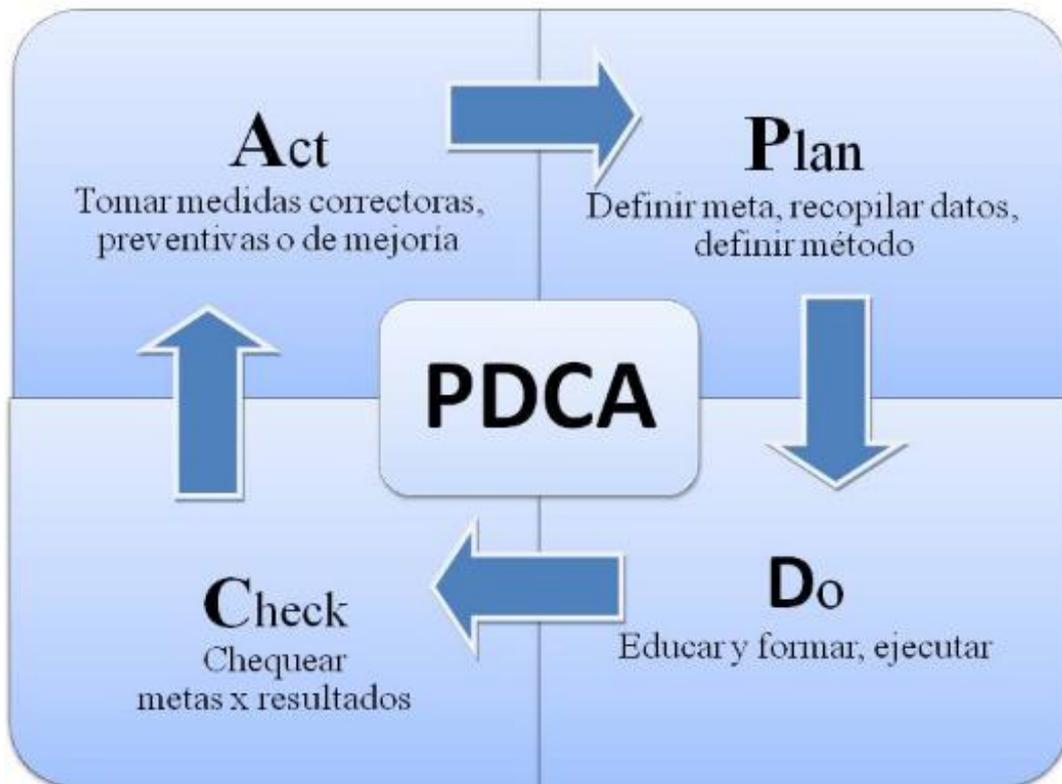


Figura 2-1: Ciclo de Demming
Fuente: Aenor Ecuador.2016

Esta es una norma estándar en la que especifica cuáles son los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI (Sistema de Gestión de Seguridad de la Información). Todo esto según el “Ciclo de Demming” y puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. (Aenor Ecuador. 2016)

Este ciclo PDCA es una ayuda que brinda al momento de implementar un sistema de seguridad, se trata de seguir pasos desde el momento de su diseño hasta la parte de finalización, con pasos que son necesarios y que ayudaran al momento de presentarse algún problema, este problema se podría solucionar en cada etapa de este ciclo.

2.1.2.1. Ciclo PDCA para el sistema de videovigilancia inalámbrico

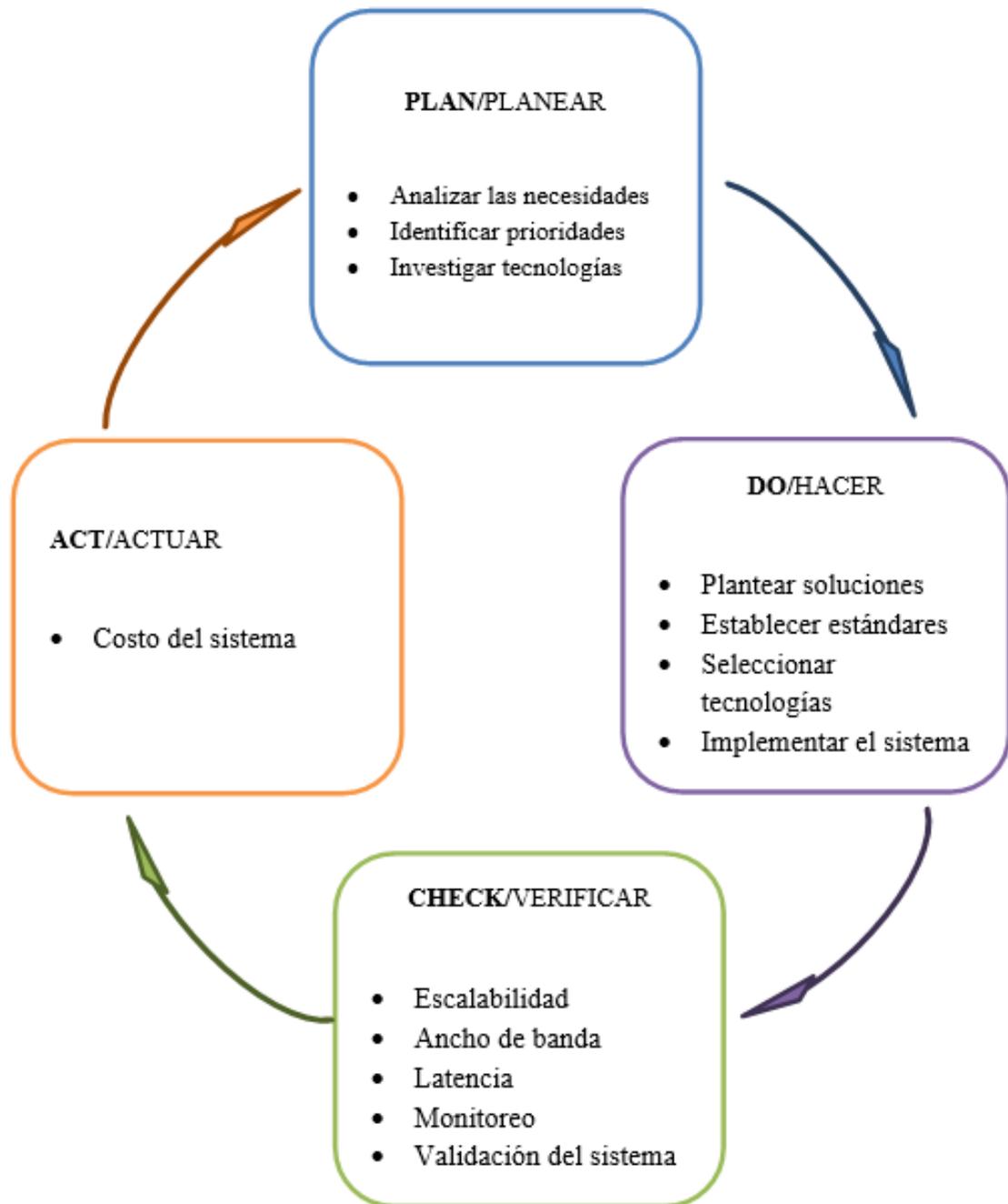


Figura 2-2: Ciclo PDCA de la norma ISO/IEC 27001 aplicada al presente trabajo
Fuente: SARABIA, Braulio.2018

2.2. Estudio de la situación actual de la FIE

A continuación, se expone la situación actual de la Facultad de Informática y Electrónica, de la Escuela Superior Politécnica de Chimborazo de la ciudad de Riobamba analizando aspectos como; número de estudiantes, aulas, oficinas, laboratorios, baterías sanitarias y tipo de comercios que existen en la zona. Para la justificación de la implementación del sistema de seguridad mediante videovigilancia inalámbrico, es necesario comprender cuál es el nivel de inseguridad actual en la FIE.

Considerando este escenario, se realizó este trabajo de titulación en el que se diseñó e implementó un sistema de seguridad mediante videovigilancia inalámbrica usando cámaras IP, para entornos en interiores como exteriores según sean las necesidades de la Facultad, con lo cual se busca fortalecer y aumentar el nivel de seguridad dentro y fuera de la Facultad.

Este proyecto garantizará la seguridad de las personas y de sus bienes, ya que mediante la instalación de este sistema de videovigilancia se podrá reducir el nivel de inseguridad, puesto que las grabaciones que se transmiten mediante son en tiempo real y gracias a esto se evitará robos o atracos manteniendo la seguridad de las personas.

2.2.1. Descripción de la infraestructura de la FIE

La Escuela Superior Politécnica de Chimborazo posee dos zonas edificadas que corresponden a la Facultad de Informática y Electrónica, estas dos infraestructuras diferenciadas se encuentran separadas por una cancha de deporte que es utilizada por los estudiantes. La primera infraestructura conocida como edificio antiguo ya posee cámaras de seguridad que mantienen dicha infraestructura en constante vigilancia.

La segunda infraestructura conocida como edificio nuevo de la FIE, dicha infraestructura no cuenta con un sistema de seguridad, razón por la cual se propuso este tema de titulación. La FIE es un edificio que consta de una planta baja y dos pisos, un ascensor y un espacio a su derecha que sirve para el estacionamiento vehicular.



Figura 2-3: Vista frontal del edificio de la FIE
Fuente: SARABIA, Braulio.2018



Figura 2-4: Vista interior del edificio de la FIE
Fuente: SARABIA, Braulio.2018

La Planta baja está constituido por:

- Dirección de la Escuela de Electrónica en Telecomunicaciones y Redes
- Dirección de la Escuela de Electrónica en Control y Redes Industriales
- Auditorio de la Facultad
- Laboratorios y aulas
- Batería sanitaria

El primer piso está constituido por:

- Decanato
- Sala de profesores
- Laboratorios y aulas
- Batería sanitaria para docentes

El segundo piso está constituido por:

- Vicedecanato
- Dirección de la Escuela de Ingeniería en Sistemas
- Dirección de la Escuela de Diseño Grafico
- Laboratorios y aulas
- Sala de profesores

2.3. Sistema de videovigilancia inalámbrico propuesto para la FIE

Con todo lo estudiando anteriormente y con la finalidad de mantener un alto nivel de seguridad en la FIE, se implemento un sistema de videovigilancia inalámbrico utilizando cámaras IP, el mismo que será beneficioso para los estudiantes, docentes y personas que de una u otra forma visitan la facultad.

2.3.1. Requerimientos del sistema de videovigilancia

Este sistema de video vigilancia inalámbrico será de alta definición, debido a su importancia en la visualización de las imágenes que deben ser claras y con buena resolución. El medio de transmisión para este sistema será inalámbrico, las cámaras serán digitales IP y gracias a esto el sistema podrá ser monitoreado de manera remota.

Los dispositivos principales, como la sala de monitoreo estarán ubicado en el tercer piso del edificio de la FIE que actualmente funciona como sala de servidores, otro dispositivo que será ubicado en esta parte es el dispositivo que permite la visualización en tiempo real y su respectivo almacenamiento.

Para la instalación/ubicación de las cámaras de este sistema, serán distribuidas y ubicadas en lugares estratégicos donde sea necesaria la visualización de dicha área, hay que tener muy en

cuenta los lugares donde se ubicaran las cámaras ya que no deberá existir puntos ciegos en el transcurso del movimiento de las personas desde la planta baja hasta el tercer piso y en sentido contrario, con la finalidad de que las cámaras no pierdan de vista a la persona.

2.3.2. Elección de las tecnologías para el sistema de video vigilancia

Un sistema de video vigilancia inalámbrico debe satisfacer las necesidades que los usuarios requieren, como tener buena calidad y resolución de las imágenes para esto la adquisición de los equipos será con la mejor tecnología y así podemos garantizar un buen funcionamiento del sistema.

2.3.2.1. Selección del medio de transmisión

A partir del estudio que se realizó de las redes inalámbricas y con la finalidad de aprovechar las redes existentes se puede concluir que el medio de transmisión y visualización remota más óptimo es el medio no guiado **WIFI**.

Un medio no guiado sin cables ha tenido gran acogida ya que es un medio de transmisión que abarcan grandes áreas y en cualquier dirección. Este medio se basa en la transmisión de ondas electromagnéticas (señales) que se propagan libremente a través de este medio, entre los más importantes se encuentran el aire y el vacío. Este tipo de comunicación inalámbrica también llamada WLAN o estándar IEEE 802.11 es la más utilizada en estos tiempos. En la actualidad encontramos dos tipos de comunicación **WIFI** basados en este estándar.

- 802.11b con velocidades de 11Mbps
- 802.11g con velocidades de 54 Mbps

Debido a que es una comunicación inalámbrica, no está a salvo de que personas inescrupulosas intercepten nuestra comunicación y tengan acceso a la información, por eso es de suma importancia la encriptación de la transmisión y así tener un entorno seguro y confiable.

2.3.2.2. Selección de las cámaras IP

Para la selección de las cámaras es necesario tener muy en cuenta parámetros tales como: lugar donde se van a ubicar las cámaras. Es un punto muy importante debido al lugar ya sea interior o exterior por el mero hecho de la iluminación tanto en el día o en la noche.

Las cámaras IP de tipo **Fija Bullet** (bala) son las más acordes para exteriores debido a su diseño y especificaciones, y tipo **Domo de lente fijo** son las más acordes para interiores debido a su diseño y sus especificaciones.

Como es un sistema inalámbrico y las cámaras serán parte de la red, deben contar con funciones tales como:

- **Alimentación PoE.** - También conocida como alimentación a través de Ethernet, permite que las cámaras reciban alimentación por medio del mismo cable que está conectado a la red.
- **Funciones y Seguridad Avanzadas.** - Tales como DHCP para administrar la dirección IP cifrada con HTTPS para una comunicación segura, y también funciones para autenticación. (Chimborazo. 2015)

2.3.2.3. Selección del medio de monitoreo y almacenamiento

Para poder visualizar se utilizó monitores de alta tecnología, pero con la ayuda de un NVR y gracias a sus funcionalidades podemos realizar la visualización y el almacenamiento de todo el sistema.

El NVR que se va a adquirir es de 8 canales y con funcionalidades de alimentación PoE, con la finalidad de que las cámaras puedan alimentarse a través de este medio.

2.4. Interferencia en las redes inalámbricas existentes en el edificio de la FIE

Uno de los principales problemas con los que nos encontramos con las redes inalámbricas son las interferencias. Este sistema de seguridad tendrá un control de acceso remoto y con la finalidad de obtener una visualización en tiempo real y sin mucho retraso en las imágenes se realizó un análisis de interferencias de las redes.

Generalmente la interferencia inalámbrica es producida o proviene de tres fuentes que son:

- Paredes y suelos que bloquean las señales inalámbricas
- Otras redes que operan en la misma banda ya sea de 2.4 o 5 GHz.
- Aparatos electrónicos que operan en la misma de frecuencia.

Las interferencias provocan que se pierdan paquetes IP provocando reenvíos continuos de datos, debido a esto la conexión se vuelve lenta y en ocasiones se corta, y luego de un tiempo se vuelve a conectar. En el caso de utilizar protocolo 802.11n esta interferencia causa grandes problemas, porque su función se basa en el envío de múltiples ondas de radio en un punto de acceso con la finalidad de conseguir mayor velocidad y cuando una es interferida el funcionamiento de las restantes ya no es el mismo.

2.4.1. *Análisis de las redes inalámbricas existentes en el edificio*

Para el análisis de la interferencia producida por cada una de las redes inalámbricas, se utilizará el **Software Acrylic**.

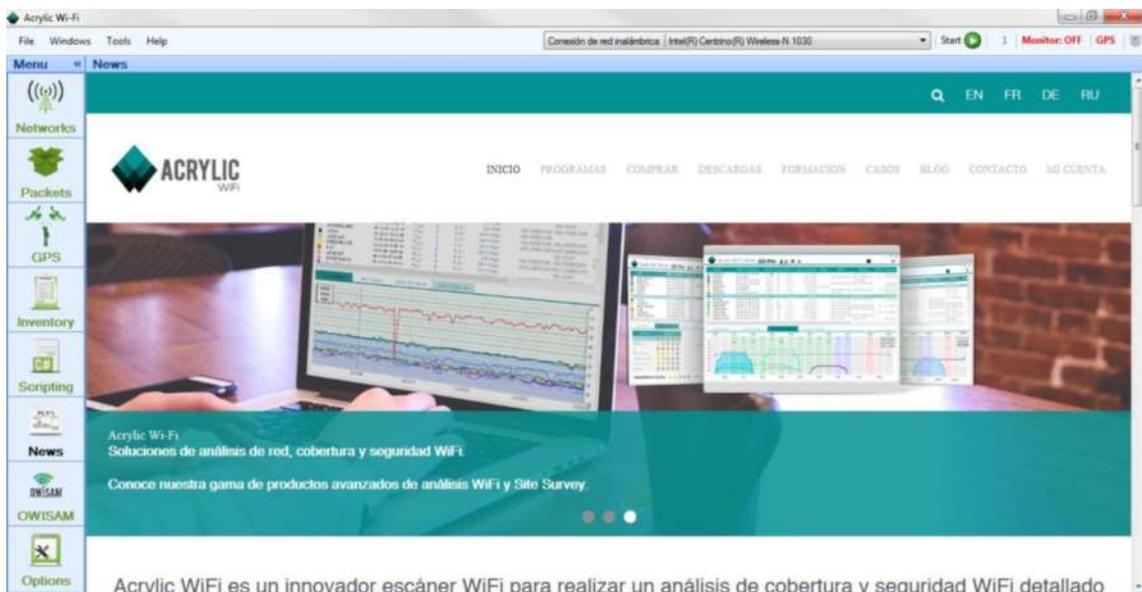


Figura 2-5: Software Acrylic

Fuente: SARABIA, Braulio.2018

El Software Acrylic fue desarrollado por la empresa Tarlogic, mediante este software podemos monitorear las redes inalámbricas existentes. Mediante las funciones de Acrylic podemos:

- Capturar el tráfico de una red
- Obtener información sobre las redes disponibles
- Obtener información sobre los clientes conectados y el tráfico en las redes
- Permite ejecutar Scripts (Comprueba la seguridad de la red)
- Geolocalización mediante GPS (Velasco. 2013)

2.4.1.1. Lista de redes WIFI al alcance y numero de dispositivos conectados

Con la ayuda del Software Acrylic podemos observar a continuación una lista con las redes Wifi que se encuentran al alcance del edificio de la FIE.

Access Points (Showing 47 of 47, Updated 16)										
	SSID	#	Mac Address	Rssi	Chan	802.11	WEP	WPA	WPA2	WPS
	ESPOCH-WIFI-P2		48:F8:B3:1D:54:88	-89	36	a, n			PSK-CCMP	1.0
	LAURA		00:26:B6:82:47:EE	-49	11	b, g		PSK-CCMP		
	eduroam		38:ED:18:B6:6F:82	-75	11	g, n			MGT-CCMP	
	FIE		48:F8:B3:1D:53:E7	-37	6	b, g, n			PSK-TKIP	
	ESPOCH-PORTAL		0C:F5:A4:EE:53:A0	-45	6	g, n	Open			
	eduroam		0C:F5:A4:EE:53:A2	-45	6	g, n			MGT-CCMP	
	ESPOCH-WIFI-P2		48:F8:B3:1D:54:87	-79	6	b, g, n			PSK-CCMP	1.0
	iMac de Imacpd10		88:63:DF:B8:9C:73	-65	11	b, g, n	Open			
	eduroam		DC:CE:C1:72:8F:C2	-66	1	g, n			MGT-CCMP	
	ESPOCH-PORTAL		DC:CE:C1:72:8F:C0	-68	1	g, n	Open			
	Red Asus		D2:57:7B:FD:BD:58	-81	6	b, g, n			PSK-CCMP	1.0
	ESPOCH-FIE-DOCENTE		68:7F:74:27:16:5E	-68	11	b, g, n		PSK- (TKIP CCMP)	PSK- (TKIP CCMP)	1.0
	LDC_SAP_MMA		B6:6D:83:13:2F:1D	-78	6	g, n			PSK-CCMP	
	ESPOCH-PORTAL-2		DC:CE:C1:72:92:EF	-83	165	a	Open			
	ESPOCH-PORTAL		38:ED:18:B6:6F:80	-75	11	g, n	Open			
	ESPOCH-PORTAL		DC:CE:C1:72:8F:CF	-77	153	a, n	Open			
	eduroam		DC:CE:C1:72:8F:CD	-77	153	a, n	SharedKey			
	eduroam		DC:CE:C1:72:92:E1	-76	11	g, n			MGT-CCMP	
	FM-UCOMPUTO		48:F8:B3:1D:55:B8	-90	1	b, g, n			PSK- (TKIP CCMP)	
	Netlife-Patricio Yanez		08:96:AD:CF:FA:10	-86	1	b, g, n			PSK-CCMP	
	eduroam		DC:CE:C1:72:92:EE	-83	165	a	SharedKey			
	ESPOCH-PORTAL-2		DC:CE:C1:72:92:E0	-77	11	g, n	Open			
	BSFASTpsilon		64:D1:54:5B:C6:7B	-80	157	n, ac			PSK-CCMP	
	eduroam		38:ED:18:B6:DE:A1	-82	6	g, n			MGT-CCMP	
	[Hidden]		02:0E:DC:44:9C:8D	-88	6	b, g, n		PSK- (TKIP CCMP)	PSK- (TKIP CCMP)	
	BS139Z2N31		02:15:6D:69:CA:09	-89	104	a	Open			
	BS139Z2N21		02:00:00:AA:00:0C	-89	104	a	Open			
	eduroam		0C:F5:A4:EE:4F:A2	-83	6	g, n			MGT-CCMP	
	JULIO		54:B8:0A:10:80:C0	-90	5	b, g, n		PSK- (TKIP CCMP)	PSK- (TKIP CCMP)	1.0
	ESPOCH-PORTAL		0C:F5:A4:EE:4F:A0	-82	6	g, n	Open			
	DOCENTES_EIA		B4:75:0E:AB:79:91	-88	11	b, g, n			PSK-CCMP	
	Netlife Monica		0A:0E:DC:44:9C:8D	-89	6	b, g, n		PSK- (TKIP CCMP)	PSK- (TKIP CCMP)	1.0
	DESKTOP-VVEMRC6 46		2A:D2:24:D7:5A:76	-84	11	g, n			PSK-CCMP	1.0
	ESPOCH-PORTAL-2		38:ED:18:B6:6F:80	-75	11	g, n	Open			

Figura 2-6: Lista de redes wifi

Fuente: SARABIA, Braulio.2018

Como se puede apreciar en la gráfica hay muchas redes inalámbricas y en cada momento esta lista se va a ir modificando, debido al ingreso de personas al edificio o ya sea que estén transcurriendo cerca de este con sus dispositivos electrónicos que cuenta con una red de datos de alumnos cerca del edificio.

