

ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE VIDEO VIGILANCIA CON CÁMARAS IP PARA EL CENTRO DE DESARROLLO INFANTIL “ANGELITOS JUGUETONES”.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ANÁLISIS DE SISTEMAS INFORMÁTICOS

NÚÑEZ MORETA IVÁN ALEJANDRO
ivan90_alejandro@hotmail.com

PILA VALDIVIEZO ERIKA PRISCILA
erikaprispi@gmail.com

DIRECTOR: Ing. Peñafiel Aguilar Myriam Guadalupe
mpenafiel07@gmail.com

Quito, Diciembre 2014

DECLARACIÓN

Nosotros, Núñez Moreta Iván Alejandro y Pila Valdiviezo Erika Priscila declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Núñez Moreta Iván Alejandro

Pila Valdiviezo Erika Priscila

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Núñez Moreta Iván Alejandro y Pila Valdiviezo Erika Priscila bajo mi supervisión.

Ing. Myriam Peñafiel
DIRECTOR DEL PROYECTO

AGRADECIMIENTO

A mi directora de tesis, Dra. Miriam Peñafiel por su esfuerzo y dedicación, con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado impulsarme a terminar mis estudios con éxito.

También me gustaría agradecer a mis profesores durante toda mi carrera profesional porque todos han aportado a mi formación.

Agradezco con todo mi cariño a mi familia, por todo su esfuerzo, para que yo pudiera lograr mis sueños, por motivarme y darme la mano cuando sentía que el camino se terminaba.

Son muchas las personas que han formado parte de mi vida profesional a las que me encantaría agradecerles, por su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida. En especial a mi amiga y compañera de tesis Erika, por tu paciencia y comprensión, preferiste sacrificar tu tiempo para que pudiéramos cumplir con nuestra meta.

Iván Núñez

DEDICATORIA

A todas las personas que formaron parte de mi vida, algunas están aquí conmigo y otras en mis recuerdos y en mi corazón, sin importar en donde estén quiero darles las gracias por formar parte de mí, por todo lo que me han brindado y por todos sus buenos deseos.

Iván Núñez

AGRADECIMIENTO

Gracias a mis padres por darme la vida y apoyarme, en especial a mi madre Zoila quien es mi pilar y mi guía. Gracias madrecita por sus consejos, su cariño, paciencia y amor. Eres la razón por la que no me rindo jamás.

A mis hermanas Diana y Yadíra. Mi hermanita mayor, gracias por demostrarme que con perseverancia puedo alcanzar mis metas. Mi pequeña hermanita, gracias por iluminar mis días con tus ocurrencias y travesuras.

A mi abuelita Blanca y mi tía Mariana por su apoyo incondicional y compañía en los momentos difíciles.

A mis mascotas queridas por no dejarme dormir, por sus travesuras, por su amor incondicional.

A mis queridos amigos: Luis, Andrea, Cristina, Darwin, Iván y Laura; por sus consejos, por creer en mí, por escucharme, por aguantarme y acompañarme siempre.

Espero que compartamos muchos momentos más juntos.

Finalmente, gracias a la vida por ponerme donde estoy, por los tropiezos y caídas, por los golpes y lecciones, por los errores y aciertos, por las tristezas y alegrías, por permitirme al fin ver cumplido este objetivo.

Sé que lo mejor aún está por venir.

Erika

DEDICATORIA

A la mujer que más admiro. Lo que soy y lo que he logrado hasta ahora ha sido gracias a ti, madrecita Zoila. Espero algún día llegar a ser la mitad de lo que tú eres, una madre amorosa, luchadora, con mucha bondad y esperanza en el corazón. ¡Te adoro manino!

Erika

RESUMEN

El presente proyecto se enfoca en la aplicación práctica del estudio de las redes de datos implementando un sistema de video vigilancia IP para monitorear el Centro Infantil “Angelitos Juguetones”.

El centro infantil, por estar al cuidado de las personas más vulnerables del hogar, requiere varias medidas de seguridad; de manera que los padres de familia y las autoridades del plantel puedan monitorear la interacción de los docentes con los niños, así como brindar mayor seguridad y resguardar los bienes de la institución. La misma no cuenta con medios para registrar las actividades que se desarrollan en las zonas con mayores requerimientos de vigilancia.

La investigación de la tecnología de video vigilancia IP, los conceptos de digitalización de imagen, así como el estudio y comparación de los dispositivos existentes en el mercado, permitieron comprender y analizar cómo cubrir las necesidades de monitoreo del plantel. Según los conocimientos adquiridos, se implementó la solución más adecuada que cumpla con los requerimientos planteados para el sistema.

La implementación del sistema de video vigilancia con cámaras IP, representó una mejora significativa con respecto a la seguridad del plantel, puesto que se mantiene un registro del comportamiento y actividades realizadas en los espacios con mayores requerimientos de vigilancia; así como asegurar el uso adecuado de los recursos de la institución.

El proyecto se encuentra dividido en 4 capítulos además de conclusiones, recomendaciones y bibliografía.

El Capítulo I se titula Aspectos Generales y detalla la situación actual del Centro de Desarrollo Infantil “Angelitos Juguetones”, el planteamiento del problema, formulación y sistematización, objetivos, justificación del proyecto y el cronograma de actividades.

El Capítulo II presentará definiciones y fundamentos teóricos que describen las tecnologías actuales de redes de datos, compresión de video, sistemas de vigilancia IP y sistemas analógicos; así como conceptos fundamentales para la elaboración del proyecto.

El Capítulo III describe las zonas con mayores requerimientos de vigilancia, además presenta el estudio y comparación de equipos en el mercado, finalmente se plantea la solución más adecuada para el sistema.

El Capítulo IV mostrará la implementación de la solución para el sistema de video vigilancia, la instalación de los dispositivos, así como su respectiva configuración y medios de gestión.

En el Capítulo V se plantean las conclusiones obtenidas al finalizar el proyecto, de igual manera las recomendaciones que se deberán poner en práctica para el buen funcionamiento del sistema.

ÍNDICE

CAPITULO I

1. ASPECTOS GENERALES	1
1.1. Visión.....	1
1.2. Misión	1
1.3. Planteamiento del problema	2
1.4. Formulación y Sistematización del problema	2
1.4.1. Formulación	2
1.4.2. Sistematización	2
1.5. Objetivos de la Investigación	3
1.5.1. Objetivo General	3
1.5.2. Objetivos Específicos.....	3
1.6. Justificación del Proyecto	4
1.7. Cronograma de Actividades	5

CAPITULO II

2. MARCO TEÓRICO	6
2.1. Redes de Datos.....	6
2.1.1. Tipos de redes de datos.....	7
2.1.1.1. Por su extensión	7
2.1.1.1.1. PAN (Personal Area Network)	7
2.1.1.1.2. LAN (Local Area Network)	7
2.1.1.1.3. CAN (Campus Area Network).....	7
2.1.1.1.4. MAN (Metropolitan Area Network)	7
2.1.1.1.5. WAN (Wide Area Network)	8
2.1.2. Modelo OSI	8
4.1.2.1. Capa Física.....	9
4.1.2.2. Capa de Enlace de Datos	10
4.1.2.3. Capa de Red.....	10
4.1.2.4. Capa de Transporte.....	10

4.1.2.5.	Capa de Sesión	10
4.1.2.6.	Capa de Presentación	11
4.1.2.7.	Capa de Aplicación	11
4.1.3.	Protocolos	11
4.1.3.1.	Modelo de Referencia TCP/IP	12
4.1.3.1.1.	Estructura Interna	12
4.1.3.1.1.1.	Capa Física.....	12
4.1.3.1.1.2.	Capa de Enlace	13
4.1.3.1.1.2.1.	ARP (Address Resolution Protocol)	14
4.1.3.1.1.2.2.	RARP (Reverse Address Resolution Protocol)	14
4.1.3.1.1.3.	Capa de Red.....	14
4.1.3.1.1.3.1.	IP (Internet Protocol).....	15
4.1.3.1.1.3.2.	ICMP (Internet Control Message Protocol)	15
4.1.3.1.1.3.3.	IGMP (Internet Group Management Protocol)	16
4.1.3.1.1.4.	Capa de Transporte.....	16
4.1.3.1.1.4.1.	UDP (User Datagram Protocol).....	16
4.1.3.1.1.4.2.	TCP (Transmission Control Protocol)	17
4.1.3.1.1.5.	Capa de Aplicación.....	17
4.1.3.1.1.5.1.	TELNET (Telecommunicating Networks).....	18
4.1.3.1.1.5.2.	FTP. (File Transfer Protocol).....	18
4.1.3.1.1.5.3.	HTTP (HyperText Transfer Protocol)	18
4.1.3.1.1.5.4.	NNTP. (Network News Transfer Protocol)	18
4.1.3.1.1.5.5.	SMTP (Simple Mail Transport Protocol).....	19
4.1.3.1.1.5.6.	POP3 (Protocolo de Oficina Postal).....	19
4.1.3.1.1.5.7.	IMAP (Internet Mail Access Protocol)	19
4.1.3.1.1.5.8.	MIME (Multipurpose Internet Mail Extensions).....	20
2.2.	Compresión de video Digital	20
2.2.1.	Códec de vídeo	21
2.2.1.1.	Compresión de imagen vs. Compresión de vídeo	21