A más de mostrar una lista de las redes que se encuentran al alcance también nos da información detallada como:

- **Mac Address.** - Es una dirección física y es única para cada dispositivo de red.
- **Canales.** - Me indica en que canal se está transmitiendo dicha señal.
- **Estándar 802.11.**- Define el uso de los dos niveles inferiores del modelo OSI, especificando las normas de funcionamiento de una red inalámbrica (WLAN).

- **Protocolos de seguridad.** - Estos protocolos de seguridad inalámbrico WEP, WPA WPA2 evitan que personas no deseadas se conecten a la red.

2.4.1.2. Niveles de las señales

Los niveles de la señal dependen principalmente del lugar o distancia donde se encuentre el punto de acceso, si el punto de acceso está cerca del dispositivo la intensidad de la señal será buena.

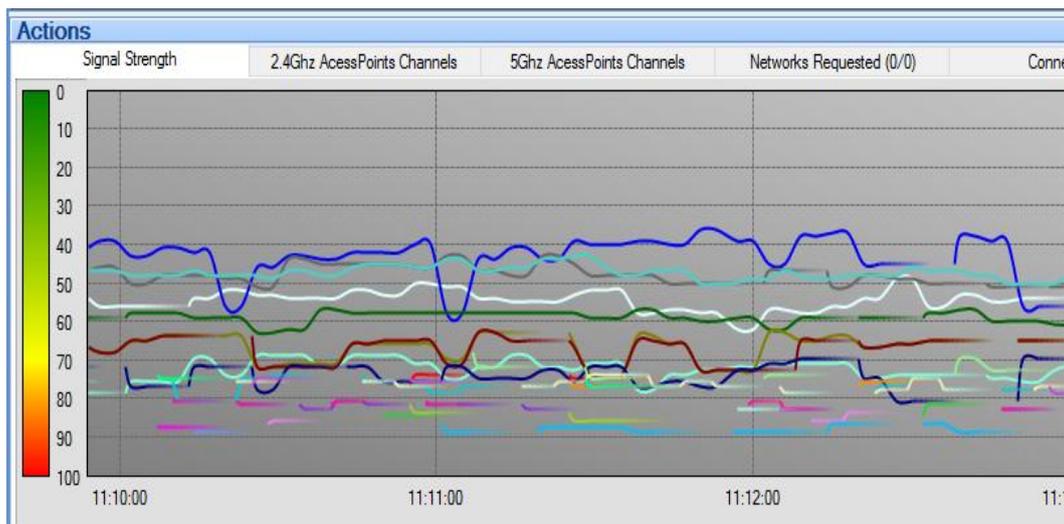


Grafico 2-1: Intensidad de la señal

Fuente: SARABIA, Braulio.2018

Como podemos apreciar la gráfica me indica el nivel de la intensidad de la señal, su unidad de medida es el decibelio (dBm) es una relación de potencia de la potencia medida. La escala del 0 al 100 es negativa. Esto quiere decir que el número que esté más cerca del 0 me indica mejor señal y la escala en sentido de lejos me indica que la señal se está transmitiendo en tiempo real.

Debemos tener en cuenta que una señal con niveles entre:

- **0.-** Señal ideal, es muy difícil de lograr
- **-40 a -60.-** Señal idónea con transferencia estable
- **-60.-** Enlace bueno
- **-70.-** Enlace normal bajo
- **-80.-** Es la señal mínima aceptable

Esto quiere decir, cuanto mayor sea el nivel de la señal mejor será la velocidad de transmisión y nos encontraremos más cerca del dispositivo.

2.4.1.3. Canales en que las redes están transmitiéndola señal

Las redes que se encuentran al alcance del edificio están transmitiendo en un canal WIFI o frecuencia diferente.

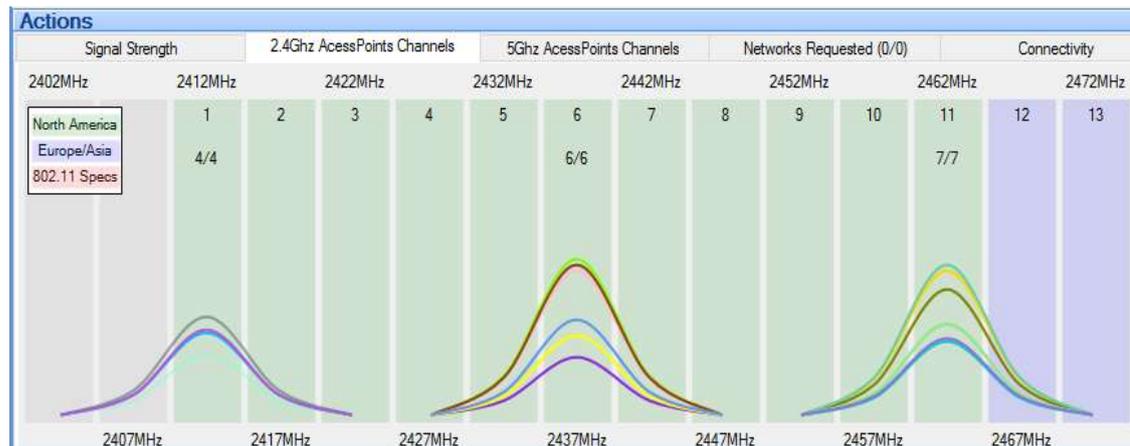


Gráfico 2-2: Rango de frecuencia y número de canales

Fuente: SARABIA, Braulio.2018

Aquí podemos apreciar la frecuencia a la que cada una de las señales está transmitiendo, así como también el número de canal. La frecuencia a la que trabajan es de 2.4 GHz y cada señal transmite en este rango de frecuencias.

Las señales pueden estar entre el canal 1 y el 14, las señales se distribuyen en el rango de frecuencias de 2.4 GHz. Como tenemos demasiadas redes que se encuentran cerca del edificio tenemos mucha interferencia, ya que cuanto mayor sea el número de redes que tenemos en un mismo canal o canales adyacentes, mayor será el ruido y la interferencia.

2.4.2. Principales redes inalámbricas existentes en el edificio de la FIE

Gracias a lista de redes WIFI que se puede obtener con la ayuda de este software, podemos observar cuales son las principales redes que existentes en el edificio de la FIE. Para la transmisión y recepción de datos en este de sistema de videovigilancia IP necesitaremos de una red WIFI, es por este motivo que se va a realizar el estudio de cada una de las redes que se determinen como principales del edificio con la finalidad de tener la mejor señal y con una vista más clara y precisa podremos escoger una de red WIFI para trabajar con nuestro sistema.

2.4.2.1. Lista de las principales redes WIFI

A continuación, y con la ayuda de una las funciones del software que es Inventory podemos seleccionar una lista específica de dichas redes a estudiar y analizar.

Access Points (Showing 47 of 47, Updated 11)									
	SSID	#	Mac Address	Rssi	Chan	802.11	WEP	WPA	WPA2
<input type="checkbox"/>	ESPOCH-WIFI-P2		48:F8:B3:1D:54:88	-88	36	a, n			PSK-CCMP
<input type="checkbox"/>	LAURA		00:26:B6:82:47:EE	-46	11	b, g		PSK-CCMP	
<input type="checkbox"/>	eduroam		38:ED:18:B6:6F:82	-76	11	g, n			MGT-CCMP
<input checked="" type="checkbox"/>	FIE		48:F8:B3:1D:53:E7	-36	6	b, g, n			PSK-TKIP
<input type="checkbox"/>	ESPOCH-PORTAL		0C:F5:A4:EE:53:A0	-46	6	g, n	Open		
<input type="checkbox"/>	eduroam		0C:F5:A4:EE:53:A2	-46	6	g, n			MGT-CCMP
<input type="checkbox"/>	ESPOCH-WIFI-P2		48:F8:B3:1D:54:87	-73	6	b, g, n			PSK-CCMP
<input type="checkbox"/>	iMac de Imacpd10		88:63:DF:B8:9C:73	-64	11	b, g, n	Open		
<input type="checkbox"/>	eduroam		DC:CE:C1:72:8F:C2	-76	1	g, n			MGT-CCMP
<input type="checkbox"/>	ESPOCH-PORTAL		DC:CE:C1:72:8F:C0	-67	1	g, n	Open		
<input type="checkbox"/>	Red Asus		D2:57:7B:FD:BD:58	-81	6	b, g, n			PSK-CCMP
<input checked="" type="checkbox"/>	ESPOCH-FIE-DOCENTE		68:7F:74:27:16:5E	-68	11	b, g, n		PSK- (TKIP CCMP)	PSK- (TKIP CCMP)
<input type="checkbox"/>	LDC_SAP_MMA		B6:6D:83:13:2F:1D	-67	6	g, n			PSK-CCMP
<input type="checkbox"/>	ESPOCH-PORTAL-2		DC:CE:C1:72:92:EF	-82	165	a	Open		

Figura 2-7: Redes principales WIFI existentes en el edificio FIE
Fuente: SARABIA, Braulio.2018

Inventory (3) - Free version limited to "5" entries.		
Mac Address	Name	Vendor
48:F8:B3:1D:53:E7	AP FIE	Cisco-Linksys. LLC
48:F8:B3:1D:54:87	AP ESPOCH-WIFI-P2	Cisco-Linksys. LLC
68:7F:74:27:16:5E	AP ESPOCH-FIE-DOCENTES	Cisco-Linksys. LLC

Figura 2-8: Lista de las redes específicas
Fuente: SARABIA, Braulio.2018

Como podemos observar tenemos tres redes WIFI específicas que existen en el edificio de la FIE. Cada una de estas redes será estudiada y analizada para determinar cuál de estas redes tiene mejor nivel de señal.

Para una mejor comprensión se estudiará cada red con el nombre específico con que el software las registra.

- 1) FIE
- 2) ESPOCH-WIFI-P2
- 3) ESPOCH-FIE-DOCENTES

2.4.2.2. Análisis y estudio de cada red

1) Señal WIFI FIE

Mediante los datos obtenidos con la ayuda del software procederemos a realizar su análisis respectivo. El color con que se muestra en esta lista es de color azul claro.

- Niveles de señal

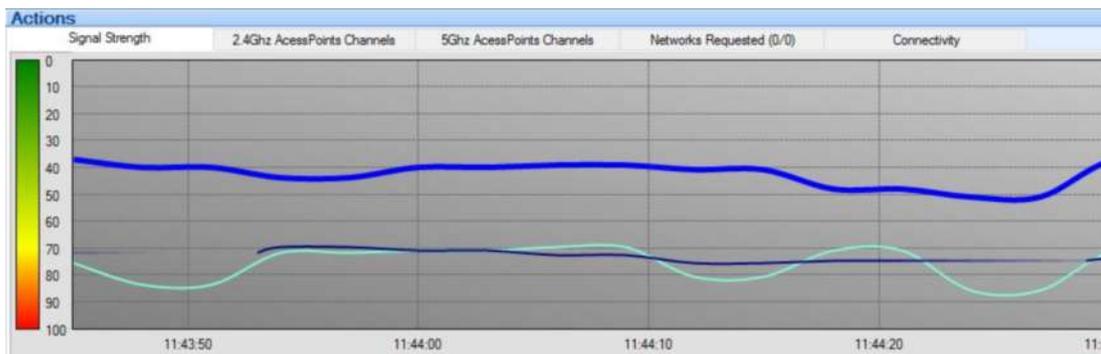


Gráfico 2-3: Intensidad de la señal FIE

Fuente: SARABIA, Braulio.2018

Como se observa esta señal está transmitiendo en tiempo real y en el rango de 40 a 50 db, por lo estudiado anteriormente podemos decir que la calidad de la señal FIE es excelente o idónea.

- Canal y rango de frecuencia en la que está transmitiendo

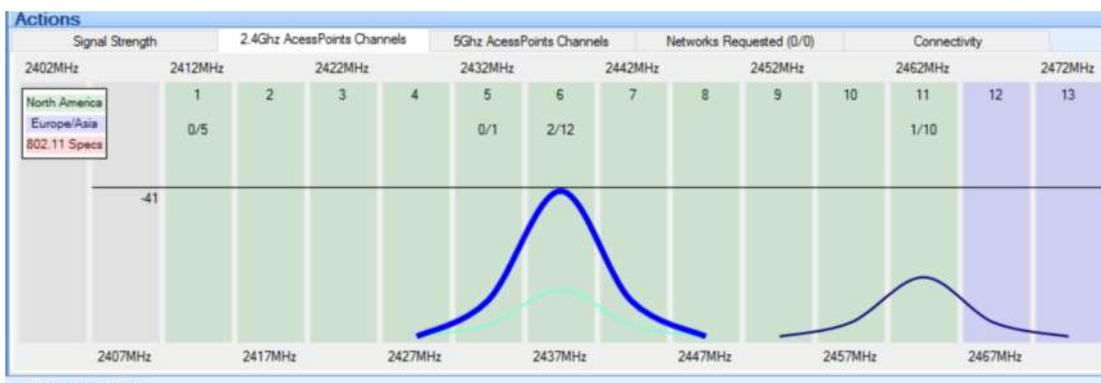


Gráfico 2-4: Canal y rango de frecuencias de la señal FIE

Fuente: SARABIA, Braulio.2018

Esta señal trabaja en la frecuencia de 2.4 GHz y pueden estar en los canales 1 y 14, podemos observar que esta señal está en el canal 6, con un rango de frecuencia de (2427 – 2447) MHz y un nivel de -41 db.

En la *Figura 5-2* lista de redes WIFI se puede observar que muchas redes están transmitiendo su señal en el canal 6, debido al mayor número de redes en este canal podemos decir que hay mucha interferencia.

Pero tenemos que tener en cuenta que muchas de las redes que transmiten en este canal son redes temporales, ya que son detectadas al momento del paso de estudiantes cerca del edificio o personas que transcurren por algún motivo a la facultad, pero su estancia no es permanente y su señal se perderá cuando estén a cierta distancia alejada del edificio.

2) Señal WIFI ESPOCH-WIFI-P2

Mediante los datos obtenidos con la ayuda del software procederemos a realizar su análisis respectivo. El color con que se muestra en esta lista es de color celeste.

- Niveles de señal

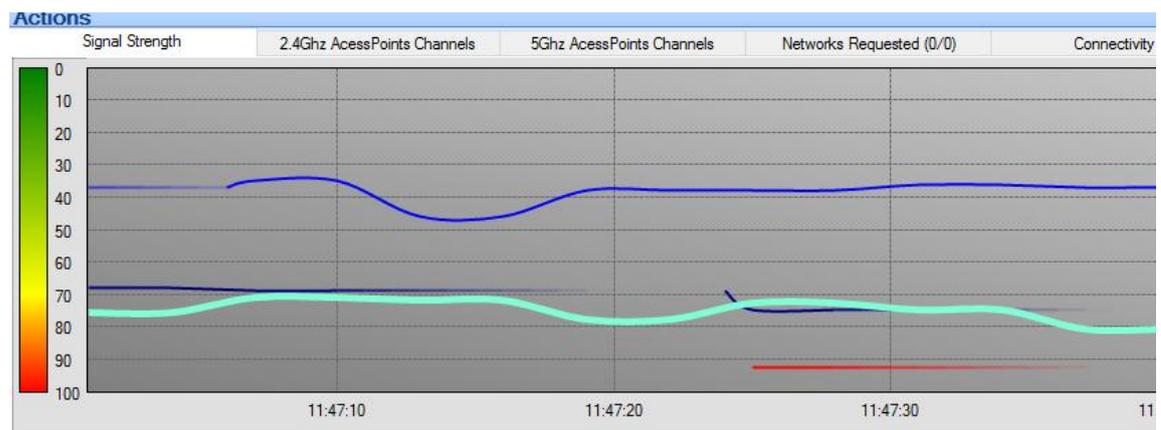


Grafico 2-5: Intensidad de la señal ESPOCH-WIFI-P2

Fuente: SARABIA, Braulio, 2018

Como se observa esta señal está transmitiendo en tiempo real y en el rango de 70 a 80 db, por lo estudiado anteriormente podemos decir que la calidad de la señal FIE es la mínima aceptable por lo que se considera como señal baja.

- Canal y rango de frecuencia en la que está transmitiendo

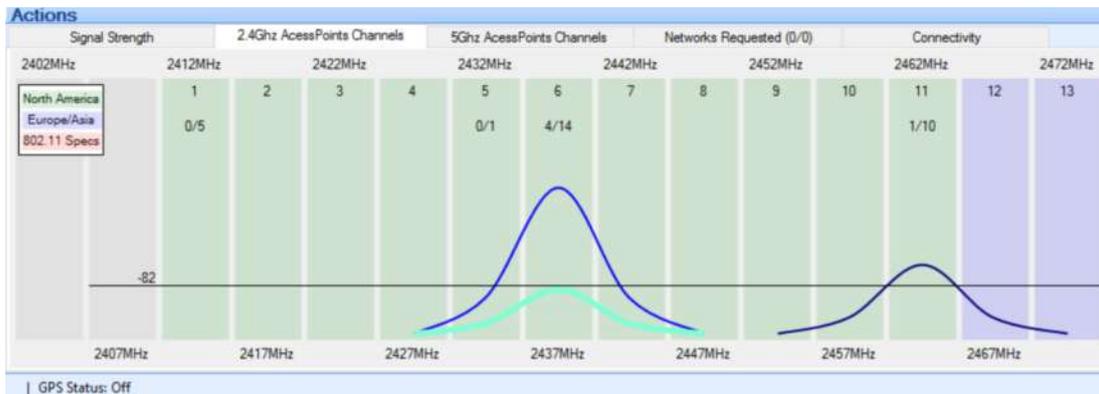


Grafico 2-6: Canal y rango de frecuencias de la señal ESPOCH-WIFI-P2

Fuente: SARABIA, Braulio.2018

Esta señal trabaja en la frecuencia de 2.4 GHz y pueden estar en los canales 1 y 14, podemos observar que esta señal también está en el canal 6, con un rango de frecuencia de (2427 – 2447) MHz y un nivel de -82 db.

Debido a que esta señal está el canal 6 y en el mismo rango de frecuencia se puede decir que hay un poco de interferencia, pero debido a los niveles de potencia y el lugar donde se encuentran los distintos puntos de acceso la interferencia producida tiene un nivel bajo.

3) Señal WIFI ESPOCH-FIE-DOCENTES

Mediante los datos obtenidos con la ayuda del software procederemos a realizar su análisis respectivo. El color con que se muestra en esta lista es de color azul oscuro.

- Niveles de señal

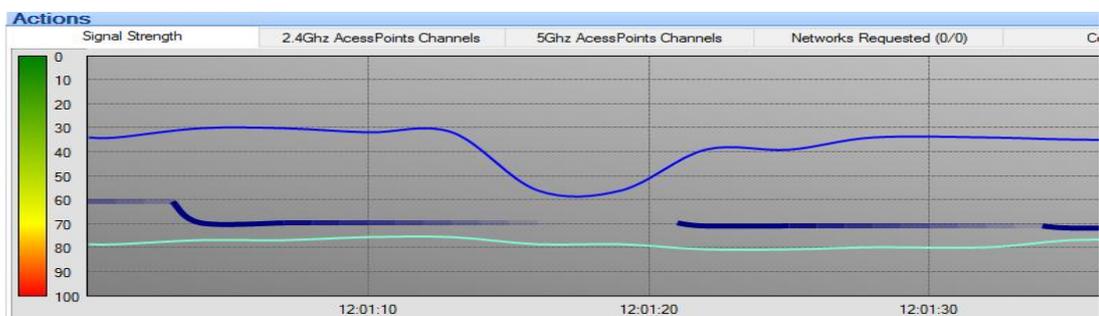


Grafico 2-7: Intensidad de la señal ESPOCH-FIE-DOCENTES

Fuente: SARABIA, Braulio.2018

Como se observa esta señal está transmitiendo en tiempo real y en el rango de 60 a 70 db, por lo estudiado anteriormente podemos decir que la calidad de la señal ESPOCH-FIE-DOCENTES se considera como señal baja.

- Canal y rango de frecuencia en la que está transmitiendo

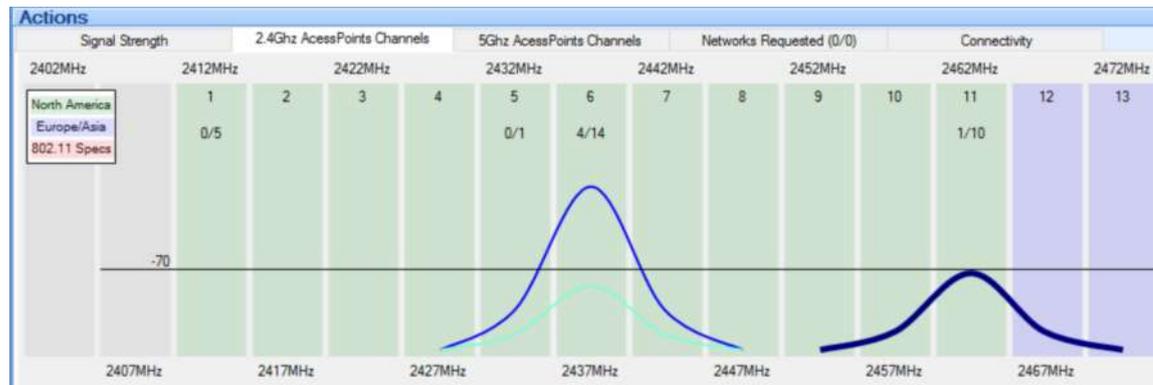


Grafico 2-8: Canal y rango de frecuencias de la señal ESPOCH-FIE-DOCENTES
Fuente: SARABIA, Braulio.2018

Esta señal trabaja en la frecuencia de 2.4 GHz y pueden estar en los canales 1 y 14, podemos observar que esta señal está en el canal 11, con un rango de frecuencia de (2457 – 2467) MHz y un nivel de -70 db.

En la *Figura 5-2* lista de redes WIFI se puede observar que algunas redes están transmitiendo su señal en el canal 11, debido al mayor número de redes en este canal podemos decir que hay mucha interferencia.

Pero tenemos que tener en cuenta que muchas de las redes que transmiten en este canal son redes temporales, ya que son detectadas al momento del paso de estudiantes cerca del edificio o personas que transcurren por algún motivo a la facultad, pero su estancia no es permanente y su señal se perderá cuando estén a cierta distancia alejada del edificio. Tomando en cuenta esto se puede decir que la interferencia producida por estas señales wifi desaparecería.

2.4.2.3. Elección de la mejor red WIFI

Para la elección de la mejor señal o la señal con la que se va a trabajar para este sistema de videovigilancia. Se tomó en cuenta el mejor nivel de la intensidad de la señal, el número de redes que están transmitiendo en ese mismo canal.

Para la elección de la mejor señal, se tomó en cuenta solo las principales redes wifi existentes en el edificio de la FIE. A continuación, se presenta una tabla con la información de estas señales para luego proceder a su elección.

Tabla 1-2: Tabla comparativa para determinar la señal WIFI con mejor calidad

Red WIFI	Nivel de señal (db)	Canal	Calidad de señal
FIE	41 db	6	Excelente
ESPOCH-WIFI-P2	82 db	6	Baja
ESPOCH-FIE-DOCENTES	70 db	11	Baja

Realizado por: SARABIA, Braulio. 2018

Basado en los parámetros que se observan en esta tabla, se puede concluir basado en el nivel de señal, canal de transmisión y la calidad de la señal que la red WIFI con el nombre **FIE** es la red con mejor nivel y una calidad excelente para la transmisión y por tanto esta red es una opción a utilizar para este sistema de videovigilancia inalámbrico.

2.4.3. Red inalámbrica para el sistema de seguridad

Con el estudio que se realizó de las redes existentes en el edificio de la FIE, se determinó la señal que presentaba mayores niveles y alta calidad. La red que cumplía con estos parámetros es la red con el nombre FIE.

La red inalámbrica FIE tiene un alto nivel de señal y por la tanto su transmisión es rápida. Estas redes inalámbricas son utilizadas tanto por los docentes y estudiantes que se encuentran a una distancia aceptable y puedan acceder a esta red y a su vez a internet, debido al número excesivo de dispositivos que se encuentran conectados a las distintas redes, dichas redes se vuelven un poco lentas en la transmisión y recepción de datos.

Por estas y otras razones y con la finalidad que nuestro sistema de videovigilancia sea un sistema seguro y confiable. Se conversó con los ingenieros del departamento de DESITEL y se les hizo conocer el tema de trabajo de titulación, como dicho sistema no necesita navegación y lo único que se necesita es una red para que las cámaras se puedan conectar mediante una dirección IP y así puedan transmitir. Dicho departamento nos ayudó con la creación de una nueva red con el nombre de **HIKVISION** que posee la misma cobertura.

2.4.3.1. Análisis de la red inalámbrica Hikvision

A continuación, se analizará esta nueva red que se creó para este sistema de videovigilancia inalámbrico, cabe recalcar que este SSID puede ser modificado.

Mediante los datos obtenidos con la ayuda del software Acrylic procederemos a realizar su análisis respectivo. El color con que se muestra en esta lista es de color azul oscuro.

Access Points (Showing 27 of 27, Updated 8)							
	SSID	#	Mac Address	Rssi	Chan	802.11	WEP
■	ESPOCH-PORTAL		0C:F5:A4:EE:56:F0	-70	11	g.n	Open
■	Hikvision		0C:F5:A4:EE:56:F3	-70	11	g.n	
■	eduroam		0C:F5:A4:EE:56:F2	-70	11	g.n	

Figura 2-9: Red Wifi principal en el edificio de la FIE

Fuente: SARABIA, Braulio, 2018

- Niveles de señal

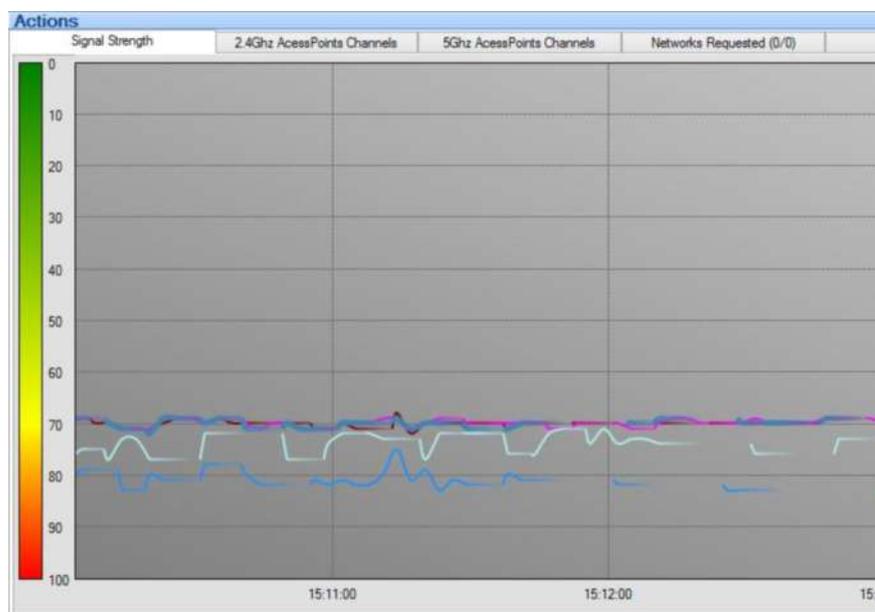


Gráfico 2-9: Intensidad de la señal HIKVISION

Fuente: SARABIA, Braulio, 2018

Como se observa esta señal está transmitiendo en tiempo real y en el rango de 60 a 70 db, por lo estudiado anteriormente podemos decir que la calidad de la señal HIKVISION se considera como señal buena.

- Canal y rango de frecuencia en la que está transmitiendo

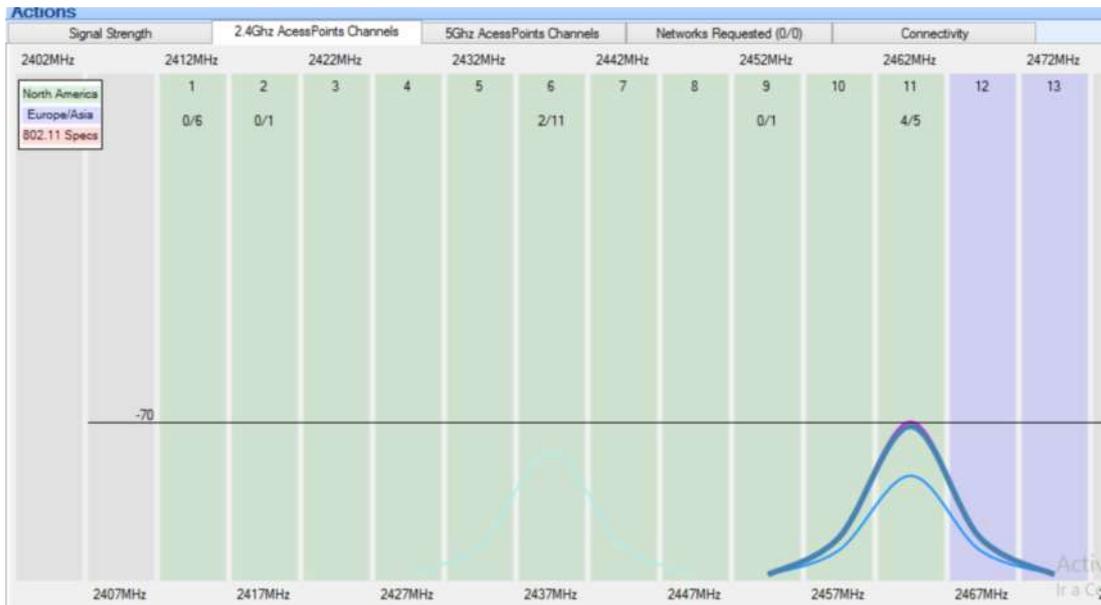


Grafico 2-10: Canal y rango de frecuencias de la señal HIKVISION

Fuente: SARABIA, Braulio, 2018

Esta señal trabaja en la frecuencia de 2.4 GHz y pueden estar en los canales 1 y 14, podemos observar que esta señal está en el canal 11, con un rango de frecuencia de (2457 – 2467) MHz y un nivel de -70 db.

Existen otras redes que estén el mismo canal, pero estas redes son solo temporales y por eso la interferencia que cusan es de muy bajo nivel.

Debemos tener muy en cuenta que el nivel de esta señal es aceptable para este sistema. Como ya se explicó no necesitamos para navegación y por esta razón dicho nivel de señal será suficiente para un buen funcionamiento de nuestro sistema.

CAPITULO III

3. MARCO DE RESULTADOS

3.1. Diseño del sistema de video vigilancia

El sistema de video vigilancia permite brindar seguridad al edificio nuevo de la FIE, el cual garantiza un adecuado manejo del monitoreo en tiempo real, así como también su almacenamiento de forma segura y sencilla, todas estas funciones deben ser realizadas por una persona la cual solo podrá acceder de manera segura mediante contraseña con la finalidad de que la información sea manejada y utilizada de forma correcta y con su respectiva confidencialidad.

El edificio contara con la seguridad tanto en la parte externa como interna del edificio y para esto se necesario conocer la situación actual y como está distribuida su planta baja y cada uno de sus pisos, así como se necesita conocer las dimensiones con que cuenta esta infraestructura.

Con la finalidad de no invadir la privacidad de los estudiantes y docentes, las cámaras se instalaron en los pasillos de la planta baja y de los dos pisos. Estas cámaras enfocaran principalmente las puertas de las oficinas, aulas y laboratorios de cada edificio, Con esto no se invadirá la privacidad tanto en el interior de las aulas y de las oficinas. Esta ubicación se preciso con la finalidad de no tener puntos ciegos en todo el edificio.

3.1.1. Infraestructura y situación actual del edificio de la FIE

Para el diseño del sistema de video vigilancia es necesario conocer las dimensiones de la infraestructura y saber las secciones con las que cuenta la planta baja y sus dos pisos.

A continuación, se realiza un análisis de toda la infraestructura del edificio.

3.1.1.1. Planta baja

La planta baja del edificio nuevo de la FIE cuenta con la siguiente infraestructura.

- Tres aulas
- Tres laboratorios
- Una oficina múltiple (secretaría y Dirección de Telecomunicaciones y Redes, secretaria y Dirección de Control y Redes Industriales)
- Una sala multimedia
- Servicio Higiénico

Tiene dos entradas y un pasillo que sirve para el ingreso tanto a la planta baja como al primer y segundo piso del edificio, además cuenta con un ascensor, también cuenta con una tercera entrada que entra en funcionamiento solo cuando se utiliza la sala multimedia. Tanto en la entrada principal como la secundaria cuentan con espacios (gradas) que permiten el acceso a los pisos superiores del edificio. (Véase ANEXO A)

3.1.1.2. Primer piso

El primer piso del edificio nuevo de la FIE cuenta con la siguiente infraestructura.

- Tres aulas
- Tres laboratorios
- Una oficina múltiple (secretaría, Decanato, Investigación y Postgrado)
- Una Biblioteca Multimedia (Funciona como oficina de Ingenieros de la FIE)
- Servicio Higiénico

El pasillo que es utilizado para el desplazamiento de las personas cuenta con gradas que permiten el acceso al segundo piso y a la planta baja del edificio, cabe destacar que estos espacios (gradas) dan salida y entrada tanto en la puerta principal como en la secundaria. (Véase ANEXO B)

3.1.1.3. Segundo piso

El segundo piso del edificio nuevo de la FIE cuenta con la siguiente infraestructura.

- Tres aulas
- Tres laboratorios
- Una oficina múltiple (secretaría, Vicedecanato, secretaria y dirección de otras escuelas)
- Bodega de laboratorios
- Sala de control

El pasillo que es utilizado para el desplazamiento de las personas cuenta con un espacio (gradas) que permiten el paso al primer piso y a la planta baja del edificio, cabe recalcar que también se puede utilizar el ascensor para su desplazamiento a los diferentes pisos. (Véase ANEXO C)

3.1.2. Requerimientos para el diseño e implementación del sistema de video vigilancia

Para una correcta instalación y un buen funcionamiento del sistema de video vigilancia, es necesario contar con requerimientos tales como:

- Energía eléctrica
- Servicio de internet
- Enrutador (Router)
- Cámaras de video vigilancia
- Cable eléctrico y cable de red
- Unidad de almacenamiento o procesador de video
- Disco duro
- Sala de monitoreo

3.2. Descripción de los elementos a utilizar para el sistema de video vigilancia

Con lo estudiado anteriormente y con todas las características que se pudo conocer de cada elemento que va a ser utilizado en este sistema de videovigilancia, se pudo seleccionar cada elemento preciso según las necesidades del sistema, gracias a este análisis podemos dar a conocer cada equipo y su descripción correspondiente. Todos los equipos son de la marca Hikvision.

3.2.1. Cámaras

El sistema de video vigilancia requiere ciertas prestaciones para un buen funcionamiento y una buena calidad de la imagen, razón por la cual las cámaras deberán ser de alta calidad, así como también tener una buena visibilidad tanto para el día como para la noche y lo que es más importante deben ser bien equipadas y protegidas en caso de que suceda algún acto ilícito o vandálico.

A continuación, se detalla los dos tipos de cámaras que se utilizaron para este sistema de videovigilancia.

3.2.1.1. Cámara IP domo DS-2CD1121-i

Este tipo de cámaras tiene una resolución de 2 MP, es de tipo domo como se puede apreciar en la *Figura 9-3*, además cuenta con una calidad en HD, su filtro IR es de gran ayuda ya que en la oscuridad permite captar imágenes con colores más reales, su utilización es para interiores en algunos casos para lugares a intemperie además cuenta con resistencia en caso de que llegue a suceder actos vandálicos.



Figura 3-1: Cámara IP DS-2CD1121-i tipo Domo

Fuente: SARABIA, Braulio.2018

Entre sus principales características se encuentran:

- Codificación: Principal:H264+ / H264 // Secundaria: H264 / MJPEG.
- Sensor CMOS de escaneo progresivo de 1/2.8".
- Hasta 2.0 Mpx de resolución.
- Óptica fija de 2,8mm
- Hasta 30 m de alcance IR
- 0,01 lux Color (F1.2, AGC ON) y 0 lux con IR.
- Doble streaming de vídeo.
- WDR digital (rango dinámico amplio).
- 3D DNR (Reducción de ruido digital) y PoE (alimentación a través de Ethernet).
(hommax. 2017)

Las especificaciones técnicas de esta cámara podemos observar en el ANEXO D

3.2.1.2. Cámara IP bullet DS-2CD1021-i

Este tipo de cámaras tiene una resolución de 2 MP, es de tipo bala como se puede apreciar en la *Figura 10-3*, además cuenta con una calidad en HD, su utilización es más para lugares a intemperie además cuentas con resistencia en caso de que llegue a suceder actos vandálicos.



Figura 3-2: Cámara IP DS-2CD1021-i tipo Bullet
Fuente: SARABIA, Braulio.2018

Entre sus principales características se encuentran:

- Codificación: Principal:H264+ / H264 // Secundaria: H264 / MJPEG.
- Resolución hasta 2.0 Mpx.
- Sensor CMOS 1/2.8".
- Alcance IR hasta 30 metros.
- Óptica fija de 2.8 mm.
- 0,01 lux Color (F1.2, AGC ON) y 0 lux con IR.
- Doble streaming de vídeo.
- WDR digital (rango dinámico expandido).
- 3D DNR (Reducción de ruido digital).
- PoE (alimentación a través de Ethernet).
- Índice de protección: IP67.
- Monitorización móvil a través de Hik-Connect o iVMS-4500.
- PoE (alimentación a través de Ethernet). (hommax. 2017)

Las especificaciones técnicas de esta cámara podemos observar en el ANEXO E

3.2.2. Servidor y medio de almacenamiento

El tráfico que circula por la red es en tiempo real y con HD (alta definición). La información que es obtenida por las cámaras se guarda por un lapso de 2 meses siempre y cuando las cámaras sean programadas para que realicen la grabación cuando haya movimiento, las cámaras van a operar todos los días las 24 horas al día. Este sistema de videovigilancia tiene un NVR en el cual se instaló un disco duro de 1 Tera.

3.2.2.1. NVR Ds7608ni-e2/8p

Grabador IP (NVR) serie 7600, soporta hasta 8 cámaras IP esto lo podemos observar en la *Figura 11-3*, o como también las especificaciones técnicas las podemos ver en el ANEXO F.



Figura 3-3: NVR IP DS7608ni-e2/8p

Fuente: SARABIA, Braulio.2018

Entre sus principales características se encuentran:

- Ancho banda de entrada: 50 Mbps
- Formato compresión H.264
- Capacidad de visualización: 1 cámara IP de 5Mpx/3Mpx o 2 de 2Mpx/1.3Mpx o 4 cámaras IP de 1Mpx o 8 cámaras IP de 4CIF/VGA
- Incorpora Switch POE de 8 puertos 10/100 Mbps
- Reproducción simultánea de 8 canales a 720P
- Salida de video: VGA y HDMI (max.1920x1080)
- Audio bidireccional: 1E/1S. Alarmas 4E/1S
- Acceso remoto desde: software incluido, navegador WEB, iPhone, Android
- IP Estática o Dinámica, con gran capacidad de envío a través de la red (puede enviar 128 canales de vídeo simultáneamente)
- Puertos: 1 x USB 2.0, 1 x USB 3.0, 1 xRJ45 Ethernet 10/100/100Mbps
- Capacidad de disco duro: 2SATA max 4TB no incluidos. Incluido ratón y mando IR. Dimensiones 445x290x45mm, chasis rack 19" 1U. (hommax. 2017)

3.2.2.2. Disco Duro Western Digital 1TB

Este tipo de discos duros son muy utilizados ya que sus características son las adecuadas para los sistemas de videovigilancia que requieren una grabación las 24 horas al día. Este disco duro fue instalado en el NVR que se está utilizando, su capacidad de almacenamiento es de 1Tb

como podemos ver en la *Figura 12-3*, además hay la posibilidad de poder incorporar otro disco duro de igual o mayor capacidad de almacenamiento en el NVR que se va a utilizar.



Figura 3-4: Disco Duro Western Digital 1TB
Fuente: SARABIA, Braulio.2018

Las especificaciones técnicas de este Disco duro se lo pueden observar en el ANEXO G.

3.2.2.3. Software gestión de almacenamiento

EL NVR que se está utilizando tiene su propio software el cual permite tener una visualización de manera local, basta con encenderlo, conectarlo un mouse y un monitor para poder tener una visualización de las cámaras que están conectadas, dicho NVR puede utilizar el software **IVMS 4200 o 4500**.