2.2.2.	Formatos de compresión.....	25
2.2.2.1.	Motion JPEG.....	25
2.2.2.2.	MPEG-4.....	26
2.2.2.3.	H.264 o MPEG-4 Part 10/AVC.....	26
2.2.3.	Frecuencia de bits variable y constante	27
2.2.3.1.	Frecuencia de bits variable	27
2.2.3.2.	Frecuencia de bits constante	28
2.2.4.	Comparación de estándares	28
2.3.	Video Vigilancia CCTV	30
2.3.1.	Evolución de los sistemas de vigilancia por vídeo	30
2.3.1.1.	Sistemas de circuito cerrado de TV analógicos usando VCR .	30
2.3.1.2.	Sistemas de circuito cerrado de TV analógicos usando DVR .	31
2.3.1.3.	Sistemas de circuito cerrado de TV analógicos usando DVR de red	32
2.3.1.4.	Sistemas de vídeo IP que utilizan servidores de vídeo.....	32
2.3.1.5.	Sistemas de vídeo IP que utilizan cámaras IP.....	33
2.3.2.	Componentes de un sistema de cctv clásico	34
2.3.2.1.	Cámaras analógicas	35
2.3.2.2.	Monitores.....	35
2.3.2.3.	Grabadoras.....	35
2.3.2.4.	Matriz de Video.....	35
2.3.2.5.	Líneas de transmisión.....	36
2.3.3.	Descripción de los problemas comunes en los sistemas de videovigilancia tradicional o analógico.....	36
2.3.3.1.	Resolución inadecuada de las cámaras	36
2.3.3.2.	Grabaciones inaudibles	37
2.3.3.3.	Cámaras analógicas ubicadas sin un estudio previo	37
2.3.3.4.	Procedimiento de respaldos manual y deficiente.....	37
2.3.3.5.	Sistema difícilmente escalable.....	38
2.3.3.6.	Requerimientos de seguridad no son cubiertos por el sistema	38

2.3.4.	VIDEO IP.....	39
2.3.4.1.	Aplicaciones de la Videovigilancia IP.....	39
2.3.4.2.	Arquitectura Básica de un sistema de video IP.....	40
2.3.4.3.	Componentes de un sistema de cctv clásico.....	41
2.3.4.3.1.	Cámara de red.....	41
2.3.4.3.1.1.	Cámaras de red fijas.....	43
2.3.4.3.1.2.	Cámaras de red domo fijas.....	43
2.3.4.3.1.3.	Cámara de red PTZ.....	44
2.3.4.3.1.4.	Cámara de red Domo PTZ.....	46
2.3.4.3.2.	Servidor De Vídeo.....	47
2.3.4.3.2.1.	Servidores de vídeo montados en rack.....	48
2.3.4.3.2.2.	Servidores de vídeo independientes.....	49
2.3.4.3.2.3.	Servidores de vídeo con cámaras PTZ y domo ...	49
2.3.4.3.3.	Software de gestión de vídeo.....	49
2.3.4.3.3.1.	Criterios para la selección de un sistema de gestión de vídeo	51
2.3.4.3.3.1.1.	Uso de arquitecturas software abiertas.....	51
2.3.4.3.3.1.2.	Uso de arquitecturas cliente/servidor.....	52
2.3.4.3.3.1.3.	Integración con proveedores externos y uso de interfaces estándar	52
2.3.4.4.	Ventajas de la videovigilancia IP respecto a los sistemas analógicos.....	53
2.3.4.4.1.	Accesibilidad remota.....	53
2.3.4.4.2.	Calidad de imagen.....	54
2.3.4.4.3.	Gestión de eventos y video inteligente.....	54
2.3.4.4.4.	Estandarización.....	55
2.3.4.4.5.	Escalabilidad y flexibilidad.....	55
2.3.4.4.6.	Rol (Rentabilidad de la inversión).....	56

CAPITULO III

3. ANÁLISIS DE LA SITUACIÓN ACTUAL	57
3.1. Antecedentes.....	57
3.2. Plano del Área a Controlar	57
3.2.1. Descripción de las áreas a controlar	58
3.2.1.1. ZONA A	58
3.2.1.2. ZONA B	58
3.3. Estudio de Equipos de video vigilancia.....	59
3.3.1. CÁMARAS IP INTERIORES	59
3.3.1.1. Cámara IP FOSCAM FI9826W	59
3.3.1.1.1. Descripción	59
3.3.1.1.2. Características Principales	59
3.3.1.1.3. Especificaciones Técnicas.....	60
3.3.1.2. Cámara IP Apexis APM-HP803-MPC-WS	64
3.3.1.2.1. Descripción	64
3.3.1.2.2. Características Principales	64
3.3.1.2.3. Especificaciones Técnicas.....	65
3.3.1.3. Cámara IP D-Link DCS-930L.....	68
3.3.1.3.1. Descripción	68
3.3.1.3.2. Características Principales	69
3.3.1.3.3. Especificaciones Técnicas.....	69
3.3.1.4. Comparación de Cámaras IP Interiores.....	72
3.3.1.5. Conclusión del Estudio de Cámaras IP Interiores.....	75
3.3.2. CÁMARAS IP EXTERIORES	76
3.3.2.1. Cámara EasyN F-M1BF.....	76
3.3.2.1.1. Descripción	76
3.3.2.1.2. Características Principales	77
3.3.2.1.3. Especificaciones Técnicas.....	77
3.3.2.2. Cámara IP FOSCAM FI9804W	80

3.3.2.2.1. Descripción	80
3.3.2.2.2. Especificaciones Técnicas.....	80
3.3.2.3. Cámara IP Apexis APM-HP602-MPC-WS	83
3.3.2.3.1. Descripción	83
3.3.2.3.2. Características Principales	83
3.3.2.3.3. Especificaciones Técnicas.....	84
3.3.2.4. Comparación de Cámaras IP Exteriores.....	86
3.3.2.5. Conclusión del Estudio de Cámaras IP Exteriores.....	90

CAPITULO IV

4. IMPLEMENTACIÓN	91
4.1.1. Monitoreo de cámaras IP	92
4.1.2. Cámara de la Zona A	93
4.1.3. Cámara de la Zona B	95
4.1.4. Red Cableada	97

CAPITULO V

5. Conclusiones y Recomendaciones	98
5.1. Conclusiones	98
5.2. Recomendaciones.....	99
Bibliografía.....	100

ÍNDICE DE FIGURAS

Fig. 1. Red de datos.....	6
Fig. 2. Tipos de redes.....	8
Fig. 3. Modelo OSI	9
Fig. 4. Capa física relacionada con la Capa de Enlace	13
Fig. 5. Capa de Enlace relacionada con Capa Física y Capa de Red.....	13
Fig. 6. Traducción de direcciones IP a Ethernet.....	14
Fig. 7. Capa de Red relacionada con la capa Enlace y capa de Transporte.....	14
Fig. 8. Capa de Transporte relacionada con las Capa de Red y Aplicación.....	16
Fig. 9. Relación entre la Capa de Aplicación con capas inferiores.....	17
Fig. 10. Formato Motion JPEG.....	22
Fig. 11. Codificación diferencial.....	22
Fig. 12. Compensación de movimiento basada en bloques.....	23
Fig. 13. Secuencia con fotogramas.....	24
Fig. 14. Comparación de estándares.....	29
Fig. 15. Sistema de circuito cerrado de TV analógicos usando VCR.....	30
Fig. 16. Sistema de circuito cerrado de TV analógicos usando DVR.....	31
Fig. 17. Sistema de circuito cerrado de TV analógico usando DVR de red.....	32
Fig. 18. Sistema de vídeo IP que utiliza servidor de vídeo.....	33
Fig. 19. Sistema de vídeo IP con cámaras IP.....	34
Fig. 20. Esquema básico de un sistema de CCTV analógico.....	36
Fig. 21. Esquema básico de un sistema de video vigilancia IP.....	41
Fig. 22. Ubicación de las cámaras de red en un sistema de videovigilancia IP....	41
Fig. 23. Esquema básico de una cámara de red.....	42
Fig. 24. Cámara de red fija.....	43
Fig. 25. Cámara de red de domo fija.....	44
Fig. 26. Cámara de red PTZ.....	45
Fig. 27. Cámara de red de domo PTZ.....	47
Fig. 28. Servidor de video.....	48
Fig. 29. Aplicación de gestión de video.....	51
Fig. 30. Plano del área a controlar	58
Fig. 31. Cámara IP FOSCAM FI9826w	59
Fig. 32. Cámara IP Apexis APM-HP803-MPC-WS.....	64

Fig. 33. Cámara IP D-Link DCS-930L	68
Fig. 34. Cámara EasyN F-M1BF	76
Fig. 35. Cámara IP FOSCAM FI9804W	80
Fig. 36. Cámara IP Apexis APM-HP602-MPC-WS.....	83
Fig. 37. Plano con ubicación de las cámaras y alcance de visión	91
Fig. 39. Software de Gestión de Cámaras (IpCamClient) mostrando las vistas de los dos dispositivos instalados.	92
Fig. 40. Interfaz Web mediante DDNS	92
Fig. 41. Cámara IP - Zona A.....	93
Fig. 42. Alcance de visión - Cámara Zona A	94
Fig. 43. Vista del patio principal - Cámara Zona A	94
Fig. 44. Cámara Ip - Zona B.....	95
Fig. 45. IpCamClient - Zona B.....	96
Fig. 46. Interfaz Web - Cámara Zona B.....	96
Fig. 47. Red Cableada - Canaletas	97

ÍNDICE DE TABLAS

Tabla 1. Especificaciones Técnicas – Cámara FOSCAM FI9826W	63
Tabla 2. Especificaciones Técnicas - Cámara IP Apexis APM-HP803-MPC-WS.	67
Tabla 3. Especificaciones Técnicas - Cámara D-Link DCS-930L.....	71
Tabla 4. Comparación de Cámaras IP Interiores	75
Tabla 5. Especificaciones Técnicas - Cámara EasyN F-M1BF	79
Tabla 6. Especificaciones Técnicas - Cámara IP modelo FI9804W	82
Tabla 7. Especificaciones técnicas - Cámara IP Apexis APM-HP602-MPC-WS..	85
Tabla 8. Comparación de Cámaras IP Exteriores	90

ÍNDICE DE ANEXOS

Anexo A: Certificado de Entrega de Equipos

Anexo B: Manual de Usuario del Software IpCamClient

Anexo C: Manual de Usuario de Administración desde el Navegador.