Figura 3-5: Software gestión de video Ivms-4200

Fuente: SARABIA, Braulio.2018

Dicho software presenta características tales como:

- Puede administrar hasta 1024 dispositivos / cámaras
- Puede administrar hasta 256 DVR's / NVR's
- Soporta hasta 4 monitores (64 cámaras simultaneas).
- Soporta equipos locales y remotos (P2P ó DDNS).
- Soporta audio de 2 vías
- Soporta configuración local y remota en dispositivos epcom y HIKVISION.
- Constantes actualizaciones GRATUITAS. (Syscom. 2017)

3.2.3. *Monitor*

Con la finalidad de poder observar las 8 cámaras IP que se encuentran distribuidas en el edificio nuevo de la FIE, se utilizó un monitor de 17 “pulgadas de la marca **Flatron L177WSB**, el cual nos fue asignado por la escuela gracias al pedido del Ing. David Moreno. Este monitor tiene una resolución Full HD que nos permite ver las imágenes a una alta calidad.



Figura 3-6: Monitor Flatron L177WSB

Fuente: SARABIA, Braulio.2018

Como se puede apreciar en la imagen se tiene un control de las 8 cámaras, pudiendo así también tener una visualización de la pantalla completa de cada una de las cámaras.

3.2.4. Protocolos

Para la conexión a internet se utilizó una LAN (red de área local) a la cual se anclará el NVR mediante una dirección IP fija la cual fue asignada por el departamento DETIC previo al oficio enviado. Así mismo cada una de las cámaras tendrá su propia dirección IP con la finalidad de que puedan trabajar normalmente y no acurra fallos al momento de la conexión.

Las cámaras IP tanto del tipo domo como tipo bala disponen del Protocolo PoE (Power Over Ethernet) para alimentación de voltaje, cuenta con el protocolo P2P el cual es para el intercambio rápido de datos, además cuentan con protocolos DHCP, FTP y RTSP.

Una de las características más importantes de estas cámaras IP es que poseen el estándar ONVIF el cual permite operar con múltiples marcas de cámaras, proporcionando así escalabilidad en la red. Utilizan el estándar H.264 que permite tener una baja tasa de bits logrando así mantener una menor latencia en la red y obteniendo un flujo de datos óptimo.

3.2.5. Acceso remoto y visualización

En los sistemas de seguridad de video vigilancia es de suma importancia tener acceso remoto a dicho sistema, con el objetivo de estar al tanto de todos los sucesos que transcurren durante el día y la noche, y más aún si nos encontramos fuera del alcance del sistema para poder verlo de manera local.

El software que trabaja directamente con las cámaras de marca Hikvision es **IVMS 4200**, es un software de gestión de video el cual permite tener una visualización en tiempo real de todas las cámaras que se encuentran instaladas en nuestro sistema, así como también permite realizar múltiples funciones que son de gran ayuda al momento de ver, grabar o reproducir los videos que fueron almacenadas.

A continuación, se procederá a la instalación de este software el cual fue utilizado en nuestro sistema.

Lo que se debe hacer es descargar este software y proceder a la instalación.

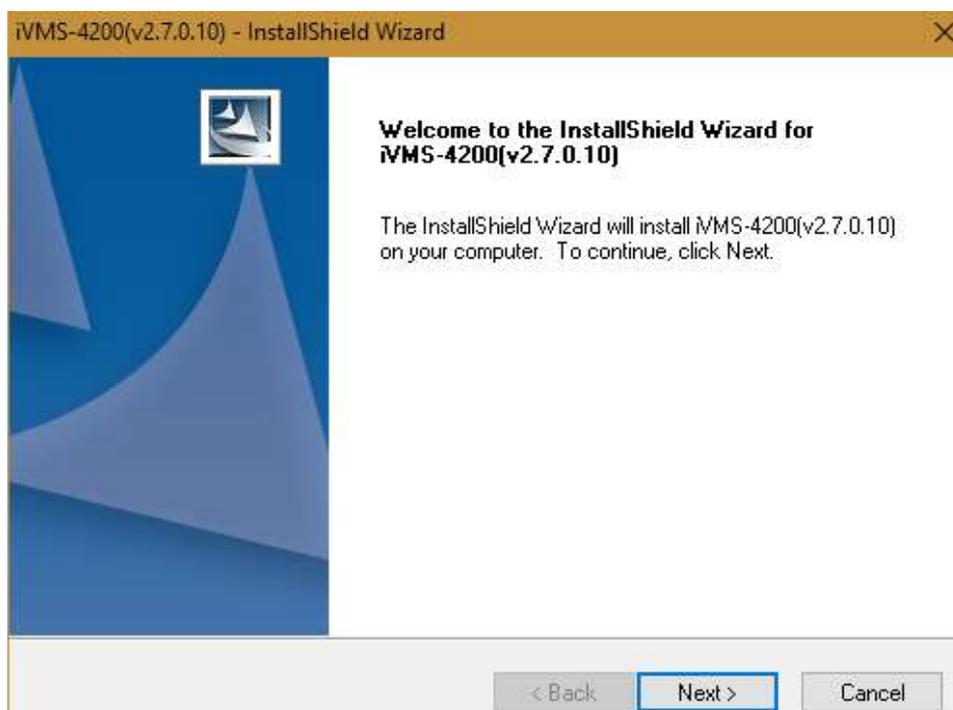


Figura 3-7: Instalación del Software IVMS 4200

Fuente: SARABIA, Braulio.2018

La instalación de este software no es complicada solo basta con dar siguiente y aceptar los términos de licencia y como se puede apreciar en la *figura16-3* debemos esperar unos minutos hasta que termine el proceso de la instalación.

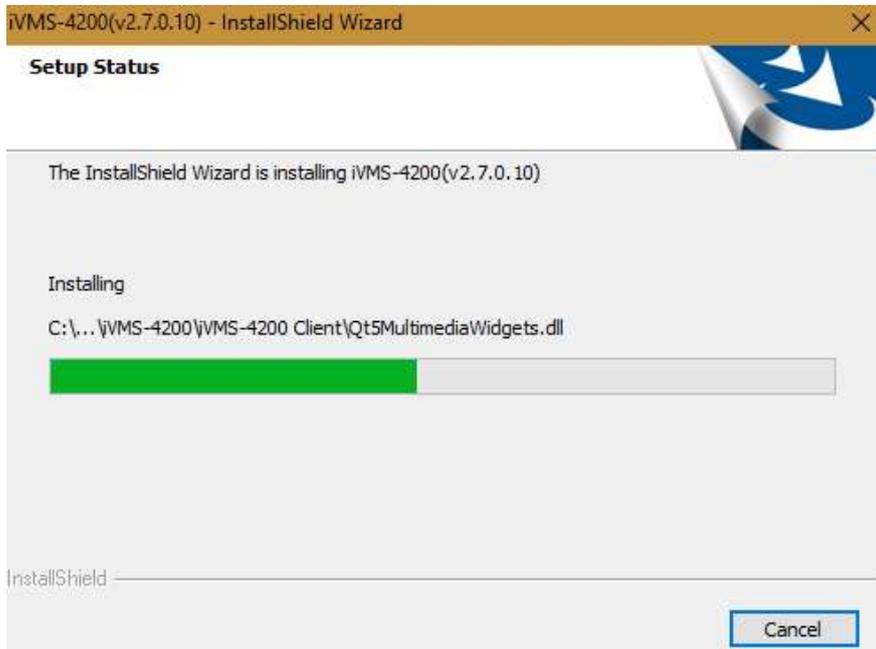


Figura 3-8: Instalación del Software IVMS 4200

Fuente: SARABIA, Braulio.2018

Una vez finalizada la instalación procedemos a iniciar el software, como se puede ver en la *figura 17-3* lo que nos pide es registrarnos.

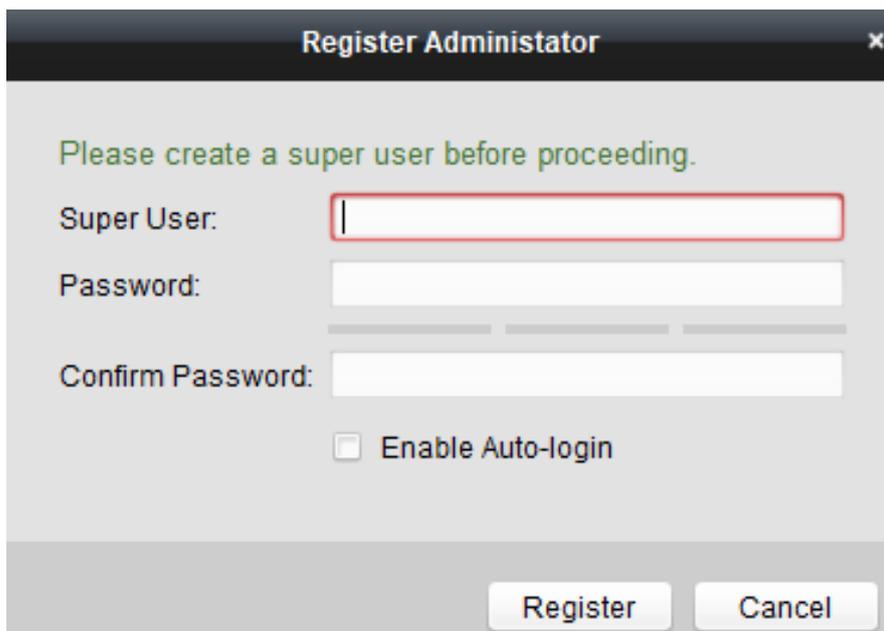


Figura 3-9: Registro en Software IVMS 4200

Fuente: SARABIA, Braulio.2018

Una vez que nos hemos registrado se nos mostrara una imagen con el logo de este software



Figura 3-10: Ejecución del Software IVMS 4200

Fuente: SARABIA, Braulio.2018

Al momento que se inicie la ejecución de este software, nos mostrara la interfaz principal del programa como podemos ver en la *figura 19-3*.

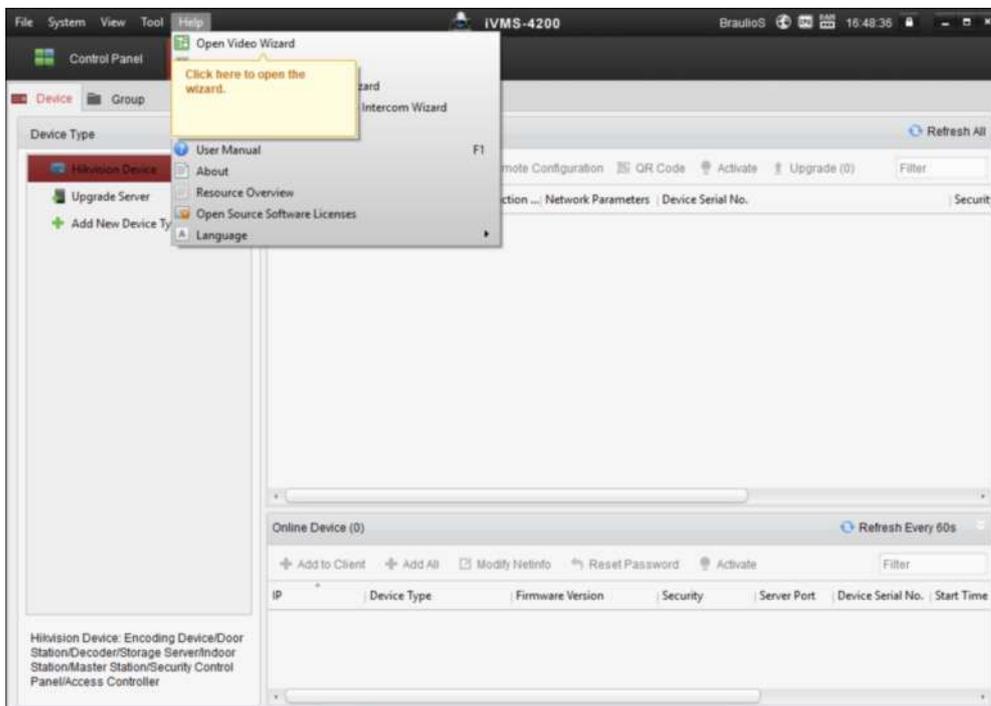


Figura 3-11: Ejecución del Software IVMS 4200

Fuente: SARABIA, Braulio.2018

En el momento que estemos en esta parte del software, empezamos con añadir el dispositivo que en este caso es nuestro NVR, pulsando click en añadir nos mostrara una ventana en la cual se ingresaran los datos de nuestro equipo.

Datos como el nombre, algo muy importante que se debe tener en cuenta es la dirección IP con la que se registró en nuestro NVR, así como también usuario y contraseña.

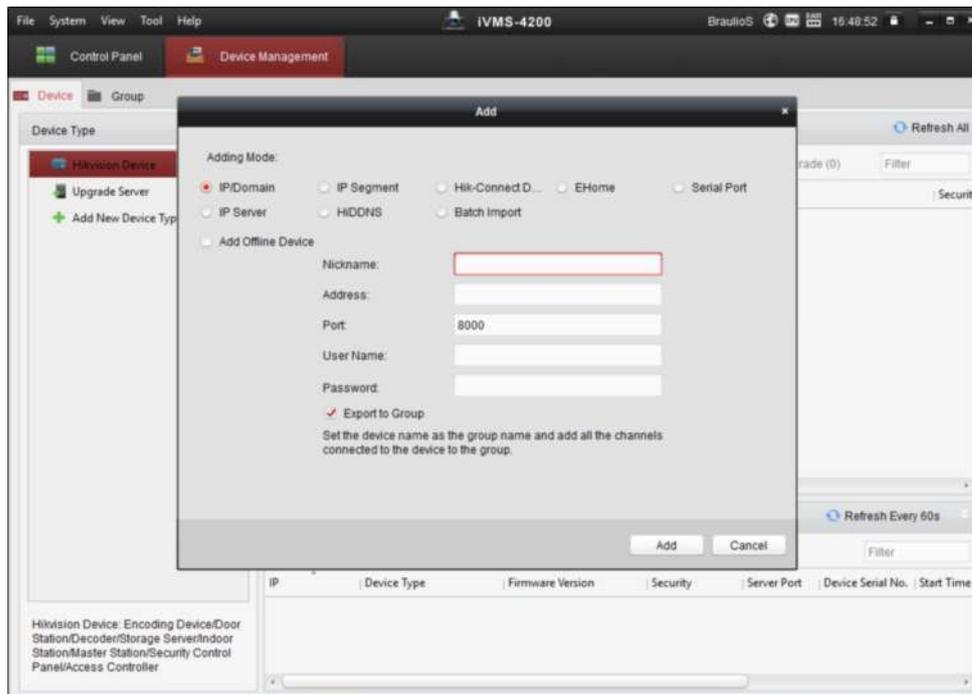


Figura 3-12: Registro del dispositivo NVR

Fuente: SARABIA, Braulio.2018

Si los datos coinciden con los datos que se configuraron en el NVR, nuestro dispositivo quedara añadido automáticamente.

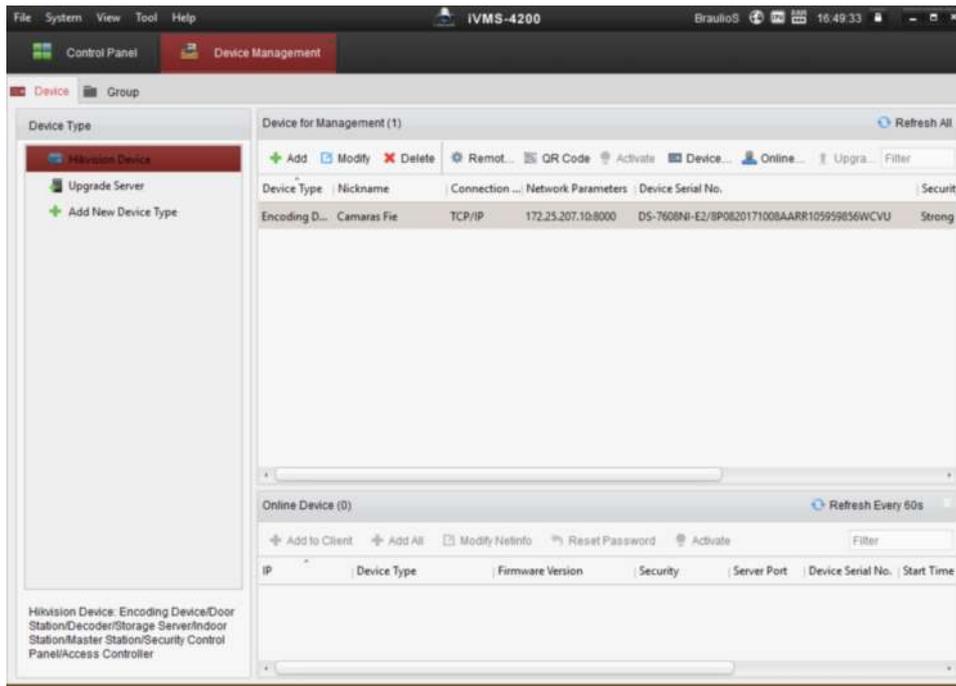


Figura 3-13: Registro del dispositivo NVR

Fuente: SARABIA, Braulio.2018

Con el dispositivo añadido correctamente, procedemos a dar click en la pestaña view y después en main view, y automáticamente se nos mostrara una pantalla en la cual se pueden observar las divisiones que en este caso vienen a ser las cámaras de seguridad que fueron añadidas en nuestro sistema de videovigilancia.

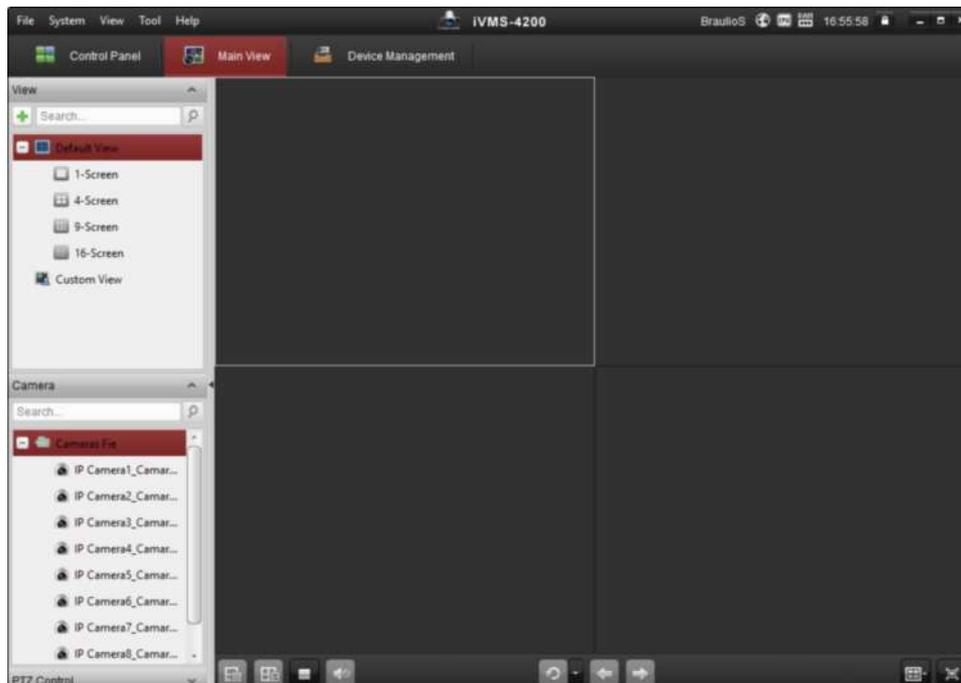


Figura 3-14: Numero de cámaras añadidas

Fuente: SARABIA, Braulio.2018

Para finalizar en la *figura 23-3* se puede observar ya el software en funcionamiento con el dispositivo y las cámaras añadidas.

En la imagen se puede ver que es nuestro sistema de seguridad ya que se muestran las imágenes del edificio nuevo de la FIE, tanto de la planta baja, primer piso, segundo piso, vista a la puerta principal y el parqueadero.

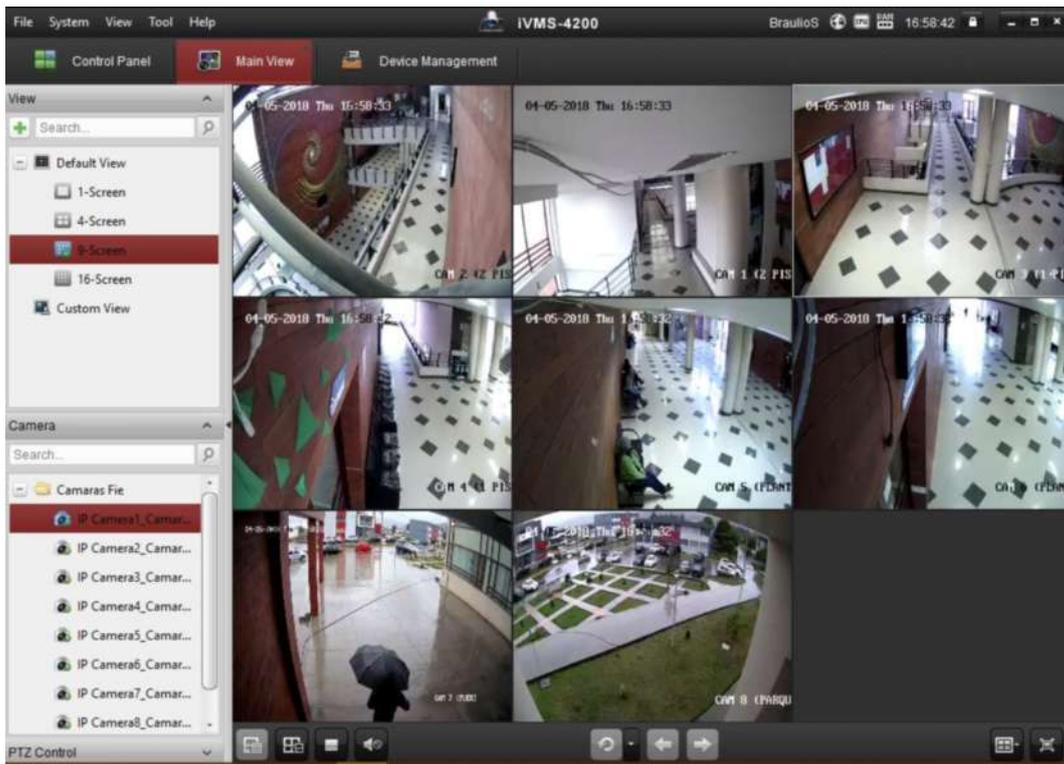


Figura 3-15: Software y cámaras en funcionamiento

Fuente: SARABIA, Braulio.2018

También podemos observar que las cámaras ya están en funcionamiento. En nuestro sistema se añadió 8 cámaras IP y como se ve en la figura se muestra 8 imágenes diferentes correspondientes a cada una de las cámaras.

3.2.6. Alimentación eléctrica

Con la finalidad de mantener la estética del edificio donde se implementó este sistema de seguridad, se optó por las cámaras IP que se mencionaron ya que entre una de sus principales características esta la del protocolo PoE (Power Over Ethernet).

El protocolo Power Over Ethernet en las cámaras tiene dos funciones principales, la primera que permite la transmisión de los datos y la segunda que permite que por medio del mismo cable se

pueda dotar de la alimentación eléctrica que necesitan las cámaras. El cable de red que se utilizó para la alimentación eléctrica fue el cable UTP categoría 6, y como se analizó en el apartado anterior se escogió este tipo de cable ya que presenta menor interferencia al momento de transmitir los datos en caso de que se necesite utilizar como cable de red.

Este protocolo PoE fue de mucha utilidad ya que no fue necesario hacer puntos eléctricos en el edificio y con esto no se dañó ni se modificó la infraestructura del edificio nuevo de la FIE.

Cabe señalar que dichos cables serán cubiertos con canaletas con la finalidad de mantener la estética del edificio.

3.3. Lugar estratégico para la ubicación de los equipos

Con los análisis que se realizó en los apartados anteriores se pudo escoger los lugares más precisos para la ubicación de cada uno de los equipos que comprenden este sistema de video vigilancia y los cuales se detallan a continuación.

Se debe tener muy en cuenta que en esta parte de la tesis los cables aún no están cubiertos con las canaletas, debido a que se debe realizar la configuración de cada cámara y así para que el sistema se ponga en marcha. Las canaletas cubrirán a los cables una vez que se haya realizado las pruebas del correcto funcionamiento del sistema y se las podrá visualizar en la parte de la instalación.

3.3.1. Ubicación de las cámaras

Uno de los objetivos más importantes de este sistema de video vigilancia es mantener seguros y con una visualización directa hacia la entrada principal del edificio de la FIE, parqueadero, entradas a las aulas y laboratorios. Con este objetivo y tomando en cuenta que el edificio consta de una planta baja y dos pisos, se ubicó las cámaras de la siguiente manera.

Con el estudio que se realizó anteriormente en la parte del análisis de la situación actual del edificio y su infraestructura y teniendo en cuenta todo este análisis se procedió elegir el lugar más adecuado para la ubicación de las cámaras.

En el interior del edificio se ubicó las cámaras de tipo domo y en las afueras del edificio se ubicó las cámaras de tipo bala, ya que son las más adecuadas para la intemperie.

3.3.1.1. Segundo Piso

Con la ayuda de dicho análisis y tomando en cuenta las secciones con las que cuenta este segundo piso del edificio, se ubicó dos cámaras que permiten tener una visualización directa a todas las entradas que son aulas, laboratorios y oficinas, así como también se tiene una vista directa a las gradas que son utilizadas por toda la gente que transcurre al edificio.

En este segundo piso del edificio se ubicaron 2 cámaras tipo domo fija.

3.3.1.2. Primer Piso

Con la ayuda de dicho análisis y tomando en cuenta las secciones con las que cuenta este primer piso del edificio, se ubicó dos cámaras que permiten tener una visualización directa a todas las entradas que son aulas, laboratorios y oficinas, así como también se tiene una vista directa a las gradas que son utilizadas por toda la gente que transcurre al edificio.

En este primer piso del edificio se ubicaron 2 cámaras tipo domo fija.

3.3.1.3. Planta Baja

Con la ayuda de dicho análisis y tomando en cuenta las secciones con las que cuenta esta planta baja del edificio, se ubicó dos cámaras que permiten tener una visualización directa a todas las entradas que son aulas, laboratorios y oficinas, así como también se tiene una vista directa a las gradas que se encuentran ubicadas tanto al lado derecho como al izquierdo de la puerta principal y que son utilizadas por toda la gente que transcurre al edificio.

En esta planta baja del edificio se ubicaron 2 cámaras tipo domo fija.

3.3.1.4. Afueras del edificio

La seguridad en el edificio de la FIE es muy importante tanto en el interior como el exterior de este, por tal razón también se procedió a ubicar 2 cámaras tipo bala cámaras en las afueras del edificio, cada cámara tiene su finalidad y su objetivo es mantener seguros y en un correcto estado todos los bienes de los estudiante, docentes y personas que visitan el edificio. Entre estos bienes están principalmente los vehículos de transporte, tanto de los docentes, alumno y de las personas en general que visitan o están de paso por el edificio.

3.3.2. *Ubicación de la central de monitoreo*

La oficina que se nos asignó para ubicar la central de monitoreo está ubicada en el segundo piso del edificio de la FIE, ya que en dicha ubicación yace la sala de servidores y en ella convergen todos los puntos de red de los equipos que manejan direccionamiento IP para la FIE. Cabe destacar que esta oficina está totalmente adecuada con las instalaciones eléctricas necesarias para la ubicación del servidor de video NVR (Grabador de video de red) y su monitor para la visualización de todo el sistema de seguridad de videovigilancia.

En esta oficina se ubicaron los siguientes equipos como son monitor, NVR, mouse, teclado y el disco duro que se instaló previamente en el NVR.



Figura 3-16: Central de monitoreo

Fuente: SARABIA, Braulio.2018

En la *figura 32-3* se puede apreciar como quedo ya la ubicación de todos los elementos necesarios para la monitorización del sistema de videovigilancia. Con la ubicación de todos los equipos necesarios para nuestro sistema de videovigilancia. Se procedió a la instalación de todos los componentes correspondiente para que nuestro sistema de seguridad empiece a funcionar y brinde la seguridad que necesita nuestro edificio de la FIE.

3.4. Diseño físico del sistema de video vigilancia

Con la ayuda de este diseño se pudo realizar un análisis físico de cada una de las conexiones entre los equipos que se van a utilizar en este sistema de videovigilancia, además se pudo identificar los puntos estratégicos donde serán ubicados cada uno de los elementos de este sistema. (Figura. 33-3)

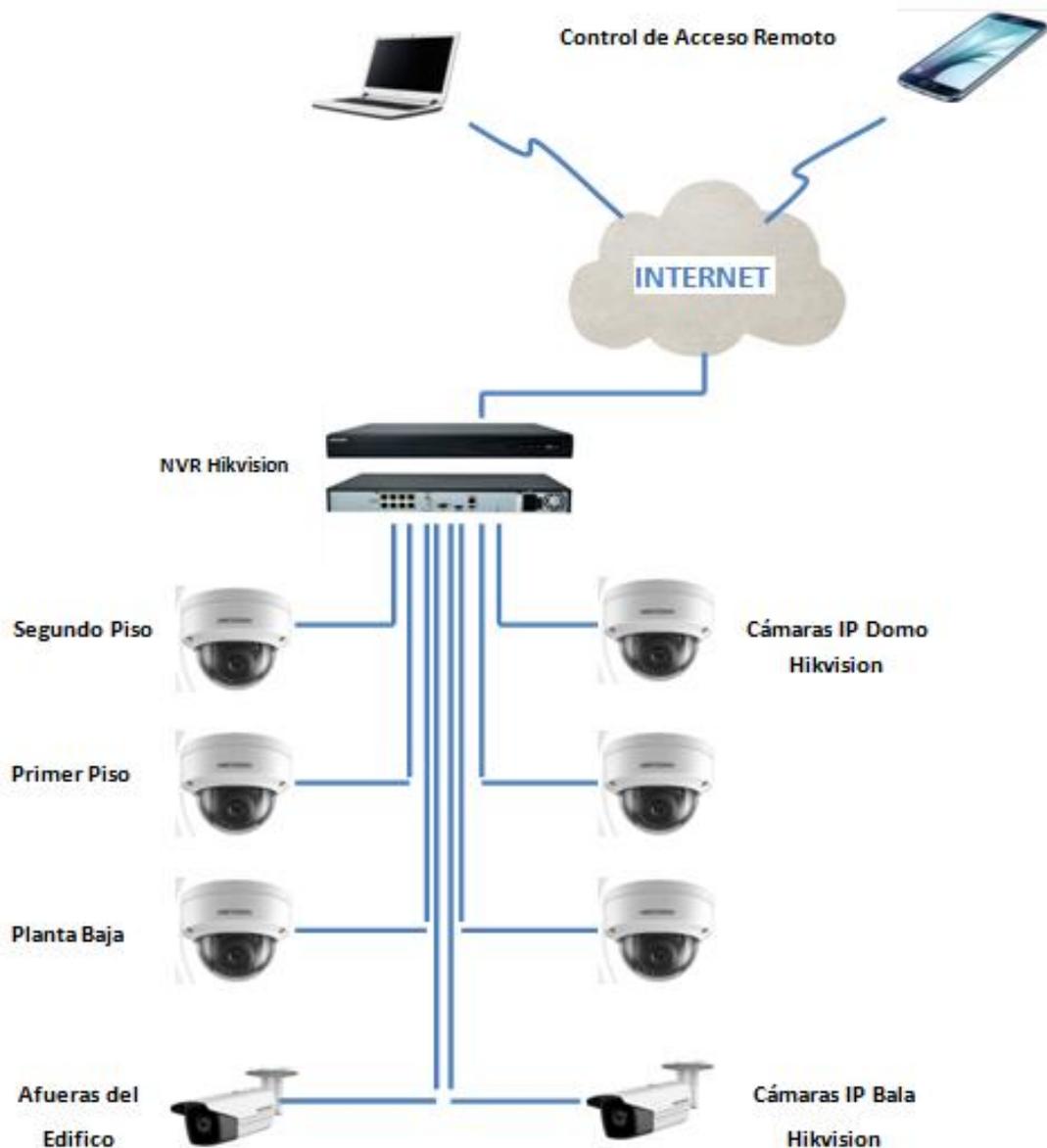


Figura 3-17: Diseño físico del sistema de video vigilancia

Fuente: SARABIA, Braulio.2018

Con la ayuda de este diseño y con los planos de la planta baja, primer y segundo piso de la infraestructura del edificio de la FIE, se pudo detallar claramente los lugares por donde se realizó la instalación de los equipos y el tendido de cables para la alimentación eléctrica.

Los planos (ver ANEXO A, ANEXO B, ANEXO C) sirvieron de referencia para calcular la cantidad de cable Ethernet que en este caso se utilizó para la alimentación de las cámaras IP y para la conexión desde el NVR hasta el puerto que fue asignado en el rack de los servidores que se encuentran en el tercer piso del edificio de la FIE.

Tabla 1-3: Longitud del cable desde las cámaras IP hasta el NVR

Descripción	Longitud (m)
Cámara 1 – Segundo piso	10
Cámara 2 – Segundo piso	35
Cámara 3 – Primer piso	20
Cámara 4 – Primer piso	30
Cámara 5 – Planta baja	25
Cámara 6 – Planta baja	35
Cámara 7 – Puerta principal	75
Cámara 8 – Parqueadero	45
Total	275

Realizado por: SARABIA, Braulio. 2018

Tabla 2-3: Longitud del cable desde el rack de servidores hasta el NVR

Descripción	Longitud (m)
Rack de servidores al NVR	10

Realizado por: SARABIA, Braulio. 2018

Se necesitará un total de **285 m** de cable de red, tanto para la conexión de la LAN y para alimentación de las cámaras IP y así poder tener comunicación con todos los equipos del sistema de videovigilancia.

3.5. Diseño lógico del sistema de video vigilancia

Mediante este diseño y como se puede ver en la *figura 34-3*, podemos apreciar la forma en la que está estructurada la red de videovigilancia, en la cual las cámaras IP se comunican con el NVR mediante una red local y el NVR transmite toda la información a través de la red de internet de la institución hacia los distintos servidores.

La comunicación de las cámaras IP con el NVR fue mediante las direcciones IP que fueron otorgadas por el departamento de DESITEL, gracias al oficio que fue enviado previamente.

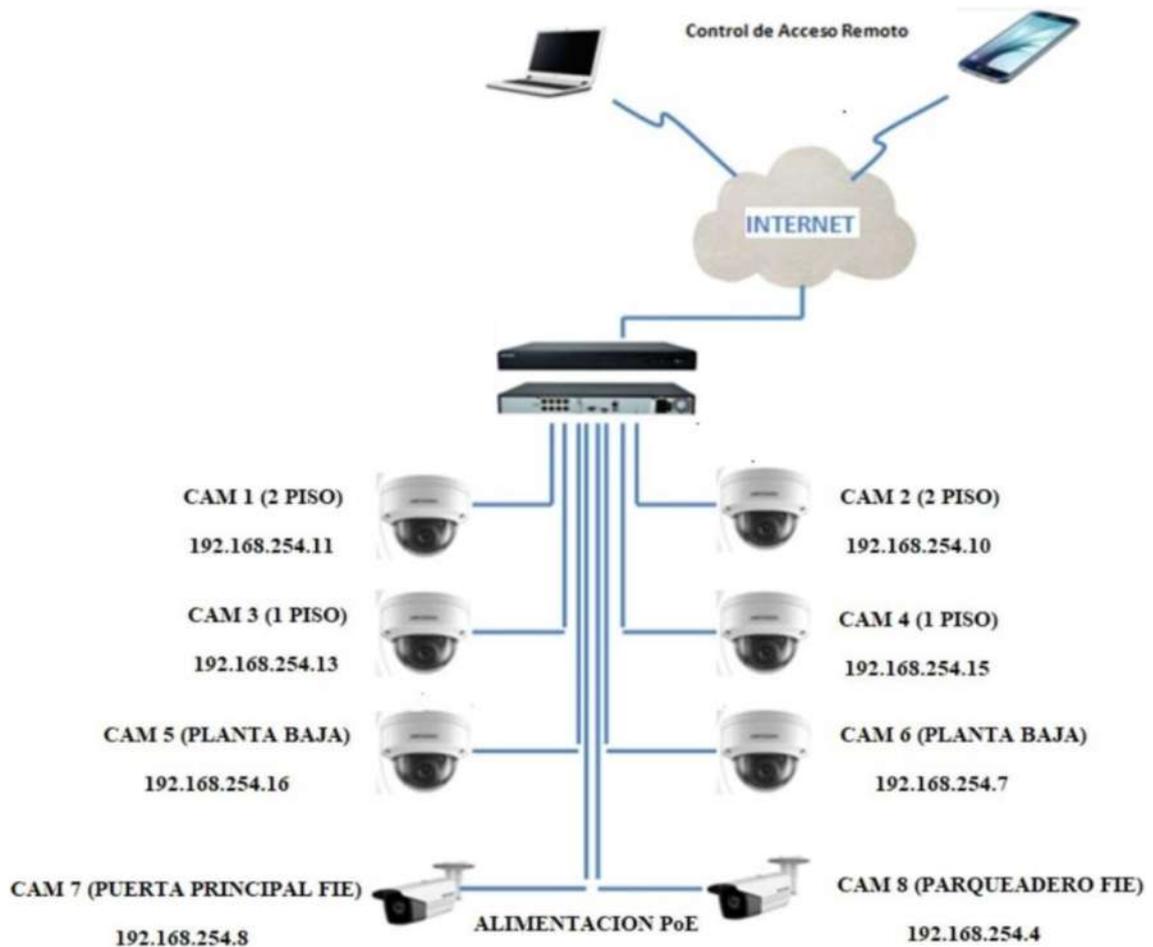


Figura 3-18: Diseño lógico del sistema de video vigilancia
Fuente: SARABIA, Braulio.2018

En esta grafica se puede observar que cada cámara IP tiene su propia dirección IP que es única, como también el NVR tiene su dirección IP para poder conectarse a internet y así poder tener una comunicación entre todos los elementos de este sistema de videovigilancia.

Cabe destacar que en la figura no se detalló la dirección IP del dispositivo NVR, ya que por seguridad del sistema no se agregó esta dirección IP.

3.6. Implementación del sistema de video vigilancia

3.6.1. Tendido de cables para la alimentación eléctrica

La alimentación eléctrica para las cámaras IP es indispensable, con la finalidad de mantener la estética del edificio no se realizaron puntos eléctricos. Una de las grandes ventajas que presenta nuestro grabador de video en red (NVR) es la utilización del protocolo Power Over Ethernet (PoE) que además de servir para el transporte de datos en la red, también tiene la funcionalidad de pasar alimentación eléctrica por el mismo cable UTP (Categoría 6).

Para las 8 cámaras IP se utilizó el cable UTP para brindar la alimentación eléctrica a las cámaras. En la *figura 35-3* se puede apreciar el tendido del cable.



Figura 3-19: Tendido de cable para alimentación eléctrica

Fuente: SARABIA, Braulio.2018

Con la finalidad de no desperdiciar el cable se compró un cartón de 300 m de cable UTP categoría 6, se procedió al tendido de cables desde el NVR hasta cada una de las cámaras IP. Como se puede apreciar en la figura el cable se lo sostuvo con grapas metálicas. Este procedimiento se realizó para cada una de las cámaras IP que se instalaron en nuestro sistema de videovigilancia.

Una vez que se tuvo la longitud del cable para cada cámara IP, se procedió a ponchar el extremo de cada uno de los cables para luego comprobar su funcionamiento ya conectado al NVR

3.6.2. *Instalación y visualización de cada cámara IP*

Las cámaras IP fueron instaladas en los lugares estratégicos que se analizó anteriormente, fueron colocadas y aseguradas con tornillos a la loza de cada piso del edificio. Posteriormente se realizó la conexión del cable UTP para la alimentación eléctrica y así tener ya su visualización en tiempo real.