CAPITULO I

1. ASPECTOS GENERALES

Angelitos Juguetones es un centro de desarrollo infantil ubicado en la calle Juan Treviño y Av. Gran Colombia; con 3 años de funcionamiento cuyos directivos llevan entre 12 y 15 años de experiencia en el ámbito educativo, garantizando un desarrollo integral fundamentados en los estándares de calidad del Ministerio de Educación y las políticas como institución privada. Fue creado el 18 de febrero de 2011, con el objetivo del cuidado de niños y niñas.

El Centro de Desarrollo Infantil “Angelitos Juguetones” es un lugar que cuenta con personal que investiga, estudia, acoge, da calor, reflexiona y hace reflexionar; todo siempre con cariño y afecto de tal manera que sus actores involucrados: directivos, docentes, auxiliares padres y madres de familia, niños y niñas se sientan humanos, bien tratados y con plenos derechos, sin olvidar que también hay obligaciones que derivan en dos lemas: el primero, que es interno “Ser y parecer”, y el segundo que es externo “A padres comprometidos, hijos exitosos”.

1.1. VISIÓN

Dedicarse a estimular, desarrollar y potencializar las necesidades de destrezas y habilidades de niños y niñas desde los 12 meses hasta los 59 meses de edad, mediante estrategias innovadoras considerando y respetando sus derechos, preparándolos para su escolaridad en su futuro más cercano, e inculcándoles valores para toda la vida.

1.2. MISIÓN

En el término de 3 a 5 años convertirse en un centro infantil reconocido por su labor educativa, estrategias innovadoras, don de comunicación, uso de la tecnología y conciencia social y ecológica, siempre enmarcado en los parámetros de calidad y excelencia que proponga el estado ecuatoriano y otras instituciones internacionales, evidentes en todos los procesos institucionales para beneficio de la comunidad en general

1.3. PLANTEAMIENTO DEL PROBLEMA

Actualmente la institución no cuenta con sistema de vigilancia, como consecuencia las zonas conflictivas no tienen supervisión, lo que impediría mantener un registro de los eventos que pueden ocurrir dentro del plantel.

Resulta necesario implementar un sistema de video vigilancia que permita evidenciar con claridad la entrada y salida de alumnos, padres de familia y personal administrativo, adicionalmente los sucesos que se presentan en las zonas previamente identificadas como problemáticas en el Centro de Desarrollo Infantil “Angelitos Juguetones”.

La implementación del sistema en el plantel brindaría eficacia y seguridad en el monitoreo de las zonas con mayores requerimientos de supervisión, además lograría asegurar el uso adecuado de los recursos de la institución como son el área de juegos y el patio del plantel.

1.4. FORMULACIÓN Y SISTEMATIZACIÓN DEL PROBLEMA

1.4.1. Formulación

- ¿Cómo apoyar a la vigilancia del Centro de Desarrollo Infantil “Angelitos Juguetones”?

1.4.2. Sistematización

- ¿Cuáles son las necesidades de monitoreo en la institución?
- ¿Cuáles son los aspectos teóricos y prácticos de la tecnología de video vigilancia IP?
- ¿En qué circunstancias se encuentra la infraestructura física y Sistema de Cableado Estructurado?
- ¿Qué tecnologías cumplen con los requerimientos para el nuevo sistema de video vigilancia?
- ¿Qué características tiene el software administrador del sistema propuesto?

- ¿Qué usuarios y políticas de uso debe tener el software administrador del sistema?
- ¿Cómo vigilar las áreas vulnerables de la unidad, de manera eficaz?
- ¿Qué documentos y actividades se deben realizar para el usuario final del sistema?

1.5. OBJETIVOS DE LA INVESTIGACIÓN

1.5.1. Objetivo General

Monitorear los acontecimientos que ocurren en las zonas conflictivas del Centro de Desarrollo Infantil “Angelitos Juguetones” mediante la implementación de un sistema de video vigilancia con cámaras IP.

1.5.2. Objetivos Específicos

- Determinar los requerimientos de monitoreo por parte autoridades del plantel.
- Analizar y comprender los aspectos teóricos y prácticos vigentes de la tecnología de video vigilancia IP.
- Analizar los aspectos físicos e infraestructura de red de la institución.
- Determinar los requerimientos tecnológicos para la implementación del sistema.
- Determinar el software administrador del sistema y determinar su mejor aplicación para el proyecto.
- Determinar las políticas de monitoreo y administración del software mediante la gestión de niveles de usuarios.
- Implementar un sistema de video vigilancia eficiente, con una interfaz amigable para el usuario.
- Asegurar el manejo adecuado del sistema mediante la capacitación y creación de manuales para el usuario final.

1.6. JUSTIFICACIÓN DEL PROYECTO

Tras el rápido crecimiento del mercado de video-vigilancia, las cámaras IP representan hoy una tendencia destacada para el futuro del video monitoreo.

El presente proyecto tiene como fin, el diseño e implementación de un sistema de video vigilancia con cámaras IP para el Centro de Desarrollo Infantil “Angelitos Juguetones”.

”Instalar cámaras de Video vigilancia IP fiables y de alta calidad para vigilar sus instalaciones aumentará la seguridad de su empresa a la par que su tranquilidad. Invertir en una completa solución ampliable que se integre con su actual red IP tiene sentido desde el punto de vista comercial. “ (DLink, 2012)

El diseño e implementación del sistema de video vigilancia IP brindaría apoyo a las autoridades del plantel para controlar la disciplina del alumnado y el personal docente del Centro de Desarrollo Infantil “Angelitos Juguetones” mediante recursos de avanzada tecnología y con una infraestructura de red que se adapte a las necesidades.

Los usuarios de este sistema tendrían la posibilidad de respaldar periódicamente las grabaciones; lo que sería de gran ayuda para los padres de familia que requieran indagar sobre alguna eventualidad y también apoyaría al personal docente para tener evidencia del caso.

1.7. CRONOGRAMA DE ACTIVIDADES

Nombre de tarea	Duración	Comienzo	Fin
☐ Análisis de los Requerimientos	38 días	lun 04/08/14	mié 24/09/14
Análisis de la situación actual	3 días	lun 04/08/14	mié 06/08/14
Análisis de la Infraestructura de Red	5 días	jue 07/08/14	mié 13/08/14
Diseño Lógico de la Situación Actual	14 días	jue 14/08/14	mar 02/09/14
Estudio de equipos existentes en el mercado	3 días	mié 03/09/14	vie 05/09/14
Diseño lógico de la red de cámaras	5 días	lun 08/09/14	vie 12/09/14
Definición de Equipos	8 días	lun 15/09/14	mié 24/09/14
☐ Implementación y Pruebas	25 días	jue 25/09/14	mié 29/10/14
Instalación de cámaras IP	13 días	jue 25/09/14	lun 13/10/14
Configuración de las cámaras	10 días	jue 25/09/14	mié 08/10/14
Instalación del servidor de video vigilancia	5 días	jue 09/10/14	mié 15/10/14
Conexión de red	8 días	jue 25/09/14	lun 06/10/14
Pruebas de conexión	10 días	mar 07/10/14	lun 20/10/14
Optimización de la implementación	7 días	mar 21/10/14	mié 29/10/14
Elaboración del manual con los datos obtenidos	30 días	jue 30/10/14	mié 10/12/14

CAPITULO II

2. MARCO TEÓRICO

En este capítulo se presentarán definiciones y fundamentos teóricos que describen las tecnologías actuales de redes de datos, compresión de video, sistemas de vigilancia IP y sistemas analógicos; así como conceptos para el mejor entendimiento del diseño e implementación del sistema de video vigilancia con cámaras IP para la el Centro de Desarrollo Infantil “Angelitos Juguetones”.