3.6.2.1. *Segundo Piso*

Cámara 1



Figura 3-20: Instalación de la cámara 1, segundo piso
Fuente: SARABIA, Braulio.2018



Figura 3-21: Visualización de la cámara 1, segundo piso
Fuente: SARABIA, Braulio.2018

Cámara 2



Figura 3-22: Instalación de la cámara 2, segundo piso
Fuente: SARABIA, Braulio.2018



Figura 3-23: Visualización de la cámara 2, segundo piso
Fuente: SARABIA, Braulio.2018

3.6.2.2. Primer Piso

Cámara 3



Figura 3-24: Instalación de la cámara 3, primer piso
Fuente: SARABIA, Braulio.2018



Figura 3-25: Visualización de la cámara 3, primer piso
Fuente: SARABIA, Braulio.2018

Cámara 4



Figura 3-26: Instalación de la cámara 4, primer piso
Fuente: SARABIA, Braulio.2018

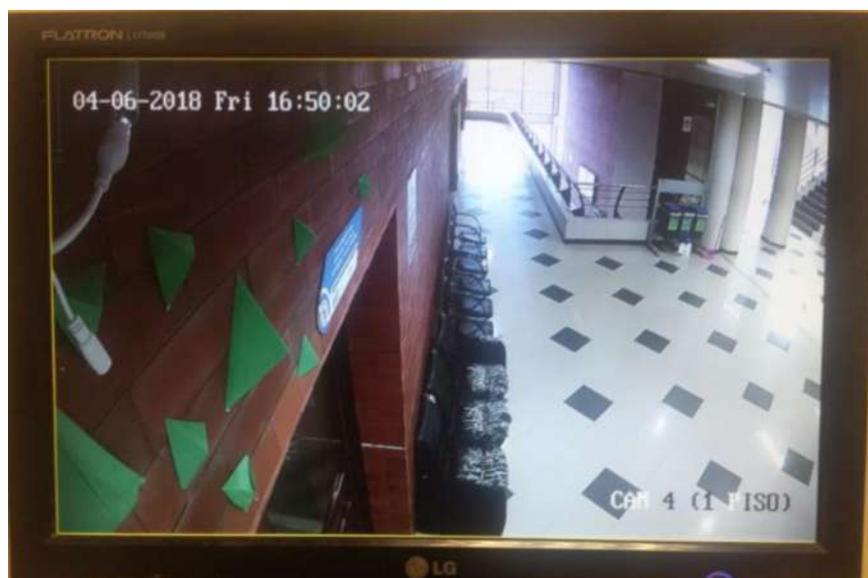


Figura 3-27: Visualización de la cámara 4, primer piso
Fuente: SARABIA, Braulio.2018

3.6.2.3. Planta Baja

Cámara 5



Figura 3-28: Instalación de la cámara 5, planta baja
Fuente: SARABIA, Braulio.2018

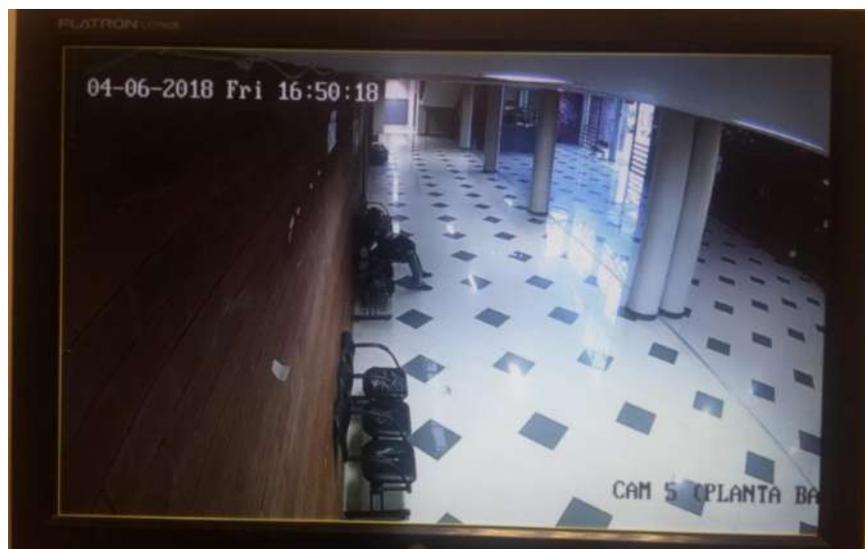


Figura 3-29: Visualización de la cámara 5, planta baja
Fuente: SARABIA, Braulio.2018

Cámara 6



Figura 3-30: Instalación de la cámara 6, planta baja
Fuente: SARABIA, Braulio.2018



Figura 3-31: Visualización de la cámara 6, planta baja
Fuente: SARABIA, Braulio.2018

3.6.2.4. Afueras del edificio

Cámara 7



Figura 3-32: Instalación de la cámara 7, puerta principal FIE
Fuente: SARABIA, Braulio.2018



Figura 3-33: Visualización de la cámara 7, puerta principal FIE
Fuente: SARABIA, Braulio.2018

Cámara 8

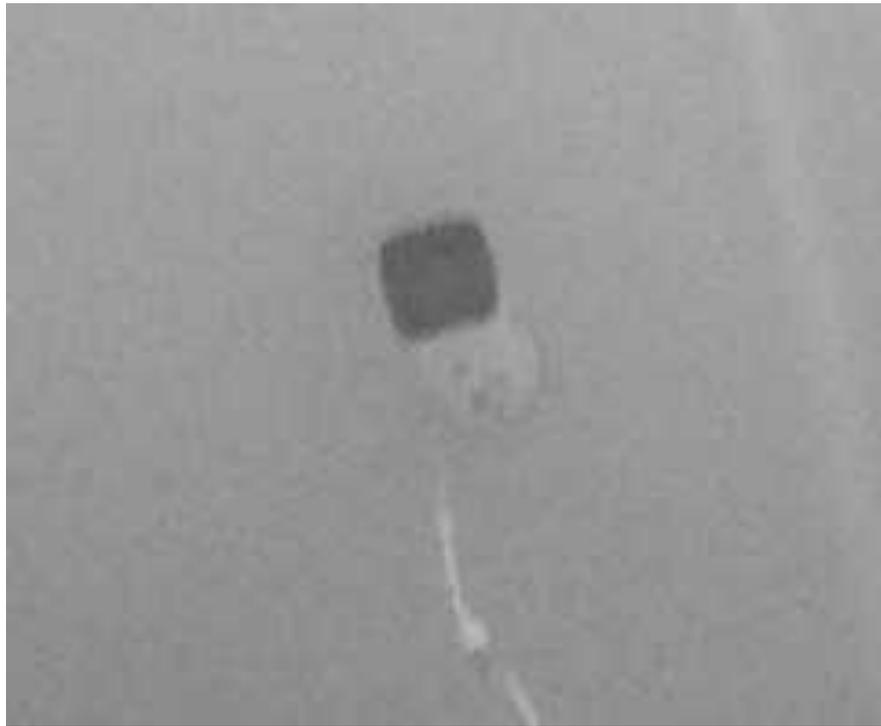


Figura 3-34: Instalación de la cámara 8, parqueadero
Fuente: SARABIA, Braulio.2018

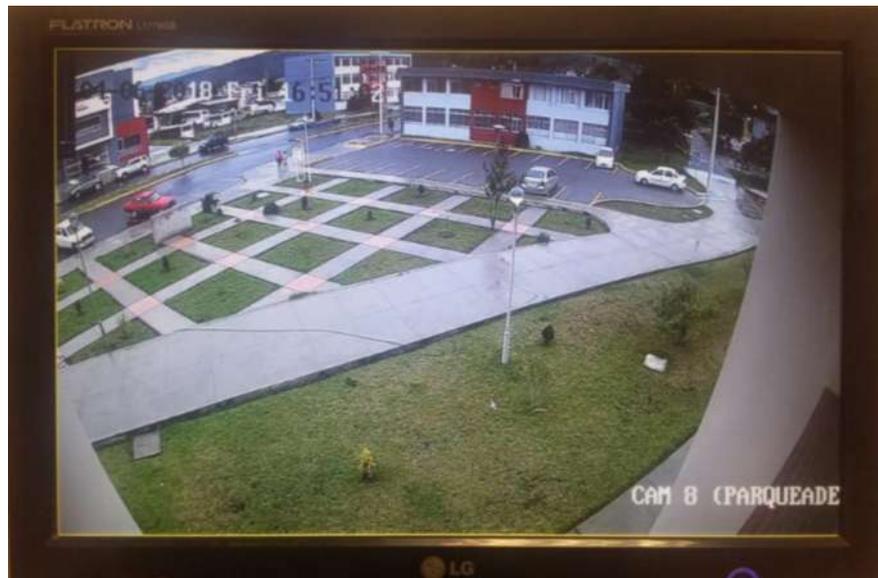


Figura 3-35: Visualización de la cámara 8, parqueadero
Fuente: SARABIA, Braulio.2018

3.6.3. *Instalación y visualización del servidor NVR*

El dispositivo de grabación de video en red (NVR) fue colocado en la sala de servidores juntamente con el monitor, mouse y teclado, teniendo así nuestra central de monitoreo. Para la conexión a internet del NVR se utilizó el puerto en los servidores, que el departamento de DESITEL nos asignó para nuestro sistema de videovigilancia.



Figura 3-36: Central de monitoreo
Fuente: SARABIA, Braulio.2018



Figura 3-37: Visualización del sistema de videovigilancia
Fuente: SARABIA, Braulio.2018

3.6.4. *Instalación de las canaletas*

Una vez que se realizó la conexión entre los equipos de nuestro sistema de videovigilancia y se verificó su correcto funcionamiento se procedió a colocar las canaletas que cubrirán los cables de alimentación, manteniendo así la estética del edificio nuevo de la FIE.



Figura 3-38: Instalación de las canaletas 2 piso
Fuente: SARABIA, Braulio.2018



Figura 3-39: Instalación de las canaletas 1 piso
Fuente: SARABIA, Braulio.2018



Figura 3-40: Instalación de las canaletas planta baja
Fuente: SARABIA, Braulio.2018



Figura 3-41: Instalación de las canaletas exterior del edificio
Fuente: SARABIA, Braulio.2018

3.6.5. *Instalación del logotipo de grabación*

Con la finalidad de que todas las personas tengan conocimiento de que las instalaciones tanto interior como exterior del edificio están siendo vigiladas, se realizó un diseño apropiado para nuestro sistema de videovigilancia. Este logotipo creara un efecto disuasorio en el caso de llegar a ocurrir algún daño a las instalaciones del edificio o las personas que se encuentran ahí, también servirá para prevenir actos ilícitos dentro o fuera del edificio.



Figura 3-42: Logotipo de seguridad de nuestro sistema de videovigilancia
Fuente: SARABIA, Braulio.2018

3.7. Configuración de los equipos

Una vez que se instalaron los equipos del sistema de videovigilancia, se procede a configurar cada uno de los equipos para que nuestro sistema ya quede en completo funcionamiento.

3.7.1. Configuración del NVR a la plataforma Hik-Connect

Hik-Connect es el servicio adicional de P2P y HDDNS para todos los equipos Hikvision, esta plataforma permite acceder a los dispositivos de videovigilancia ya sean analógico e IP por medio de Smartphone y PC.

Por medio de nuestro navegador ingresamos a la página de Hik-Connect, en la *figura 60-3* nos muestra la ventana principal de Hikvision y damos click en registrarse.



Figura 3-43: Ventana principal Hikvision
Fuente: SARABIA, Braulio.2018

Como se puede apreciar en la *figura 61-3* debemos llenar algunos campos que son obligatorios para el registro.

Figura 3-44: Registro en Hikvision
Fuente: SARABIA, Braulio.2018

Luego de habernos registrado nos dirigirá a una ventana como se ve en la *figura 62-3* en la cual ya podemos añadir nuestro dispositivo NVR.

Device Domain	Device Serial No.	IP/Port No.	Status	Device Operation
No device.				

Figura 3-45: Vinculo para añadir dispositivo
Fuente: SARABIA, Braulio.2018

Una vez que estemos en esta ventana damos click en add y nos mostrara una ventana como se ve en la *figura 63-3*, en la cual nos pide los datos como el número de serie y la verificación del código para añadir el dispositivo NVR, una vez que ingresemos estos datos automáticamente nuestro dispositivo se mostrara ya añadido y en línea ver *figura 64-3*.

Figura 3-46: Registro del dispositivo NVR
Fuente: SARABIA, Braulio.2018

Alias	Device Domain	Device Serial No.	IP/Port No.	Status	Device Operation
			/80	Online	[Edit] [Delete] [Refresh] [Reset]

Figura 3-47: Vista del dispositivo en línea
Fuente: SARABIA, Braulio.2018

Por seguridad de nuestro sistema se han borrado los datos más importantes en la *figura 64-3*, pero como podemos apreciar nuestro dispositivo está en online (letras verdes).

Una vez que nuestro dispositivo este en línea procederemos a la configuración de cada uno de los equipos de nuestro sistema de videovigilancia.

3.7.2. Configuración del NVR

Para la configuración de nuestro dispositivo NVR ingresamos a configuración del sistema y procedemos a realizar la configuración según los requerimientos de nuestro sistema. En la *figura 65-3* se muestra los parámetros que se configuraron en nuestro dispositivo NVR, como configuración general, configuración general de la red, configuración de acceso a la plataforma.

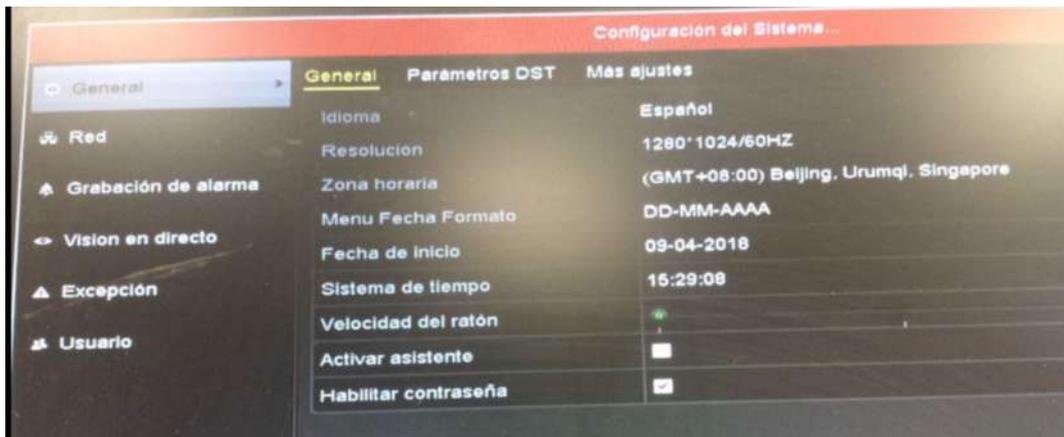


Figura 3-48: Configuración general del Sistema de videovigilancia
Fuente: SARABIA, Braulio.2018



Figura 3-49: Configuración del NVR a la LAN
Fuente: SARABIA, Braulio.2018

En la *figura 66-3* se realizó la configuración del NVR para que tenga acceso a internet, mediante la dirección IP que nos asignaron por parte del departamento de DESITEL y pero por seguridad de nuestro sistema de videovigilancia se han borrado los datos, para así poder proteger nuestro sistema.

Se puede apreciar en la *figura 67-3* que luego de haber configurado nuestro dispositivo NVR con los requerimientos necesarios y correctos, ya se puede ver que nuestro dispositivo está en línea, por seguridad se ha borrado nuestro código de verificación.



Figura 3-50: Acceso a la plataforma, dispositivo en línea
Fuente: SARABIA, Braulio.2018

3.7.3. Configuración de las cámaras IP

La configuración de cada una de las cámaras IP se realizó con las direcciones IP que fueron otorgadas por DESITEL.

3.7.3.1. Detección de las Direcciones IP para cada cámara

Las direcciones IP que fueron asignadas por el departamento de DESITEL, se las agrego a los dispositivos de la siguiente manera:

NVR	xxx.xx.xxx.xx
CAM 1 (2 PISO)	192.168.254.11
CAM 2 (2 PISO)	192.168.254.10
CAM 3 (1 PISO)	192.168.254.13
CAM 4 (1 PISO)	192.168.254.15
CAM 5 (PLANTA BAJA)	192.168.254.10
CAM 6 (PLANTA BAJA)	192.168.254.7
CAM 7 (PUERTA PRINCIPAL FIE)	192.168.254.8
CAM 8 (PARQUEADERO FIE)	192.168.254.4

Por seguridad de nuestro sistema no se dio a conocer la dirección de nuestro dispositivo, ya que mediante esta dirección se realiza el proceso de visualización por acceso remoto.

3.7.3.2. Configuración de cámaras IP tipo Domo y tipo Bala

Para una mejor visualización de nuestro sistema y saber cuál cámara está en el primer piso o en el segundo piso se configuro o se las nombro de la siguiente manera.

Lo que debemos hacer es ingresar al menú principal del sistema y luego en la pestaña cámaras y luego en la configuración OSD y realizamos la configuración correspondiente. En la *figura 68-3* se muestra un ejemplo de la manera en que se configuro cada una de las cámaras para saber reconocerlas por su nombre, este procedimiento se realizó para las 8 cámaras IP,



Figura 3-51: Configuración de cada cámara IP

Fuente: SARABIA, Braulio.2018

También se puede realizar la configuración del ajuste de las imágenes como se ve en la *figura 69-3*, así como también en la *figura 70-3* se puede tener una visualización de como las cámaras IP realizan la detección de movimiento que se está sucediendo en el edificio de la FIE.

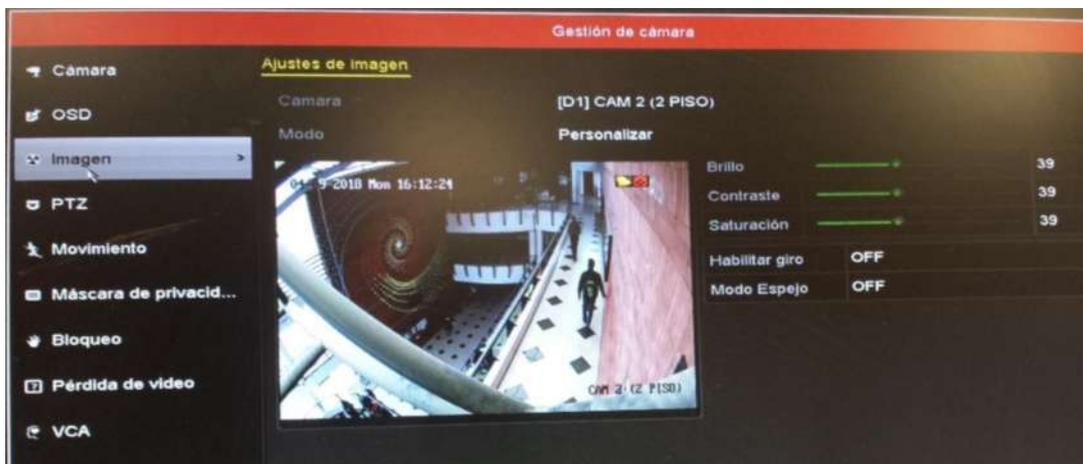


Figura 3-52: Ajustes de imagen de cada cámara IP

Fuente: SARABIA, Braulio.2018



Figura 3-53: Detección de movimiento de cada cámara IP
Fuente: SARABIA, Braulio.2018

Una vez que se realizó la configuración de cada una de las cámaras IP con sus respectivas direcciones IP y su configuración general. El sistema nos muestra la configuración general de todas las cámaras, como lo podemos ver en la *figura 71-3* se detalla la configuración de cada cámara IP.

Nombre de cám...	Protocolo	Modelo de dispositivo	Puerto pri...	N° de serie	Firmware
CAM 2 (2 PISO)	HIKVISION	DS-2CD1121-I	8000	DS-2CD1121-I2...	V5.4.5 build 170123
CAM 1 (2 PISO)	HIKVISION	DS-2CD1121-I	8000	DS-2CD1121-I2...	V5.4.5 build 170123
CAM 3 (1 PISO)	HIKVISION	DS-2CD1121-I	8000	DS-2CD1121-I2...	V5.4.5 build 170123
CAM 4 (1 PISO)	HIKVISION	DS-2CD1121-I	8000	DS-2CD1121-I2...	V5.4.5 build 170123
CAM 5 (PLANT...	HIKVISION	DS-2CD1121-I	8000	DS-2CD1121-I2...	V5.4.5 build 170123
CAM 7 (PUERT...	HIKVISION	DS-2CD1041-I	8000	DS-2CD1041-I2...	V5.5.0 build 170725
CAM 8 (PARQU...	HIKVISION	DS-2CD1021-I	8000	DS-2CD1021-I2...	V5.4.5 build 170123

Figura 3-54: Configuración general de las cámaras IP
Fuente: SARABIA, Braulio.2018

- Cámara 1 (2 Piso)
- Cámara 2 (2 Piso)
- Cámara 3 (1 Piso)
- Cámara 4 (1 Piso)
- Cámara 5 (Planta Baja)
- Cámara 6 (Planta Baja)
- Cámara 7 (Puerta Principal FIE)
- Cámara 8 (Parqueadero FIE)

3.7.4. Conexión entre el NVR y las cámaras IP

Una vez que se haya finalizado las configuraciones necesarias y con los requerimientos que se desean para que nuestro sistema de seguridad mediante videovigilancia, la conexión entre el NVR y las cámaras IP se dará automáticamente, esto quiere decir que se podrá visualizar ya en tiempo real lo que está sucediendo en las instalaciones del edificio de la FIE ya sea en la parte interna como externa del edificio.

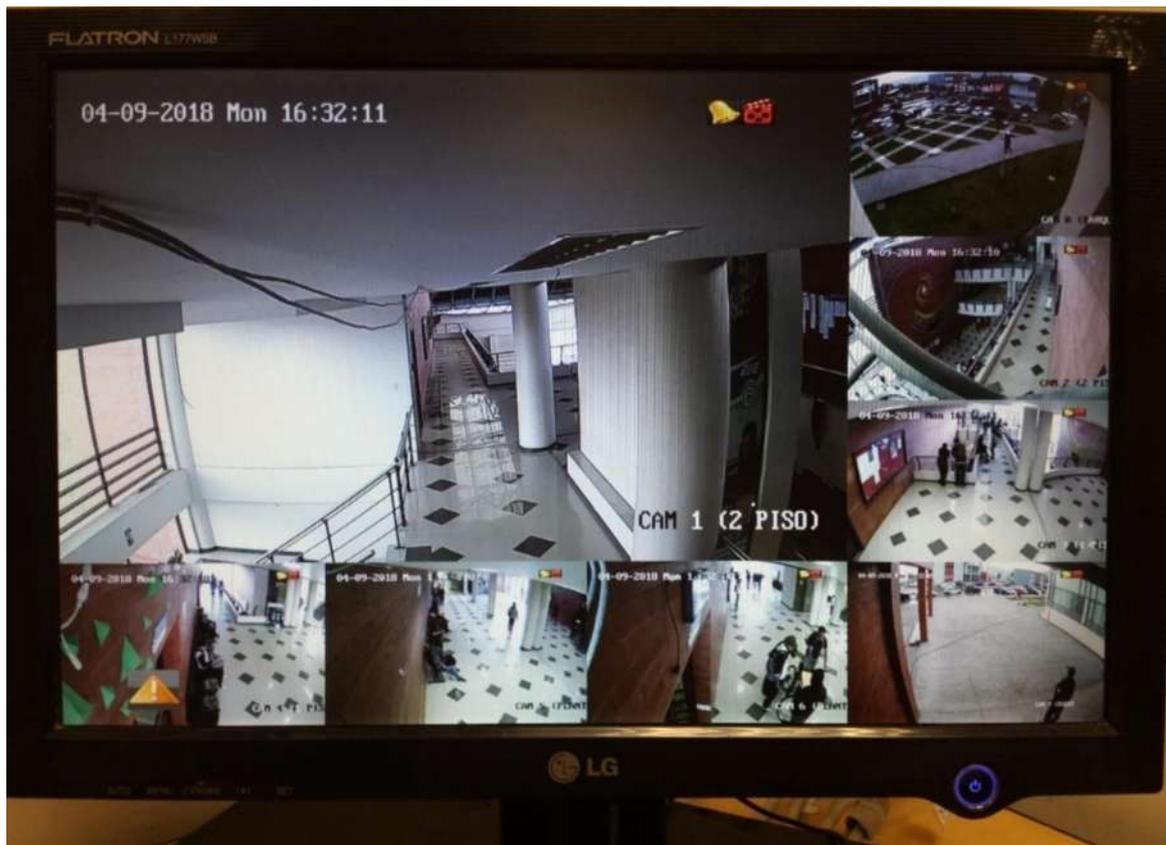


Figura 3-55: Funcionamiento del sistema de videovigilancia

Fuente: SARABIA, Braulio.2018

En la *figura 73-3* se puede observar en nuestro monitor que ya las 8 cámaras IP están funcionando correctamente y están grabando en tiempo real.

Como se puede apreciar el monitor muestra 8 diferentes imágenes, cada imagen corresponde a cada cámara que se instaló en el edificio. Con la instalación estas 8 cámaras IP el edificio de la FIE tendrá mayor seguridad y confort para todas las personas.

3.7.5. Configuración de la alimentación eléctrica por medio de PoE

Como se mencionó anteriormente el protocolo (Power Over Ethernet) PoE, se utilizó para dar alimentación eléctrica a las cámaras IP.

Su configuración solo se basó en conectar los cables UTP a cada uno de los canales en los que se configuro y mediante esta conexión ya se tenía alimentadas a las cámaras IP.

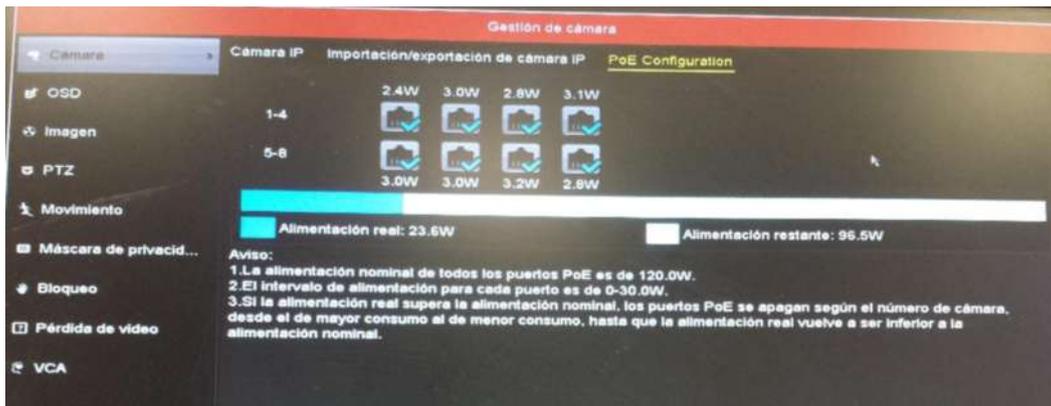


Figura 3-56: Alimentación eléctrica de las cámaras, por medio del protocolo PoE

Fuente: SARABIA, Braulio.2018

3.7.6. Configuración para la grabación de los videos

En los sistemas de video vigilancia tener un respaldo de lo que sucede en el transcurso de los días es muy importante, por eso es necesario que nuestro sistema funcione las 24 horas al día y los 7 días a la semana y que realice su correspondiente grabación.

Para esto debemos entrar a la ventana principal de nuestro sistema, luego en la pestaña configuración de grabación y damos click en programación. En nuestro caso y para que nuestro sistema tenga más tiempo de duración en el almacenamiento.

El tipo de grabación se configuro solo cuando haya movimiento como se puede ver en la figura 75-3, el color verde me indica que las cámaras IP grabaran solo cuando exista movimiento, cabe destacar que este procedimiento se realizó para todas las cámaras IP.



Figura 3-57: Tipo de grabación del video

Fuente: SARABIA, Braulio.2018

En la *figura 76-3* se puede ver los parámetros generales de la grabación del video, entre estos parámetros están tipo de codificación del video, tasa de bits, resolución y la calidad del video.

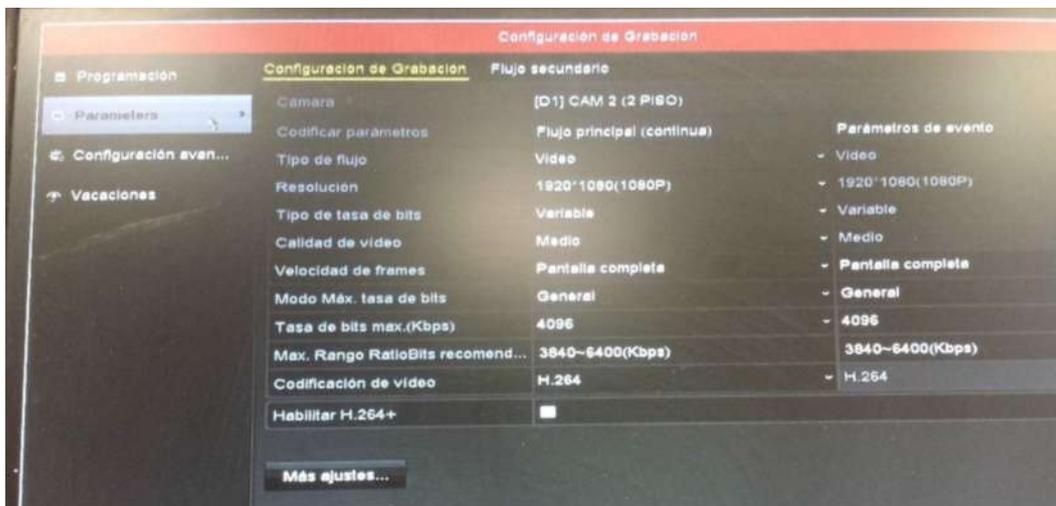


Figura 3-58: Parámetros generales de grabación del video

Fuente: SARABIA, Braulio.2018

3.8. Cálculo del almacenamiento para nuestro sistema de video vigilancia

3.8.1. Ancho de banda del sistema

En este sistema de video vigilancia las cámaras necesitarán un ancho de banda que están en el rango de 32 kbps a 8 Mbps, esto va a depender de la configuración que se realice en el NVR según sean las necesidades del usuario y dependerá mucho en la manera en la que desea visualizar sus videos o imágenes.

En nuestro sistema de video vigilancia se utilizó 1 NVR de 8 canales y con 8 cámaras IP con los siguientes datos:

NVR= 50 Mbps ancho de banda entrante

Número de canales = 8

Por medio de estos datos podemos obtener el valor del ancho de banda que necesitara cada cámara.

BW= 50 Mbps / 8 canales = 6.25 Mbps

Por lo tanto, cada cámara va a necesitar un ancho de banda de 6.25 Mbps, este valor nos indica que la calidad de la imagen y video será alta y la que se necesita para que el flujo de datos sea normal de manera local.

Para una visualización en tiempo real de manera remota va a depender mucho de la conexión a internet, ya que de lo contrario si se podrá visualizar, pero vamos a tener retraso en las imágenes.

3.8.2. Cálculo del almacenamiento

Para el cálculo del almacenamiento se utilizará una calculadora en línea **Stardot Technologies** es una herramienta muy utilizada en el cálculo del almacenamiento. La cantidad de almacenamiento dependerá mucho de la calidad en la que se desea observar, en base al estándar a utilizar la resolución y los fotogramas por segundo.

Para el cálculo del almacenamiento de nuestro sistema se realizó con los siguientes datos:

Estándar = H.264

Fps = 30 fps

Tiempo de almacenamiento = 22 días laborables sin fines de semana (1 mes)

En la *figura 76-3* se puede observar los datos calculados para la capacidad de almacenamiento de nuestro sistema de video vigilancia.

Stream Type:	<input type="radio"/> MJPEG <input checked="" type="radio"/> H.264	
Resolution:	<input type="radio"/> D1 (704x480) <input checked="" type="radio"/> 720P HD <input type="radio"/> 1080P HD	<input type="radio"/> 1.3 Megapixel <input type="radio"/> 3 Megapixel <input type="radio"/> 5 Megapixel <input type="radio"/> 10 Megapixel
Video Quality:	<input type="radio"/> Low <input checked="" type="radio"/> Medium <input type="radio"/> High	
Average Frame Size:	16 KB	
Number of Cameras:	8	
Frame Rate per Camera:	30 FPS	
Hours of Motion:	12 Hours a Day	
Storage in Days (per camera):	22	
Total Bandwidth:	30.7 Mbps	
Average Bandwidth per Camera:	3.8 Mbps	
Estimated Storage:	3.6 TB	

Figura 3-59: Capacidad de almacenamiento de nuestro sistema de video vigilancia
 Fuente: SARABIA, Braulio.2018

Algo muy importante que debemos tener en cuenta es que este método de cálculo no tienen en cuenta el tipo de grabación, esto quiere decir que esta calculadora toma la grabación como continua y por eso es el resultado de 3.6 TB.

Pero nuestro sistema está con la configuración para que las cámaras graben solo cuando detecten movimiento, este es un factor muy importante que influye de una manera alta en el tamaño del almacenamiento.

Nuestro sistema de seguridad cuenta con un disco duro de 1 TB, capacidad que abarcara para los 22 días de almacenamiento, ya que no se toma en cuenta los fines de semana ya que la facultad pasa cerrada, este es otro factor más a tomar en cuenta. Por lo que en nuestro sistema será suficiente el disco duro de 1 TB para el almacenamiento, se debe tomar en cuenta también que el dispositivo NVR es apilable, esto quiere decir que se puede acoplar otro disco duro de mayor o igual capacidad, además, cuenta con un dispositivo NVR de 8 canales y con un ancho de banda entrante de 50Mbps y como se puede apreciar en la figura 76-3 el total del ancho de banda es de 30.7 Mbps, con estos datos obtenidos podemos darnos cuenta de que nuestro

sistema de seguridad está funcionando correctamente ya que tenemos un ancho de banda entrante suficiente para que el sistema de seguridad trabaje con normalidad.

3.9. Pruebas de funcionamiento

Para la comprobación de nuestro sistema de videovigilancia se procedió a ingresar nuestro dispositivo NVR (Grabador de Video en Red) y a la aplicación IVMS-4200, mediante la cual se realizó la monitorización remota de las instalaciones de la FIE, mediante esta aplicación se realizó un control del desempeño y funcionamiento correcto de nuestro sistema de seguridad.

Para poder ingresar a nuestro servidor NVR es necesario ingresar el patrón de seguridad, ya que para mayor seguridad de mantener protegido nuestro sistema aparte de ingresar usuario y contraseña también se lo configuro para que se ingrese el patrón de seguridad. Cabe destacar que estos datos solo los tendrán la persona que vaya a estar a cargo de este sistema.

A continuación, se detallan: el estado del servidor NVR y de las aplicaciones necesarias para el control de nuestro sistema mediante monitorización remota.

- **Grabador de Video en Red (NVR).** - Ingresando a nuestro servidor NVR se pudo constatar que nuestro sistema se encuentra funcionando de manera correcta según los requerimientos que se configuro, también se comprobó las funciones necesarias y están trabajando correctamente.



Figura 3-60: Sistema de video vigilancia, visto desde NVR
Fuente: SARABIA, Braulio.2018

- **Almacenamiento y grabación de videos.** – Una de las pruebas de funcionamiento que se realizó también fue la ver los videos almacenados y guardados en el disco duro, en la *figura 78-3* se puede ver que las 6 de las 8 cámaras IP están en mostrando imágenes que fueron grabadas, y las 2 cámaras restantes no muestran nada ya que la configuración de las cámaras IP se realizó para que graben solamente cuando detecten algún movimiento.

Con este análisis se llega a la conclusión de que nuestro sistema de videovigilancia si está funcionando correctamente y con los requerimientos con los cuales fueron configurados los equipos.



Figura 3-61: Videos almacenados y grabados

Fuente: SARABIA, Braulio.2018

También se puede apreciar los cuadritos de color rojo, esto significa que las cámaras se encuentran grabando ya 9 días. Las grabaciones también se las puede extraer y tener almacenados en un disco duro aparte, esto con la finalidad de tener almacenados estos videos ya sean de mucha importancia para la Facultad.

- **IVMS-4200.-** Para acceder a la aplicación se debe ingresar mediante el usuario y la contraseña con la que se registró el dispositivo, una vez que se ingresó se observó que la interfaz de la aplicación está trabajando normalmente, también se procedido a ingresar a diferentes funciones y se verifico que todo está funcionando correctamente.

- **Visualización en directo.** - Ingresando a la aplicación se pudo constatar que nuestro sistema está en correcto funcionamiento y se observó que verdaderamente las cámaras están grabando en tiempo real, la calidad de la imagen es buena y todas las funciones que requiere nuestro sistema están activas y funcionando de manera correcta, además los videos se almacenan directamente en el disco, ya que es un sistema operativo dedicado a control de cámaras IP.



Figura 3-62: Sistema de video vigilancia, visto desde IVMS-4200
Fuente: SARABIA, Braulio.2018

3.10. Costos

3.10.1. Costos Directos

Tabla 3-3: Costos directos del sistema de video vigilancia

Cantidad	Descripción	Valor Unitario	Valor Total
8	Cámaras Domo	135	810
2	Cámaras Bala	95	190
1	NVR con PoE	220	220
1	Disco Duro	100	100
1	Cartón de cable UTP cat. 6	195	195
Total			1515

3.10.2. Costos indirectos

Tabla 4-3: Costos indirectos del sistema de video vigilancia

Cantidad	Descripción	Valor Unitario	Valor Total
15	Conectores RJ-45	0.15	2.25
15	Capuchones para conectores RJ-45	0.10	1
40	Canaletas	1.10	44
1	Broca de 6 mm x 100 mm	2	2
1	Broca de 13 mm x 330 mm	12	12
2	Fundas de grapas metálicas (100 c/u)	1.70	3.40
Total			64.65

3.10.3. Costos totales

Tabla 5-3: Costos totales del sistema de video vigilancia

Descripción	Cantidad
Costos Directos	1515
Costos Indirectos	64.65
Costo Total	1579.65

CONCLUSIONES

- El edificio nuevo de la Facultad de Informática y Electrónica no contaba con un sistema de seguridad motivo por el cual se decidió realizar este proyecto de tesis, el sistema de seguridad que se implemento con cámaras IP es la mejor opción que se eligió con la finalidad de mantener resguardados los equipos e instalaciones del edificio nuevo de la FIE.
- Con el análisis que se realizo de los sistemas de seguridad mediante video vigilancia, se determino que el sistema de seguridad mediante videovigilancia con cámaras IP presenta mejores prestaciones para el edificio de la FIE y brindara la seguridad tanto en la parte interna como externa del edificio.
- Con la finalidad de tener un sistema de seguridad mediante video vigilancia confiable, se procedió a realizar un análisis completo de las áreas o lugares más estratégicos para la ubicación de los equipos; dichos equipos fueron elegidos según sus prestaciones y mejores características y que sean los adecuados para nuestro sistema.
- Una vez elegidos todos los lugares, equipos y componentes para nuestro sistema de seguridad mediante videovigilancia se procedió a la instalación de todos los equipos finalizando así la etapa de implementación.
- Para garantizar la correcta funcionalidad del sistema de video vigilancia, se realizaron las pruebas correspondientes, como son la conexión entre el dispositivo NVR y las cámaras IP, así también la visualización en directo de todas las cámaras IP ya sea de manera local o remota llegando a la conclusión de que nuestro sistema está en correcto funcionamiento.

RECOMENDACIONES

- Para un correcto funcionamiento del sistema de seguridad mediante video vigilancia, se procederá a dar a conocer a la persona quien va a estar a cargo de la monitorización del sistema todos los parámetros necesarios para que pueda acceder y monitorizar este sistema, quedando así en su totalidad responsable de los videos y grabaciones así como también quedara a cargo de la monitorización para mantener vigiladas las instalaciones del edificio nuevo de la FIE.
- Con el fin de no violar el derecho a la intimidad personal se deberá informar del sistema de seguridad mediante video vigilancia implementado y así se respetara el derecho de todas las personas que ingresan a las instalaciones del edificio de la FIE que están siendo monitoreadas.
- Este sistema de seguridad de video vigilancia solo será utilizado para mantener resguardadas las instalaciones y los equipos así como también los bienes de todas las personas que asisten al edificio, mas no deberá ser utilizado como un sistema para el control de la asistencia.
- Se recomienda que para el acceso a la información almacenada se implemente políticas de seguridad, para mantener la integridad de la información y esto solo tendrá acceso la persona quien está a cargo del monitoreo del sistema de videovigilancia.
- Se deberá realizar un plan de mantenimiento para los equipos en especial para las cámaras debido a las condiciones ambientales, ya que las cámaras se encuentran tanto en el exterior como interior del edificio, logrando así mantener un adecuado funcionamiento del sistema de seguridad mediante videovigilancia.

GLOSARIO

ATW:	Balance de blanco con seguimiento automático
AWC:	Control automático del balance del blanco
BLC:	Compensación de luz de fondo
CCD:	Dispositivo de carga acoplada
CCTV:	Circuito cerrado de televisión
CMOS:	Semiconductor de óxido de metal complementario
DHCP:	Dynamic Host Configuration Protocol (protocolo de configuración huésped dinámico)
DVR:	Grabador de video digital
FPS:	Medida de imágenes por segundo
H.624:	Compresión de video digital con pérdida
IP:	Protocolo de Internet
IEEE:	El Instituto de Ingeniería Eléctrica y Electrónica
ISP:	Internet service provider (Proveedor de servicio de internet)
JPEG:	Joint Photographic Experts Group
LAN:	Red de Area Local
LUX:	Intensidad de luz que incide en una superficie
MJPEG:	Motion Joint Photographic Experts Group
MPEG-4:	Grupo de expertos en imágenes en movimiento
NVR:	Grabador de video de red
OSI:	Open System Interconnection (Interconexión del sistema abierto)
PoE:	Alimentación a través de Ethernet
RSSI:	Received Signal Strength Indicator (Indicador de intensidad de señal recibida)
SSID:	Service Set Identifier (Identificador de conjunto de servicios)
SGSI:	information security management system, ISMS
TCP/IP:	Transmission Control Protocol/Internet Protocol (Protocolo de Control de Transmisión/Protocolo de Internet)
UTP:	Par trenzado no blindado
VCR:	Grabador de video – videocasetera
WI-FI:	Fidelidad inalámbrica (Wireless Fidelity)
WLAN:	Red de área local inalámbrica
WPAN:	Red de área personal inalámbrica
WMAN:	Red de área metropolitana inalámbrica
WWAN:	Red de área extensa inalámbrica

BIBLIOGRAFIA

AENOR ECUADOR. *Seguridad de la información* [En línea]. 2016. [Consulta: 22 enero 2018]. Disponible en: <http://www.aenorecuador.com/seguridad-de-la-informaci%C3%B3n.aspx>

AXIS COMMUNICATIONS. *Productos y soluciones* [En línea]. Network cameras. 2009. [Consulta: 20 enero 2018]. Disponible en: <https://www.axis.com/cl/es/learning/web-articles/technical-guide-to-network-video/types-of-network-cameras>

AXIS COMMUNICATIONS. *Productos y soluciones* [En línea]. Video encoders. 2009. [Consulta: 20 enero 2018]. Disponible en: <https://www.axis.com/cl/es/learning/web-articles/technical-guide-to-network-video/video-encoders>

AXIS COMMUNICATIONS. *Productos y soluciones* [En línea]. Audio. 2009. [Consulta: 20 enero 2018]. Disponible en: <https://www.axis.com/cl/es/learning/web-articles/technical-guide-to-network-video/audio>

AXIS COMMUNICATIONS. *Videovigilancia IP* [En línea]. 2009. [Consulta: 07 noviembre 2017]. Disponible en: <https://www.axis.com/cl/es/learning/web-articles/technical-guide-to-network-video/types-of-network-cameras>

BLACIO MOSQUERA, Diego Andrés, & CARRASCO CAYAMBE, Esteban Andrés. *Implementación de un sistema de videovigilancia con cámaras IP para la planta baja del modular dos de la Escuela de Ingeniería Industrial de la ESPOCH* (Tesis). [Pdf]. Escuela Superior Politécnica de Chimborazo, Facultad de Mecánica, Escuela de Ingeniería Industrial. Ecuador. 2016. [Consulta: 2018-01-30]. Disponible en: <http://dspace.esPOCH.edu.ec/handle/123456789/5815>

CCM. *Redes Inalámbricas* [En línea]. 2017. [Consulta: 21 enero 2018]. Disponible en: <http://es.ccm.net/contents/818-redes-inalambricas>

CCM. *Vlans* [En línea]. 2017. [Consulta: 21 enero 2018]. Disponible en: <http://es.ccm.net/contents/286-vlan-redes-virtuales>