2.1. REDES DE DATOS

Las redes de datos, también llamadas redes de ordenadores o redes informáticas, son un conjunto de sistemas informáticos o interfaces conectados entre sí (interconectados) que comparten elementos, incrementando así la eficiencia de los procesos. Los sistemas informáticos son la suma de unos componentes hardware (elementos físicos como la pantalla, el teclado, el ratón, etc.), software (elementos intangibles como los programas, el sistema operativo, etc.) y las interfaces, que pueden ser periféricos o máquinas autónomas. (Gómez, 2011, pág. 11)

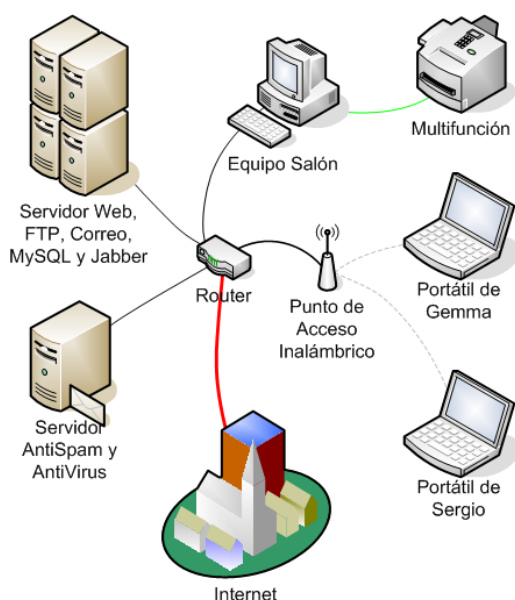


Fig. 1. Red de datos.

Fuente: (Redes Locales, 2011, pág. 11)

2.1.1. Tipos de redes de datos

2.1.1.1. *Por su extensión*

Existen distintos tipos de redes dependiendo de muchos factores, pasamos a enumerar solo los tipos más comunes en función de su extensión o alcance:

2.1.1.1.1. *PAN (Personal Area Network)*

La red de área personal es la interconexión de periféricos que se puede encontrar tanto a unos pocos centímetros, como a metros de distancia del emisor, sus velocidades de transmisión son inferiores al megabit por segundo. El estándar más conocido es el bluetooth, que se utiliza para el intercambio de archivos «Persona a Persona» (Person to Person, Peer-to-Peer o P2P) o «Terminal a Terminal » (Device-to-Device o D2D).

2.1.1.1.2. *LAN (Local Area Network)*

La red de área local es la que suele situarse en el mismo edificio o en entornos de unos 200 m, llegando al kilómetro con repetidores, o a 450 m en versiones inalámbricas.

“Una red de área local (LAN) es una red de "alta" velocidad (decenas de Megabits), generalmente confinada a un mismo piso o edificio.” (Universidad del Azuay)

2.1.1.1.3. *CAN (Campus Area Network)*

La red de área campus posee una extensión de un campus universitario, una base militar, un polígono industrial o un grupo de grandes edificios en un área geográfica limitada. Las dimensiones solían ser superiores a las de las redes locales, sin embargo, tienen la misma tecnología, ya que suelen ser del mismo propietario. Muchos la consideran como un subtipo de las redes MAN.

2.1.1.1.4. *MAN (Metropolitan Area Network)*

La red de área metropolitana es la que se sitúa en un barrio, urbanización, ciudad o municipio pequeño (a pocos kilómetros, normalmente oscila entre 1 y 7 Km y excepcionalmente puede llegar a decenas de kilómetros con repetidores).

2.1.1.1.5. WAN (Wide Area Network)

Es la red de área mundial o red de área amplia (varios países, un continente o incluso mundial). Estas redes suelen estar diseñadas para la interconexión de redes.

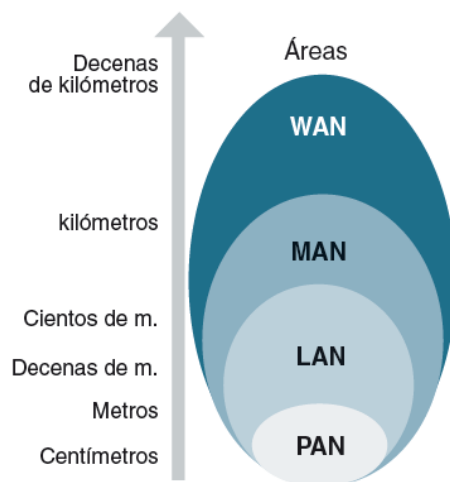


Fig. 2. Tipos de redes
Fuente: (Redes Locales, 2011, pág. 24)

4.1.2. Modelo OSI

El modelo OSI se basa en una propuesta desarrollada por la Organización Internacional de Normas (ISO) como el primer paso hacia la estandarización internacional de los protocolos utilizados en las diversas capas. El Modelo de referencia OSI (Interconexión de Sistemas Abiertos/ Open Systems Interconnection) se ocupa de la conexión de sistemas abiertos; esto es, sistemas que están abiertos a la comunicación con otros sistemas.

El modelo OSI tiene siete capas. Los principios que se aplicaron para llegar a las siete capas se pueden resumir de la siguiente manera:

- Se debe crear una capa en donde se requiera un nivel diferente de abstracción.
- Cada capa debe realizar una función bien definida.
- La función de cada capa se debe elegir teniendo en cuenta la definición de protocolos estandarizados internacionalmente.

- Es necesario elegir los límites de las capas de modo que se minimice el flujo de información a través de las interfaces.
- La cantidad de capas debe ser suficiente como para no tener que agrupar funciones distintas en la misma capa; además, debe ser lo bastante pequeña como para que la arquitectura no se vuelva inmanejable.

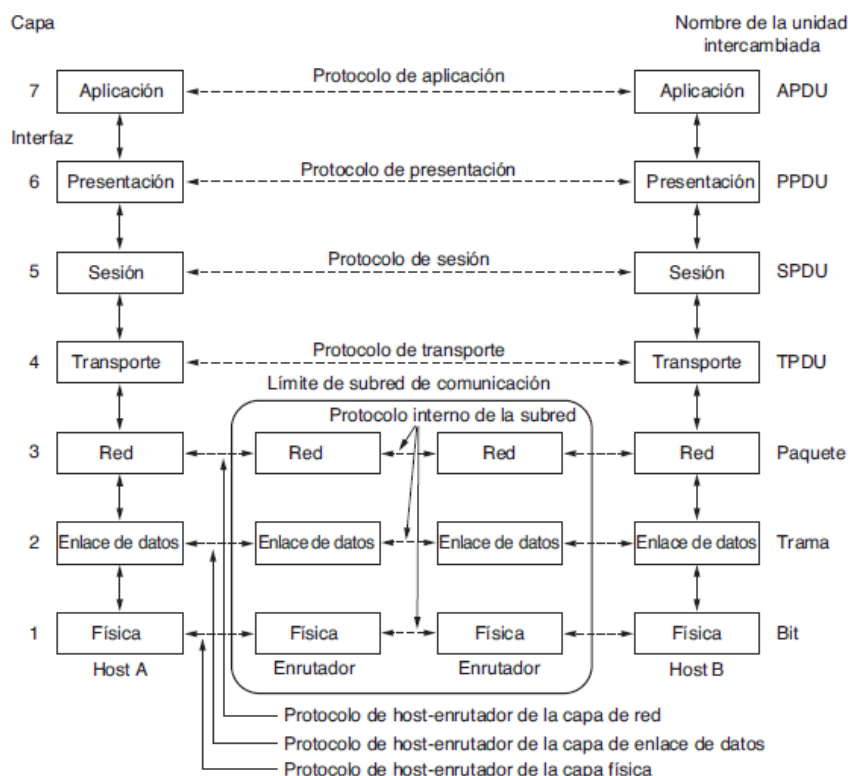


Fig. 3. Modelo OSI

Fuente: (Redes de Computadoras, 2012, pág. 36)

El modelo OSI en sí no es una arquitectura de red, ya que no especifica los servicios y protocolos exactos que se van a utilizar en cada capa. Sólo indica lo que una debe hacer.

4.1.2.1. Capa Física

La capa física se relaciona con la transmisión de bits puros a través de un canal de transmisión. Los aspectos de diseño tienen que ver con la acción de asegurarse que cuando uno de los lados envíe un bit 1 el otro lado lo reciba como un bit 1, no como un bit 0.

4.1.2.2. *Capa de Enlace de Datos*

La principal tarea de la capa de enlace de datos es transformar un medio de transmisión puro en una línea que esté libre de errores de transmisión. Enmascara los errores reales, de manera que la capa de red no los vea. Para lograr esta tarea, el emisor divide los datos de entrada en tramas de datos (por lo general, de algunos cientos o miles de bytes) y transmite las tramas en forma secuencial. Si el servicio es confiable, para confirmar la recepción correcta de cada trama, el receptor devuelve una trama de confirmación de recepción.

4.1.2.3. *Capa de Red*

La capa de red controla la operación de la subred. Una cuestión clave de diseño es determinar cómo se encaminan los paquetes desde el origen hasta el destino. Las rutas se pueden basar en tablas estáticas que se “codifican” en la red y rara vez cambian, aunque es más común que se actualicen de manera automática para evitar las fallas en los componentes.

4.1.2.4. *Capa de Transporte*

La función básica de la capa de transporte es aceptar datos de la capa superior, dividirlos en unidades más pequeñas si es necesario, pasar estos datos a la capa de red y asegurar que todas las piezas lleguen correctamente al otro extremo.

La capa de transporte también determina el tipo de servicio que debe proveer a la capa de sesión y, en última instancia, a los usuarios de la red.

4.1.2.5. *Capa de Sesión*

La capa de sesión permite a los usuarios en distintas máquinas establecer sesiones entre ellos. Las sesiones ofrecen varios servicios, incluyendo el control del diálogo (llevar el control de quién va a transmitir), el manejo de tokens (evitar que dos partes intenten la misma operación crítica al mismo tiempo) y la sincronización (usar puntos de referencia en las transmisiones extensas para reanudar desde el último punto de referencia en caso de una interrupción).

4.1.2.6. *Capa de Presentación*

A diferencia de las capas inferiores, que se enfocan principalmente en mover los bits de un lado a otro, la capa de presentación se enfoca en la sintaxis y la semántica de la información transmitida. Para hacer posible la comunicación entre computadoras con distintas representaciones internas de datos, podemos definir de una manera abstracta las estructuras de datos que se van a intercambiar, junto con una codificación estándar que se use “en el cable”. La capa de presentación maneja estas estructuras de datos abstractas y permite definir e intercambiar estructuras de datos de mayor nivel (por ejemplo, registros bancarios).

4.1.2.7. *Capa de Aplicación*

La capa de aplicación contiene una variedad de protocolos que los usuarios necesitan con frecuencia. Un protocolo de aplicación muy utilizado es HTTP (Protocolo de Transferencia de Hipertexto, HyperText Transfer Protocol), el cual forma la base para la World Wide Web. Cuando un navegador desea una página web, envía el nombre de la página que quiere al servidor que la hospeda mediante el uso de HTTP. Después el servidor envía la página de vuelta. Hay otros protocolos de aplicación que se utilizan para transferir archivos, enviar y recibir correo electrónico y noticias.

4.1.3. Protocolos

El protocolo de red establece la semántica y la sintaxis del intercambio de información, algo que constituye un estándar. Las computadoras en red, de este modo, tienen que actuar de acuerdo a los parámetros y los criterios establecidos por el protocolo en cuestión para lograr comunicarse entre sí y para recuperar datos que, por algún motivo, no hayan llegado a destino. (Definicion.de, 2008)

4.1.3.1. Modelo de Referencia TCP/IP

TCP/IP fue desarrollado y presentado por el Departamento de Defensa de EE.UU. En 1972 y fue aplicado en ARPANET (Advanced Research Projects Agency Network), que era la red de área extensa del Departamento de Defensa como medio de comunicación para los diferentes organismos de EE.UU. La transición hacia TCP/IP en ARPANET se concretó en 1983.

El modelo TCP/IP es implementado por la pila de protocolos sobre los cuales se fundamenta Internet y que permiten la transmisión de datos entre las redes de computadoras.

Los dos protocolos más importantes y que fueron también los primeros en definirse y también los más utilizados, son TCP e IP, de ahí que se denomine también como Conjunto de Protocolos TCP/IP.

4.1.3.1.1. Estructura Interna

La arquitectura está basada en capas. Esto hace más fácil implementar nuevos protocolos. El conjunto de protocolos TCP/IP, al estar integrado plenamente en Internet, también dispone de este tipo de arquitectura.

4.1.3.1.1.1. Capa Física

La capa física en una red TCP/IP es idéntica a la capa física del modelo ISO/OSI, la cual incluye el medio de transmisión que transporta los datos por la red. Este medio es casi siempre algún tipo de cable coaxial, par trenzado o fibra óptica. El modelo TCP/IP no considera oficialmente el medio hardware como componente específico en su diseño. TCP/IP tiende a agrupar la interfaz hardware con el nivel de interfaz de red.

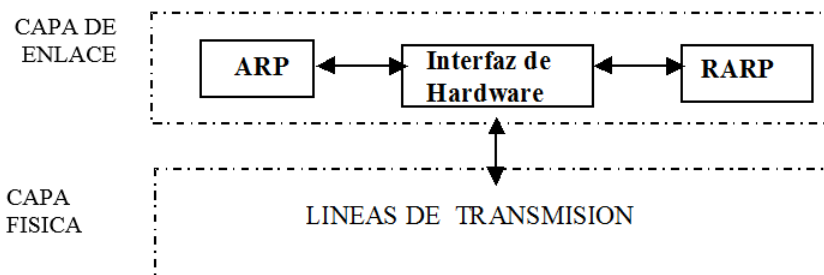


Fig. 4. Capa física relacionada con la Capa de Enlace
Fuente: (Metodología para la implementación de Intranets, 2013, p. 20)

4.1.3.1.1.2. Capa de Enlace

La capa de enlace incluye una interfaz de Hardware y dos módulos de protocolos: El Protocolo de Resolución de Direcciones (ARP) y el Protocolo de Resolución de Direcciones Inverso (RARP).

Las direcciones Ethernet (a nivel físico) son de seis bytes de longitud, mientras las direcciones IP son de cuatro bytes. Todos los datos transmitidos a través de la red mediante tecnología Ethernet deben utilizar tramas de datos Ethernet; las tarjetas de interface Ethernet observan las tramas en la red en busca de sus propias direcciones Ethernet. Las tarjetas de interface no saben ni se preocupan por la dirección IP.

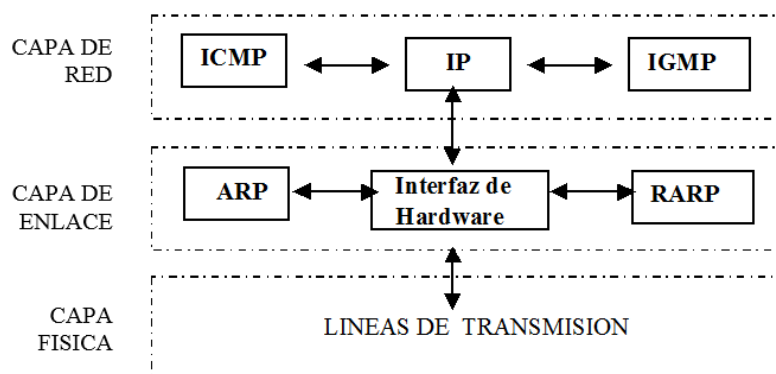


Fig. 5. Capa de Enlace relacionada con Capa Física y Capa de Red.
Fuente: (Metodología para la implementación de Intranets, 2013, p. 21)

En otras palabras, los protocolos de TCP/IP sólo funcionan con direcciones IP; las tramas Ethernet con direcciones Ethernet. Estos diferentes tipos de direcciones representan un problema de comunicación en la red. Los protocolos de Resolución de Direcciones y de Resolución de Direcciones Inverso solucionan

este problema analizando las direcciones: traducen las direcciones IP a direcciones de la capa de enlace y viceversa.

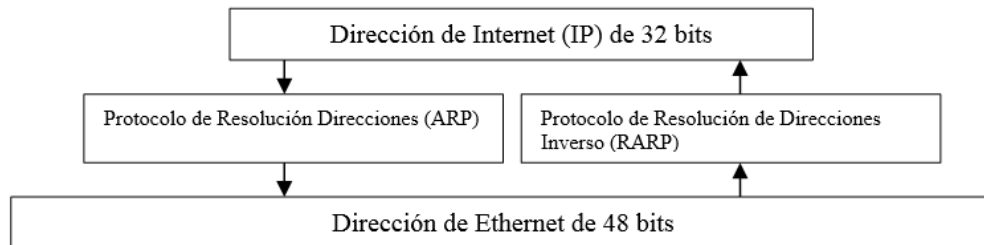


Fig. 6. Traducción de direcciones IP a Ethernet.

Fuente: (Metodología para la implementación de Intranets, 2013, p. 22)

4.1.3.1.1.2.1. ARP (Address Resolution Protocol)

El protocolo de resolución de direcciones se usa para traducir las direcciones IP (lógicas) en direcciones de la red local (físicas).

4.1.3.1.1.2.2. RARP (Reverse Address Resolution Protocol)

El protocolo de resolución de direcciones reverso es el encargado de asignar una dirección física a una dirección lógica (IP).

4.1.3.1.1.3. Capa de Red

La capa de red es el núcleo de cualquier red basada en el protocolo TCP/IP. Esta capa incluye: IP, ICMP y el protocolo IGMP. IP hace casi todo el trabajo dentro de la capa de red. ICMP e IGMP son protocolos de apoyo para IP, pues lo ayudan a manejar los mensajes especiales de la red, como los de error y de transmisiones múltiples (mensajes enviados a dos o más sistemas).

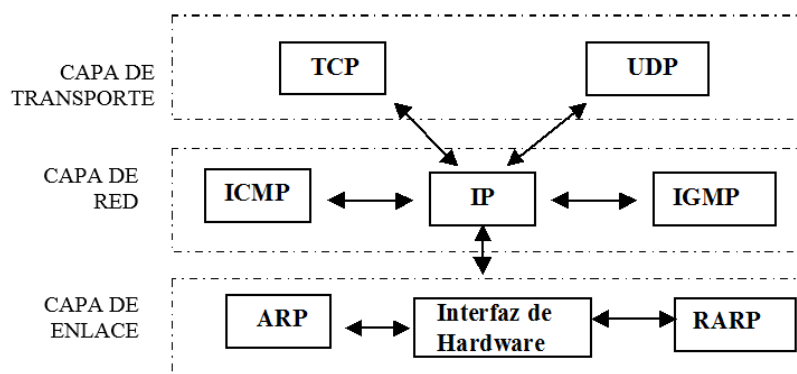


Fig. 7. Capa de Red relacionada con la capa Enlace y capa de Transporte.