CHIMBORAZO TORO, Dorys Liliana. *Diseño de un sistema de videovigilancia con tecnología IP para el barrio la Delicia de la ciudad de Ambato* (Tesis). [Pdf]. Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica. Ambato. 2015. [Consulta: 2017-10 -18]. Disponible en:

<http://bibdigital.epn.edu.ec/bitstream/15000/10770/1/CD-6313.pdf>

GARCIA, F. *Videovigilancia: CCTV usando videos IP*. España: Editorial Vértice, 2010. [Consulta: 16 enero 2018]. Disponible en:

https://books.google.com.ec/books?id=xb3mzBEyIoC&pg=PA3&lpg=PA3&dq=videovigilancia+ip+evolucion&source=bl&ots=I9vP3dPD4J&sig=60qCjm_XoZnQfCvHoeRZ5umLSIo&hl=es&sa=X&ved=0ahUKEwiv45rSnMvYAhXwSN8KHVwMAVcQ6AEISTAG#v=onepage&q=videovigilancia%20ip%20evolucion&f=false

GOMEZ AUCANCELA, Adriana Cecilia, & LÓPEZ PÉREZ, Freddy Marcelo. *Diseño de una red de supervisión y control con transmisión de audio y video en alta definición para la ESPOCH* (Tesis). [Pdf]. Escuela Superior Politécnica de Chimborazo, Facultad de Informática y Electrónica, Escuela de Ingeniería Electrónica Telecomunicaciones y Redes. Ecuador. 2016. [Consulta: 2018-01-19]. Disponible en:

<http://dspace.esPOCH.edu.ec/handle/123456789/6389>

GUEVARA BETANCOURT, Edder. *Sistema de Videovigilancia Remota de bajo costo con microcomputadora y celdas solares* (Tesis). [Pdf]. Universidad de Costa Rica, Facultad de Ingeniería, Escuela de Ingeniería Eléctrica. Costa Rica. 2013. [Consulta: 2017-12-6]. Disponible en:

http://eie.ucr.ac.cr/uploads/file/proybach/pb2013/pb2013_035.pdf

HOMMAX. *Cámaras Bullet IP* [En línea]. 2017. [Consulta: 03 abril 2018]. Disponible en: <https://www.hommaxistemas.com/product/camara-ip-hw-ds-2cd1021-i-2-8mm/>

HOMMAX. *Video Hikvision IP (NVR)* [En línea]. 2017. [Consulta: 03 abril 2018]. Disponible en: <https://www.hommaxistemas.com/product/video-hikvision-ip-ds-7608ni-e28pa/>

HOMMAX. *Cámaras Minidomo IP* [En línea]. 2017. [Consulta: 03 abril 2018]. Disponible en: <https://www.hommaxistemas.com/product/camara-ip-hw-ds-2cd1121-i2-8mm/>

INFORMATICA MODERNA. *Cable de red UTP* [En línea]. 2008. [Consulta: 28 febrero 2018]. Disponible en: http://www.informaticamoderna.com/Cable_lan.htm

INFORMATICA MODERNA. *Las Redes Inalámbricas* [En línea]. 2008. [Consulta: 21 enero 2018]. Disponible en: http://www.informaticamoderna.com/Redes_inalam.htm

JIE, Ma Wen. *Categoría de cables* [En línea] 2014. [Consulta: 28 febrero 2018.] Disponible en: https://techlandia.com/cable-cat-5-vs-cat-6-sobre_76877/

JUSTIA ECUADOR. *Ley de seguridad pública y del estado* [En línea] 2018. [Consulta: 28 febrero 2018.] Disponible en: <https://ecuador.justia.com/nacionales/leyes/ley-de-seguridad-publica-y-del-estado/gdoc/>

MARKGRAF, Bert. *Especificación de cable* [En línea] 2014. [Consulta: 28 febrero 2018] Disponible en: https://techlandia.com/especificaciones-cables-cat-5-cat-6-info_197062/

MARTÍ, Silvia. *Diseño de un sistema de televigilancia sobre IP para el edificio CRAI de la Escuela Politécnica Superior de Gandía* (Tesis). [Pdf]. Universidad Politécnica de Valencia, Escuela Politécnica Superior de Gandía. España. 2013. [Consulta: 2017-11-22]. Disponible en: <https://riunet.upv.es/bitstream/handle/10251/34082/memoria.pdf?sequence=1>

ORACLE. *Modelo de referencia OSI* [En línea]. 2010. [Consulta: 21 enero 2018]. Disponible en: <https://docs.oracle.com/cd/E19957-01/820-2981/ipov-8/index.html>

SYSCOM. *Software de monitoreo local y remoto* [En línea]. 2017. [Consulta: 04 abril 2018]. Disponible en: <https://www.syscom.mx/producto/IVMS-4200-HIKVISION-76556.html>

TXDATOS. *Modelo OSI* [En línea]. 2011. [Consulta: 21 enero 2018]. Disponible en: <https://txdatos.wordpress.com/2011/02/21/modelo-osi/>

VELASCO, Rubén. *Acrylic WIFI* [En línea]. 2013. [Consulta: 23 enero 2018]. Disponible en: <https://www.redeszone.net/redes/acrylic-wifi/>

ANEXOS

Anexo A: Planta baja del edificio FIE

Anexo B: Primer piso del edificio FIE

Anexo C: Segundo piso del edificio FIE

Anexo D: Hoja de especificaciones técnicas de cámara domo

HIKVISION

DS-2CD1121-I
2.0 MP CMOS Network Dome Camera



2.8 mm Fixed Focal Lens



Non 2.8 mm Fixed Focal Lens



Key Features

- 1/2.8" progressive scan CMOS
- Up to 2.0 megapixel
- 2.8mm/4mm/6mm fixed focal lens
- Up to 30 m IR range
- Dual stream
- Digital WDR (Wide Dynamic Range)
- 3D DNR (Digital Noise Reduction)
- PoE (Power over Ethernet)
- IP67, IK10
- Mobile monitoring via Hik-Connect or iVMS-4500



www.hikvision.com

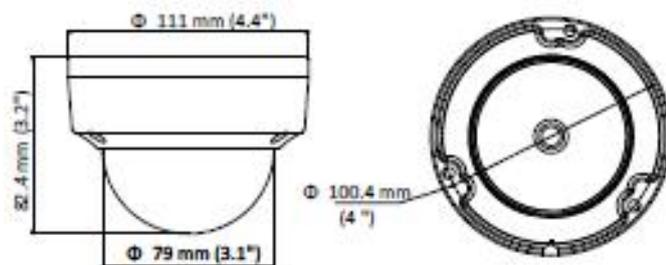
Specification

Camera	
Image Sensor	1/2.8" progressive scan CMOS
Min. Illumination	Color: 0.01Lux @(F1.2,AGC ON),0 lux with IR
Shutter Speed	1/3s to 1/100,000 s, supports low shutter
Lens	2.8 mm @F2.0, horizontal field of view 105°, 4 mm @F2.2, horizontal field of view 84° 6 mm @F2.0, horizontal field of view 55°
Lens Mount	M12
Day & Night	IR cut filter with auto switch
2-Axis Adjustment	Pan: 0° to 355°, tilt: 0° to 70°
DNR(Digital Noise Reduction)	3D DNR
WDR(Wide Dynamic Range)	Digital WDR
Compression Standard	
Video Compression	Main stream: H.264+/H.264 Sub stream: H.264/MJPEG
H.264 Type	Baseline profile/Main profile
Video Bit Rate	32 Kbps to 8 Mbps
Image	
Max. Resolution	1920 × 1080
Main Stream Max. Frame Rate	50Hz: 25fps @(1920 × 1080, 1280 × 960, 1280 × 720) 60Hz: 30fps @(1920 × 1080, 1280 × 960, 1280 × 720)
Sub-stream Max. Frame Rate	50Hz: 25fps @(704 × 576, 640 × 480, 352 × 288, 320 × 240) 60Hz: 30fps @(704 × 480, 640 × 480, 352 × 240, 320 × 240)
Image Settings	Brightness, saturation, contrast, sharpness are adjustable via web browser or client software
Day/Night Switch	Support auto, scheduled
Others	Mirror, BLC (area configurable), region of interest (support 1 fixed region)
Network	
Network Storage	NAS (NFS,SMB/CIFS)
Detections	Motion detection
Alarms	Video tampering, network disconnected, IP address conflicted
Protocols	TCP/IP,ICMP,HTTP,HTTPS,FTP,DHCP,DNS,DDNS,RTP,RTSP,RTCP, NTP,UPnP,SMTP,IGMP,802.1X,QoS,IPv6, Bonjour
Standard	ONVIF(PROFILE S,PROFILE G),PSIA,CG(ISA)
General Function	One-key reset, anti-flicker, heartbeat, mirror, password protection, privacy mask, watermark, IP address filter
Interface	
Communication Interface	1 RJ45 10M/100M self-adaptive Ethernet port
Reset	Support
General	
Operating Conditions	-30 °C to 60 °C (-22 °F to 140 °F), humidity: 95% or less (non-condensing)
Power Supply	12V DC± 25%, PoE (802.3af)
Power Consumption	Max. 5 W
Protection Level	IP67, IK10
IR Range	Up to 30 m
Dimensions	Φ111 mm × 82 mm (4.4" × 3.2")
Weight	500 g (1.1 lb.)

Available Models

DS-2CD1121-H

Dimension



Accessory



DS-1250ZJ
Inclined Base Mounting Bracket



DS-1275ZJ
Vertical Pole Mounting Bracket



DS-1272ZJ-110
Wall Mounting Bracket



DS-1272ZJ-110B
Wall Mounting Bracket



DS-1271ZJ-110
Pendant Mounting Bracket



DS-1276ZJ
Corner Mounting Bracket



DS-1280ZJ-DM18
Junction Box



DS-1250ZJ
Rain Shade

DS-1250ZJ



HIKVISION

Headquarters

No. 379, Gaoxin Road, Jiangyin District,
Wuxi, Jiangsu, 210651, China
T +86-512-6807-8899
www.hikvision.com

Hikvision USA
T +1-303-895-0930
usa.usa@hikvision.com

Hikvision Italy
T +39-0432-6982
it.ita.it@hikvision.com

Hikvision Singapore
T +65-6394-4718
sg.singapore@hikvision.com

Hikvision Africa
T +27-102-0331700
africa.africa@hikvision.com

Hikvision Europe
T +31-20-55-42-770
eu.eu@hikvision.com

Hikvision France
T +33-1-69-69-139-668
fr.fr@hikvision.com

Hikvision Spain
T +34-91-809-4033
es.es@hikvision.com

Hikvision Hong Kong
T +852-2331-1761

Hikvision Middle East
T +971-4-3011895
me.me@hikvision.com

Hikvision Spain
T +34-91-707-16-50
info.es@hikvision.com

Hikvision Canada
T +1-905-800-1940
canada.usa@hikvision.com

Hikvision Russia
T +7-905-660-97-99
rus.rus@hikvision.com

Hikvision Poland
T +48-22-663-02-02
poland@hikvision.com

Hikvision Korea
T +82-31-712-4941
south.korea@hikvision.com

Hikvision India
T +91-02-26468831
www@pranahikvision.com

Hikvision UK
T +44-1296-302340
support.uk@hikvision.com

Hikvision Brazil
T +55-11-3318-0091
latin.support@hikvision.com

Anexo E: Hoja de especificaciones técnicas de cámara Bullet

HIKVISION

DS-2CD1021-I 2.0 MP CMOS Network Bullet Camera



Key Features

- 1/2.8" progressive scan CMOS
- Up to 2.0 megapixel
- 2.8 mm/4 mm/6 mm fixed focal lens
- Up to 30 m IR range
- Dual stream
- Digital WDR (Wide Dynamic Range)
- 3D DNR (Digital Noise Reduction)
- PoE (Power over Ethernet)
- IP67
- Mobile monitoring via Hik-Connect or iVMS-4300



www.hikvision.com

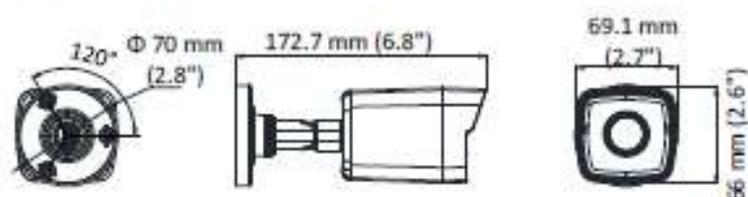
Specification

Camera	
Image Sensor	1/2.8" progressive scan CMOS
Min. Illumination	Color: 0.01 Lux @(F1.2, AGC ON), 0 Lux with IR
Shutter Speed	1/3 s to 1/100,000 s, support slow shutter
Lens	2.8 mm @F2.0, horizontal field of view 105.8°, 4 mm @F2.2, horizontal field of view 83.6° 8 mm @F2.0, horizontal field of view 55°
Lens Mount	M12
Day & Night	IR cut filter with auto switch
3-Axis Adjustment (Bracket)	Pan: 0° to 360°, tilt: -90° to 90°, rotation: 0° to 360°
DNR (Digital Noise Reduction)	3D DNR
WDR (Wide Dynamic Range)	Digital WDR
Compression Standard	
Video Compression	Main stream: H.264+/H.264 Sub stream: H.264/MJPEG
H.264 Type	Baseline profile/Main profile
Video Bit Rate	32 Kbps to 8 Mbps
Image	
Max. Resolution	1920 × 1080
Main Stream	50Hz: 25fps @(1920 × 1080, 1280 × 960, 1280 × 720)
Max. Frame Rate	60Hz: 30fps @(1920 × 1080, 1280 × 960, 1280 × 720)
Sub-stream	50Hz: 25fps @(704 × 576, 640 × 480, 352 × 288, 320 × 240)
Max. Frame Rate	60Hz: 30fps @(704 × 480, 640 × 480, 352 × 240, 320 × 240)
Image Settings	Brightness, saturation, contrast, sharpness are adjustable via web browser or client software
Day/Night Switch	Support auto, scheduled
Others	Mirror, BLC (area configurable), region of interest (support 1 fixed region)
Network	
Network Storage	NAS (NFS, SMB/CIFS)
Detections	Motion Detection
Alarms	Video tampering, network disconnected, IP address conflicted
Protocols	TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, RTP, UPnP, SMTP, IGMP, 802.1X, QoS, IPv6, Bonjour
Standard	ONVIF (PROFILE S, PROFILE G), PSIA, CGI, SAM
General Function	Anti-flicker, heartbeat, mirror, password protection, privacy mask, watermark, IP address filter
Interface	
Communication Interface	1 RJ45 10M/100M self-adaptive Ethernet port
General	
Operating Conditions	-30 °C to 60 °C (-22 °F to 140 °F), humidity: 95% or less (non-condensing)
Power Supply	12 VDC ± 25%, PoE (802.3af)
Power Consumption	Max. 5 W/6.5 W (PoE)
Ingress Protection	IP67
IR Range	Up to 30 m
Dimensions	69.1 mm × 68 mm × 172.7 mm (2.7" × 2.6" × 6.8")
Weight	500 g (1.1 lb.)

Available Models

DS-2CD1021-I

Dimension



Accessory



**DS-1280Z-05
Junction Box**

Download by



HIKVISION

HEADQUARTERS
No. 355, Taohu Road, Ningbo, Zhejiang, 315000, China
T +86-571-8951-8888
yves@hikvision.com

Hikvision USA
T +1-888-855-8689
usa@hikvision.com

Hikvision Italy
T +39-049-2601-2601
it@hikvision.com

Hikvision Singapore
T +65-6500-4215
sg@hikvision.com

Hikvision Africa
T +212-22 051 120
africa@hikvision.com

Hikvision Canada
T +1-416-223-5570-779
ca@hikvision.com

Hikvision France
T +33-01-69-39-400
fr@hikvision.com

Hikvision Germany
T +49-0-4209-4211
germany@hikvision.com

Hikvision Hong Kong
T +852-2715-1151

Hikvision Middle East
T +971-4-8800388
middleeast@hikvision.com

Hikvision Spain
T +34-91-721-28-38
es@hikvision.com

Hikvision Canada
T +1-888-855-8689
canada@hikvision.com

Hikvision Russia
T +7-495-959-97-98
russia@hikvision.com

Hikvision Poland
T +48-22-660-11-00
poland@hikvision.com

Hikvision Korea
T +82-31-731-8341
korea@hikvision.com

Hikvision India
T +91-20-29668890
india@hikvision.com

Hikvision UK
T +44-12-960-01-00
support_uk@hikvision.com

Hikvision Brazil
T +55-11-5319-9292
global.support@hikvision.com

Anexo G: Hoja de especificaciones técnicas del disco duro



WD Purple™

Discos duros para videovigilancia

Los discos WD Purple están fabricados para los sistemas de seguridad de alta definición siempre en funcionamiento que operan las 24 horas, todos los días. Con una carga de trabajo de hasta 180 TB/año y admisión de hasta 64 cámaras, los discos WD Purple están optimizados para los sistemas de videovigilancia. Los discos de almacenamiento para videovigilancia WD Purple también incorporan la exclusiva tecnología AllFrame 4K™ de WD, para que pueda crear un sistema de seguridad fiable a la medida de las necesidades de la empresa.



CONEXIONES SATA a 6Gb/s	FORMATO 3,5 pulgadas	CLASE DE RENDIMIENTO Clase de 9,400 t p. m.	CAPACIDADES De 500 GB a 10 TB
-----------------------------------	--------------------------------	---	---

NÚMEROS DE MODELO

WD100PURZ	WD800PURZ
WD150PURZ	WD100PURZ
WD200PURZ	WD150PURZ
WD300PURZ	WD200PURZ

Características del producto

Almacenamiento líder en el sector.

Videovigilancia en la que puede confiar.

WD es líder mundial en el sector de los discos duros de almacenamiento para videovigilancia. WD Purple le permite obtener un disco diseñado para sistemas de videovigilancia que operan ininterrumpidamente a altas temperaturas y de esta forma, disfrutar de una reproducción de los vídeos fiable y de calidad, cuando más lo necesita. Tanto si está protegiendo a sus seres queridos como si está operando su empresa, WD Purple ofrece un rendimiento en el que puede confiar.

Tecnología AllFrame 4K exclusiva de WD

Todos los discos WD Purple están equipados con la tecnología AllFrame 4K, que mejora la transmisión 4K para reducir la pérdida de fotogramas, mejorar la reproducción de vídeo en general y aumentar el número de compartimentos de disco admitidos en un NVR. Prepárese su solución de videovigilancia para el futuro con los discos WD Purple compatibles con cámaras de vídeo alta definición.

Carga de trabajo mejorada

Con una carga de trabajo de 180 TB/año (tres veces superior a la de los discos para ordenadores de sobremesa) WD Purple está diseñado para gestionar las exigentes demandas de los sistemas DVR y NVR de videovigilancia de vídeo continua.

Amplie su visión hasta 64 cámaras

Cada uno de los discos WD Purple está optimizado para poder utilizar hasta 64 cámaras. Con esa capacidad, tendrá flexibilidad para actualizar o ampliar su sistema de seguridad en el futuro.

Diseñado para las soluciones

de videovigilancia actuales y futuras.

Diseñado para un funcionamiento ininterrumpido en todos los formatos de DVR y NVR de videovigilancia estándar. Con compatibilidad para más de 8 compartimentos* y componentes resistentes al desgaste, los discos WD Purple ofrecen un funcionamiento fiable en sistemas de videovigilancia a mayor escala en entornos más duros.

Alta capacidad a prueba de fallos

de campo

En su 4ª generación y con más de 10 millones de discos enviados, la tecnología HelioSeek™ a prueba de fallos de campo proporciona almacenamiento de alta capacidad de confianza WD Purple (5 TB y 10 TB) para las exigentes necesidades de almacenamiento de vídeo de videovigilancia 4K.

Amplia compatibilidad.

Integración impecable.

Los discos duros WD Purple se han creado pensando en la compatibilidad, por lo que puede ampliar la capacidad de sistemas de videovigilancia de formato HD y 4K. Al ser compatibles con una amplia gama de dispositivos y chips del sector, su disco encontrará la configuración de DVR o NVR que se ajuste a sus necesidades.

Menor consumo. Más eficiencia.

Con nuestra exclusiva tecnología IntelliSeek™, los discos WD Purple pueden calcular las velocidades de búsqueda óptimas. De esta forma, se reducen al mínimo el consumo de energía, las vibraciones y el ruido ambiental.

Tres años de garantía limitada.

Como fabricante de discos duros líder del sector, WD avala sus soluciones de almacenamiento para videovigilancia con una garantía limitada de 3 años que se incluye con cada disco WD Purple.

La ventaja de WD

En WD, sometemos todos los productos a completas Pruebas de Integridad Funcional (FIT™) antes de su lanzamiento. Estas pruebas aseguran que nuestros productos satisfacen los más altos estándares de calidad y fiabilidad de la marca WD. WD también tiene una detallada base de conocimiento con más de 1.000 artículos útiles, así como software y utilidades de ayuda. Nuestras líneas telefónicas de atención al cliente tienen un amplio horario para asegurar que obtiene asistencia cuando la necesita. Puede llamar a nuestro teléfono gratuito de atención al cliente para solicitar ayuda o visitar la página web de Soporte de WD para obtener más información.