Fuente: (Metodología para la implementación de Intranets, 2013, p. 23)

Además la capa de red controla la comunicación entre un equipo y otro. Conformar los paquetes IP que serán enviados por la capa inferior; desencapsula los paquetes recibidos pasando a la capa superior la información dirigida a una aplicación. (Metodología para la implementación de Intranets, 2013, p. 24)

4.1.3.1.1.3.1. IP (Internet Protocol)

El protocolo de internet y sus protocolos de enrutamiento asociados son posiblemente la parte más significativa del conjunto TCP/IP. El protocolo IP se encarga de:

- Direcciones IP: Las convenciones de direcciones IP forman parte del protocolo IP.
- Comunicaciones de host a host: El protocolo IP determina la ruta que debe utilizar un paquete, basándose en la dirección IP del sistema receptor.
- Formato de paquetes: el protocolo IP agrupa paquetes en unidades conocidas como datagramas.
- Fragmentación: Si un paquete es demasiado grande para su transmisión a través del medio de red, el protocolo IP del sistema de envío divide el paquete en fragmentos de menor tamaño. A continuación, el protocolo IP del sistema receptor reconstruye los fragmentos y crea el paquete original. (Oracle, 2010)

4.1.3.1.1.3.2. ICMP (Internet Control Message Protocol)

Internet es un sistema autónomo que no dispone de ningún control central. El protocolo de Mensajes de control de internet proporciona el medio para que el software de hosts y gateways intermedios se comuniquen. El protocolo ICMP tiene su propio número de protocolo (número 1), que lo habilita para utilizar el IP directamente. La implementación de ICMP es obligatoria como un subconjunto lógico del protocolo IP. Los mensajes de error de este protocolo los genera y procesa TCP/IP, y no el usuario

ICMP sólo proporciona servicios para notificar errores, es decir que no proporciona ningún servicio de corrección de errores, además, no especifica

ninguna acción que los módulos de software de la capa de red deben tomar en respuesta a los errores que reporta.

4.1.3.1.1.3.3. IGMP (*Internet Group Management Protocol*)

El protocolo de manejo de grupos de internet funciona como una extensión del protocolo IP. Se utiliza exclusivamente por los miembros de una red multicast para mantener su status de miembros, o para propagar información de direccionamiento.

4.1.3.1.1.4. *Capa de Transporte.*

Para comunicarse con Internet, las aplicaciones que se utilizan intercambian datos con la capa de transporte TCP/IP. Esta incluye dos protocolos de transporte: TCP y UDP.

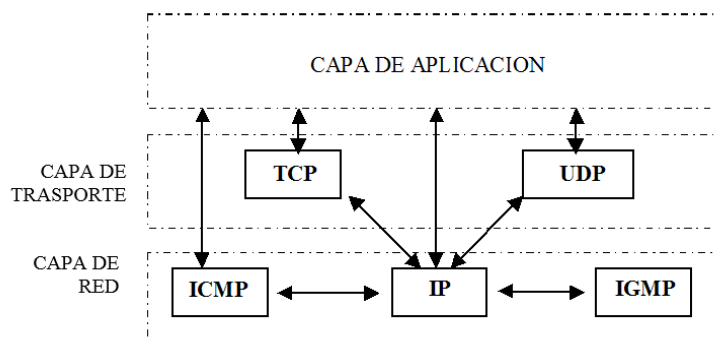


Fig. 8. Capa de Transporte relacionada con las Capa de Red y Aplicación.
Fuente: (Metodología para la implementación de Intranets, 2013, p. 30)

4.1.3.1.1.4.1. *UDP (User Datagram Protocol)*

El protocolo de datagrama de usuario proporciona aplicaciones con un tipo de servicio de datagramas orientado a transacciones. El servicio es muy parecido al protocolo IP en el sentido de que no es fiable y no está orientado a la conexión. El UDP es simple, eficiente e ideal para aplicaciones como el TFTP y el DNS. Una dirección IP sirve para dirigir el datagrama hacia una máquina en particular, y el número de puerto de destino en la cabecera UDP se utiliza para dirigir el datagrama UDP a un proceso específico localizado en la cabecera IP. La

cabecera UDP también contiene un número de puerto origen que permite al proceso recibido conocer cómo responder al datagrama.

4.1.3.1.1.4.2. TCP (Transmission Control Protocol)

Al igual que UDP, TCP transporta datos entre las capas de red y de aplicación, pero es mucho más complejo que UDP, pues proporciona un servicio de entrega de datos confiable, de flujo de bytes y orientado a conexión; en otras palabras, TCP asegura la entrega, así como también se encarga que la aplicación destino reciba los datos en la secuencia correcta. En contraste, UDP no garantiza la entrega de datagramas, ni que estos lleguen en la secuencia adecuada.

TCP también intenta optimizar el ancho de banda de la red. Para hacerlo, controla dinámicamente el flujo de datos entre las conexiones. Por lo tanto, si el buffer de datos en el lado receptor de la conexión TCP comienza a sobrecargarse, TCP indica al lado emisor que reduzca la velocidad de transmisión.

4.1.3.1.1.5. Capa de Aplicación.

Este es el punto en que el modelo OSI y el modelo TCP/IP empiezan a ir por caminos separados. TCP/IP reconoce cualquier cosa a partir de este punto como un protocolo de aplicación, mientras que el modelo OSI descompone aún más las descripciones.

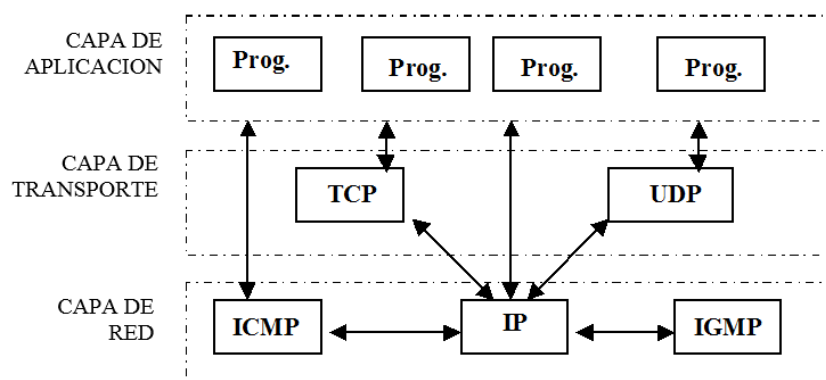


Fig. 9. Relación entre la Capa de Aplicación con capas inferiores.
Fuente: (Metodología para la implementación de Intranets, 2013, p. 36)

En la actualidad se utilizan cientos de protocolos de aplicación. Algunos están todavía en fase experimental, otros están en espera de un reconocimiento formal.

4.1.3.1.1.5.1. TELNET (Telecommunicating Networks)

Las aplicaciones de acceso remoto, también llamadas TELNET nos permiten acceder a un servidor emulando un terminal que se encontrase físicamente conectado a él.

4.1.3.1.1.5.2. FTP. (File Transfer Protocol)

El protocolo para transmisión de archivos permite la transferencia de archivos entre dos ordenadores. Define la manera en que los datos deben ser transferidos a través de una red TCP/IP.

El objetivo del protocolo FTP es:

- Permitir que equipos remotos puedan compartir archivos.
- Permitir la independencia entre los sistemas de archivo del equipo del cliente y del equipo del servidor.
- Permitir una transferencia de datos eficaz.

4.1.3.1.1.5.3. HTTP (HyperText Transfer Protocol)

El protocolo para la transferencia de Hipertexto es el conjunto de reglas para la transmisión y recepción de documentos hipertexto. Es usado por la WWW desde 1990 y es el protocolo responsable del entendimiento universal de las páginas de la WWW escritas en HTML.

HTTP se diseñó específicamente para el World Wide Web: es un protocolo rápido y sencillo que permite la transferencia de múltiples tipos de información de forma eficiente y rápida. Se puede comparar, por ejemplo, con FTP, que es también un protocolo de transferencia de ficheros, pero tiene un conjunto muy amplio de comandos, y no se integra demasiado bien en las transferencias multimedia.

4.1.3.1.1.5.4. NNTP (Network News Transfer Protocol)

El protocolo de transferencia de noticias por red permite la distribución, petición, recuperación y envío de news (noticias) entre los servidores de news de la comunidad ARPA-Internet a través de USENET utilizando un sistema cliente-servidor con intercambio fiable de información (TCP). Está diseñado de forma y manera que los artículos están en un host, que actúa de servidor de news, y los usuarios "enganchados" a otros hosts de la misma red pueden acceder a los artículos a través de la conexión de éstos con el servidor central de news.

4.1.3.1.1.5.5. SMTP (Simple Mail Transport Protocol)

El protocolo simple de transferencia de correo hace uso de los dominios para transferir los mensajes, pero para conocer la dirección de red de un dominio dado, usa los servicios de un DNS o sistema de nombres de dominio; que convierte un nombre de dominio dado en una dirección IP

4.1.3.1.1.5.6. POP3 (Protocolo de Oficina Postal).

El protocolo de oficina postal fue diseñado para trabajar conjuntamente con el protocolo TCP, inicialmente el proceso está escuchando el puerto 110, a la espera de una conexión, cuando esta se establece el servidor envía un saludo y luego comienza un diálogo en el que se intercambian comandos y respuestas, hasta que la conexión se libera.

El Protocolo de correo- Versión 3 (POP3) fue creado para permitir a una red el acceso dinámico a una casilla sobre un servidor HOST de manera útil. Usualmente, esto significa que el protocolo POP3 es usado para dejar que una red recupere el correo que el servidor accionaría por él. POP3 no está hecho para proveer operaciones de manipulación extensivas de correo en el servidor; normalmente, el correo es bajado y es borrado.

4.1.3.1.1.5.7. IMAP (Internet Mail Access Protocol)

El protocolo de acceso a mensajes de Internet es un protocolo alternativo al de POP3; permite a los usuarios acceder a sus e-mails directamente en el servidor y sólo descargar, hacia la máquina local, los mensajes y archivos adjuntos que le resulten de interés. Esto ahorra tiempo de descarga.

4.1.3.1.1.5.8. MIME (*Multipurpose Internet Mail Extensions*)

El protocolo MIME (extensiones multipropósito de correo de internet) define una metodología para codificar mensajes con contenido más complejo que el texto común. Una parte importante del MIME está dedicada a mejorar las posibilidades de transferencia de texto en distintos idiomas y alfabetos. En sentido general las extensiones de MIME van encaminadas a soportar:

- Texto en conjuntos de caracteres distintos de US-ASCII;
- adjuntos que no son de tipo texto;
- cuerpos de mensajes con múltiples partes (multi-part);
- información de encabezados con conjuntos de caracteres distintos de ASCII.

2.2. COMPRESIÓN DE VIDEO DIGITAL

Las técnicas de compresión de vídeo consisten en reducir y eliminar datos redundantes del vídeo para que el archivo de vídeo digital se pueda enviar a través de la red y almacenar en discos informáticos. Con técnicas de compresión eficaces se puede reducir considerablemente el tamaño del fichero sin que ello afecte muy poco, o en absoluto, la calidad de la imagen. Sin embargo, la calidad del vídeo puede verse afectada si se reduce en exceso el tamaño del fichero aumentando el nivel de compresión de la técnica que se utilice.

Existen diferentes técnicas de compresión, tanto patentadas como estándar. Hoy en día, la mayoría de proveedores de vídeo en red utilizan técnicas de compresión estándar. Los estándares son importantes para asegurar la compatibilidad y la interoperabilidad. Tienen un papel especialmente relevante en la compresión de vídeo, puesto que éste se puede utilizar para varias finalidades y, en algunas aplicaciones de video vigilancia, debe poderse visualizar varios años después de su grabación. Gracias al desarrollo de estándares, los usuarios finales tienen la opción de escoger entre diferentes proveedores, en lugar de optar a uno solo para su sistema de video vigilancia.

2.2.1. Códec de vídeo

En el proceso de compresión se aplica un algoritmo al vídeo original para crear un archivo comprimido y ya listo para ser transmitido o guardado. Para reproducir el archivo comprimido, se aplica el algoritmo inverso y se crea un vídeo que incluye prácticamente el mismo contenido que el vídeo original. El tiempo que se tarda en comprimir, enviar, descomprimir y mostrar un archivo es lo que se denomina latencia. Cuanto más avanzado sea el algoritmo de compresión, mayor será la latencia.

El par de algoritmos que funcionan conjuntamente se denomina códec de vídeo (codificador/ decodificador). Los códec de vídeo de estándares diferentes no suelen ser compatibles entre sí, es decir, el contenido de vídeo comprimido con un estándar no se puede descomprimir con otro estándar diferente. Por ejemplo, un decodificador MPEG-4 no funcionará con un codificador H.264. Esto ocurre simplemente porque un algoritmo no puede descodificar correctamente los datos de salida del otro algoritmo, pero es posible usar muchos algoritmos diferentes en el mismo software o hardware, que permitirían la coexistencia de varios formatos. (Compresión de video, 2013)

2.2.1.1. *Compresión de imagen vs. Compresión de vídeo*

Los diferentes estándares de compresión utilizan métodos distintos para reducir los datos y, en consecuencia, los resultados en cuanto a frecuencia de bits y latencia son diferentes. Existen dos tipos de algoritmos de compresión: compresión de imágenes y compresión de vídeo.

La compresión de imagen utiliza la tecnología de codificación intrafotograma. Los datos se reducen a un fotograma de imagen con el fin de eliminar la información innecesaria que puede ser imperceptible para el ojo humano. Motion JPEG es un ejemplo de este tipo de estándar de compresión. En una secuencia Motion JPEG, las imágenes se codifican o comprimen como imágenes JPEG individuales.



Fig. 10. Formato Motion JPEG.
Fuente: (Compresión de vídeo, 2013)

Con el formato Motion JPEG, las tres imágenes de la secuencia se codifican y se envían como imágenes únicas y separadas (fotogramas I), sin que dependan unas de otras.

Los algoritmos de compresión de vídeo-4 como el MPEG-4 y el H.264 utilizan la predicción interfotograma para reducir los datos de vídeo entre las series de fotogramas. Ésta consiste en técnicas como la codificación diferencial, en la que un fotograma se compara con un fotograma de referencia y sólo se codifican los píxeles que han cambiado con respecto al fotograma de referencia. De esta forma, se reduce el número de valores de píxeles codificados y enviados. Cuando se visualiza una secuencia codificada de este modo, las imágenes aparecen como en la secuencia de vídeo original.

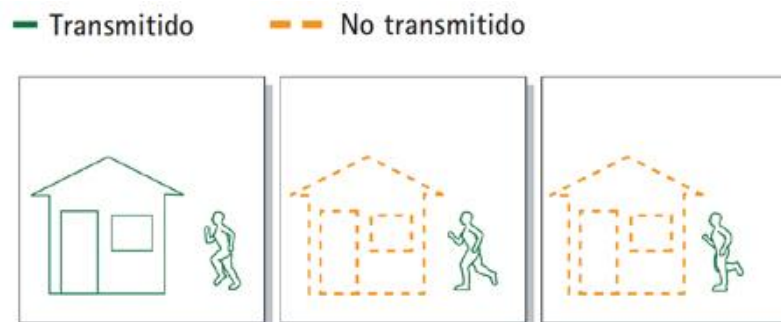


Fig. 11. Codificación diferencial.
Fuente: (Compresión de vídeo, 2013)

Con la codificación diferencial sólo la primera imagen (fotograma I) se codifica en su totalidad. En las dos imágenes siguientes (fotogramas P) existen referencias a la primera imagen en lo que se refiere a elementos estáticos, como la casa. Sólo se codifican las partes en movimiento (el hombre que corre) mediante vectores de movimiento, reduciendo así la cantidad de información que se envía y almacena.

Para reducir aún más los datos, se pueden aplicar otras técnicas como la compensación de movimiento basada en bloques. La compensación de movimiento basada en bloques tiene en cuenta que gran parte de un fotograma nuevo está ya incluido en el fotograma anterior, aunque quizás en un lugar diferente del mismo. Esta técnica divide un fotograma en una serie de macrobloques (bloques de píxeles). Se puede componer o “predecir” un nuevo fotograma bloque a bloque, buscando un bloque que coincida en un fotograma de referencia. Si se encuentra una coincidencia, el codificador codifica la posición en la que se debe encontrar el bloque coincidente en el fotograma de referencia. La codificación del vector de movimiento, como se denomina, precisa de menos bits que si hubiera de codificarse el contenido real de un bloque.

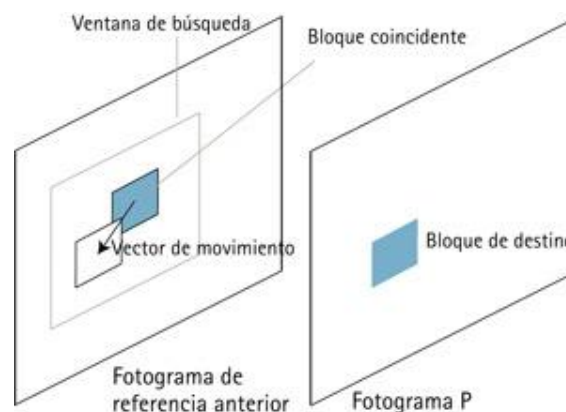


Fig. 12. Compensación de movimiento basada en bloques.
Fuente: (Compresión de video, 2013)

Con la predicción interfotograma, cada fotograma de una secuencia de imágenes se clasifica como un tipo de fotograma concreto, como un fotograma I, P o B.

Un fotograma I, o intrafotograma, es una imagen autónoma que se puede codificar de forma independiente sin hacer referencia a otras imágenes. La primera imagen de una secuencia de vídeo es siempre un fotograma I. Los fotogramas I sirven como puntos de inicio en nuevas visualizaciones o como puntos de resincronización si la transmisión de bits resulta dañada. Los fotogramas I se pueden utilizar para implementar funciones de avance o retroceso rápido o de acceso aleatorio. Un codificador insertará automáticamente fotogramas I a intervalos regulares o a petición de nuevos clientes que puedan

incorporarse a la visualización de una transmisión. La desventaja de este tipo de fotogramas es que consumen muchos más bits, pero por otro lado no generan demasiados defectos provocados por los datos que faltan.

Un fotograma P (de interfotograma Predictivo), hace referencia a partes de fotogramas I o P anteriores para codificar el fotograma. Los fotogramas P suelen requerir menos bits que los fotogramas I, pero con la desventaja de ser muy sensibles a la transmisión de errores, debido a la compleja dependencia con fotogramas P o I anteriores.

Un fotograma B, o interfotograma Bipredictivo, es un fotograma que hace referencia tanto a fotogramas anteriores como posteriores. El uso de fotogramas B aumenta la latencia.

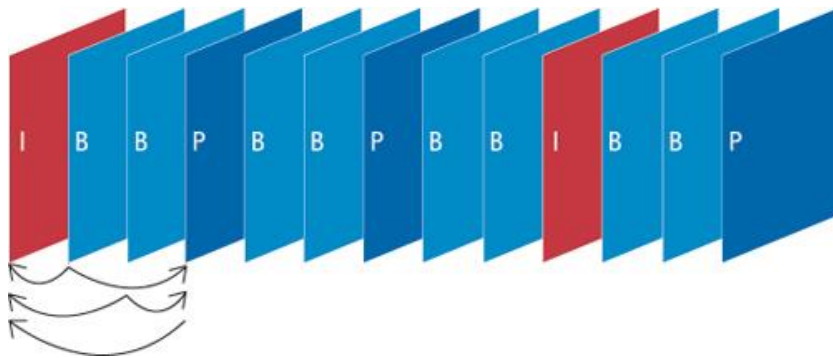


Fig. 13. Secuencia con fotogramas.
Fuente: (Compresión de vídeo, 2013)

Secuencia típica con fotogramas I, B y P. Un fotograma P sólo puede hacer referencia a fotogramas I o P anteriores, mientras que un fotograma B puede hacerlo a fotogramas I o P tanto anteriores como posteriores.

Cuando un decodificador de vídeo restaura un vídeo descodificando la transmisión de bits fotograma a fotograma, la descodificación debe comenzar siempre por un fotograma I. Los fotogramas P y B, en caso de usarse, deben descodificarse junto a los fotogramas de referencia.

Los productos de vídeo en red Axis permiten a los usuarios configurar la longitud de GOV (grupo de vídeo), la cual determina la cantidad de fotogramas P que se deberían enviar antes de realizar el envío de otro fotograma I. La frecuencia de

bits se puede disminuir mediante la reducción de la frecuencia de fotogramas I (GOV más largo). Para reducir la latencia no se utilizan fotogramas B.

Además de la codificación diferencial y la compensación de movimiento, se pueden emplear otros métodos avanzados para reducir aún más los datos y mejorar la calidad de vídeo. El H.264, por ejemplo, admite técnicas avanzadas como los esquemas de predicción para codificar fotogramas I, la compensación de movimiento mejorada con una precisión inferior a un píxel y el filtro de eliminación de bloques en bucle para suavizar los bordes de los bloques (defectos). (Compresión de video, 2013)

2.2.2. Formatos de compresión

2.2.2.1. Motion JPEG

Motion JPEG o M-JPEG es una secuencia de vídeo digital compuesta por una serie de imágenes JPEG individuales. (JPEG - Joint Photographic Experts Group - Grupo de Expertos Fotográficos Unidos). Cuando se visualizan 16 o más imágenes por segundo, el ojo humano lo percibe como un vídeo en movimiento. Un vídeo en completo movimiento se percibe a 30 (NTSC) o 25 (PAL) imágenes por segundo.

Una de las ventajas de Motion JPEG es que cada imagen de una secuencia de vídeo puede conservar la misma calidad garantizada que se determina mediante el nivel de compresión elegido para la cámara de red o codificador de vídeo. Cuanto más alto es el nivel de compresión, menor es el tamaño del archivo y la calidad de imagen. En algunas situaciones, como cuando hay poca luz o la escena es compleja, el tamaño del archivo puede ser bastante grande y, por lo tanto, usar más ancho de banda y espacio de almacenamiento.

Al no haber dependencia alguna entre los fotogramas de Motion JPEG, un vídeo Motion JPEG es resistente, lo que significa que si falla un fotograma durante la transmisión, el resto del vídeo no se verá afectado.

Motion JPEG es un estándar que no requiere licencia. Tiene una amplia compatibilidad y su uso es muy habitual en aplicaciones donde se requieren fotogramas individuales en una secuencia de vídeo y donde se utiliza una frecuencia de imagen de 5 fotogramas por segundo o inferior. Motion JPEG también puede ser útil para aplicaciones que requieren integración con sistemas que sólo son compatibles con Motion JPEG. (Formatos de compresión, 2013)

Sin embargo, el principal inconveniente de Motion JPEG es que no utiliza ninguna técnica de compresión de vídeo para reducir datos, ya que consiste en una serie de imágenes fijas y completas. El resultado es una frecuencia de bits relativamente alta o una relación de compresión baja para la calidad proporcionada, en comparación con estándares de compresión de vídeo como MPEG-4 y H.264.

2.2.2.2. *MPEG-4*

Cuando se menciona MPEG-4 en las aplicaciones de video vigilancia, normalmente nos referimos a MPEG-4 Parte 2, también conocido como MPEG-4 Visual. Como todos los estándares MPEG (Moving Picture Experts Group), requiere una licencia, es decir, los usuarios deben pagar una tasa de licencia por cada estación de supervisión. MPEG-4 es compatible con aplicaciones de ancho de banda reducido y aplicaciones que requieren imágenes de alta calidad, sin limitaciones de frecuencia de imagen y con un ancho de banda virtualmente ilimitado.

2.2.2.3. *H.264 o MPEG-4 Part 10/AVC*

El H.264, también conocido como MPEG-4 Parte 10/AVC para Codificación de Vídeo Avanzada, es el estándar MPEG más actual para la codificación de vídeo. Se espera que el H.264 se convierta en la alternativa de estándar en los próximos años. Ello se debe a que, sin comprometer la calidad de la imagen, un codificador H.264 puede reducir el tamaño de un archivo de vídeo digital en más de un 80% si se compara con el formato Motion JPEG, y hasta un 50% más en comparación con el estándar MPEG-4. Esto significa que se requiere menos ancho de banda y espacio de almacenamiento para los archivos de vídeo. O, visto de otra manera,

se puede lograr mayor calidad de imagen de vídeo para una frecuencia de bits determinada.

El H.264 ha sido definido conjuntamente por organizaciones de normalización del sector de las telecomunicaciones (ITU-T's Video Coding Experts Group) y de las tecnologías de la información (ISO/IEC Moving Picture Experts Group), y se espera que tenga una mayor adopción que los estándares anteriores. En el sector de la video vigilancia, H.264 encuentra su mayor utilidad en aplicaciones donde se necesiten velocidades y resoluciones altas, como en la vigilancia de autopistas, aeropuertos y casinos, lugares donde por regla general se usa una velocidad de 30/25 (NTSC/PAL) imágenes por segundo. Es aquí donde las ventajas económicas de un ancho de banda y un almacenamiento reducidos se harán sentir de forma más clara.

Se espera que H.264 acelere también la adopción de cámaras megapíxel, ya que con esta eficiente tecnología de compresión se pueden reducir los archivos de gran tamaño y las frecuencias de bits sin que la calidad de la imagen se vea afectada. En cualquier caso, tiene sus exigencias: aunque H.264 permite ahorrar en costes de ancho de banda y almacenamiento, también necesita cámaras de red y estaciones de control de mejor rendimiento. (Formatos de compresión, 2013)

2.2.3. Frecuencia de bits variable y constante

Con el MPEG-4 y el H.264, los usuarios pueden determinar que una transmisión de vídeo codificado tenga una frecuencia de bits variable o constante. La selección óptima dependerá de la aplicación y de la infraestructura de red. (Frecuencia de bits variable y constante, 2013)

2.2.3.1. Frecuencia de bits variable

Con la VBR (frecuencia de bits variable), se puede mantener un nivel predefinido de calidad de imagen independientemente del movimiento o falta de movimiento en una escena. Esto significa que el uso de ancho de banda aumentará cuando haya mucha actividad en una escena, y disminuirá cuando no haya movimiento. A menudo esta opción es ideal para las aplicaciones de video vigilancia que

requieren una alta calidad, especialmente si hay movimiento en una escena. Debido a que la frecuencia de bits puede variar, incluso aunque se haya definido una frecuencia de bits media de destino, la infraestructura de red (ancho de banda disponible) debe poder adaptarse a grandes caudales de datos.

2.2.3.2. *Frecuencia de bits constante*

Con un ancho de banda limitado se recomienda utilizar el modo CBR (frecuencia de bits constante), ya que este modo genera una frecuencia de bits que el usuario puede predefinir. La desventaja que tiene la CBR es que si, por ejemplo, hay mucha actividad en una escena que da como resultado una frecuencia de bits mayor que la velocidad de destino, la restricción para mantener una frecuencia de bits constante conlleva una calidad y frecuencia de imagen inferiores. (Axis Communications, 2013)

2.2.4. **Comparación de estándares**

Al comparar los rendimientos de los estándares MPEG como el MPEG-4 y H.264, es importante tener en cuenta que los resultados pueden variar entre codificadores que usen el mismo estándar. Esto se debe a que el diseñador de un codificador puede elegir implementar diferentes conjuntos de herramientas definidas por un estándar. Siempre que los datos de salida de un codificador se ajusten al formato de un estándar, se pueden realizar implementaciones diferentes. De ahí que un estándar MPEG no pueda garantizar una frecuencia de bits o calidad determinadas, del mismo modo que no se puede realizar una comparación como es debido sin definir primero cómo se han implementado los estándares en un codificador. Un decodificador, a diferencia de un codificador, debe implementar todas las partes necesarias de un estándar para descodificar una transmisión de bits compatible. Un estándar especifica exactamente la forma en la que el algoritmo de descompresión debe restaurar cada bit de un vídeo comprimido.

El gráfico siguiente compara la frecuencia de bits, partiendo de la misma calidad de imagen, entre los siguientes estándares de vídeo: Motion JPEG, MPEG-4

Parte 2 (sin compensación de movimiento), MPEG-4 Parte 2 (con compensación de movimiento) y H.264 (perfil de base).

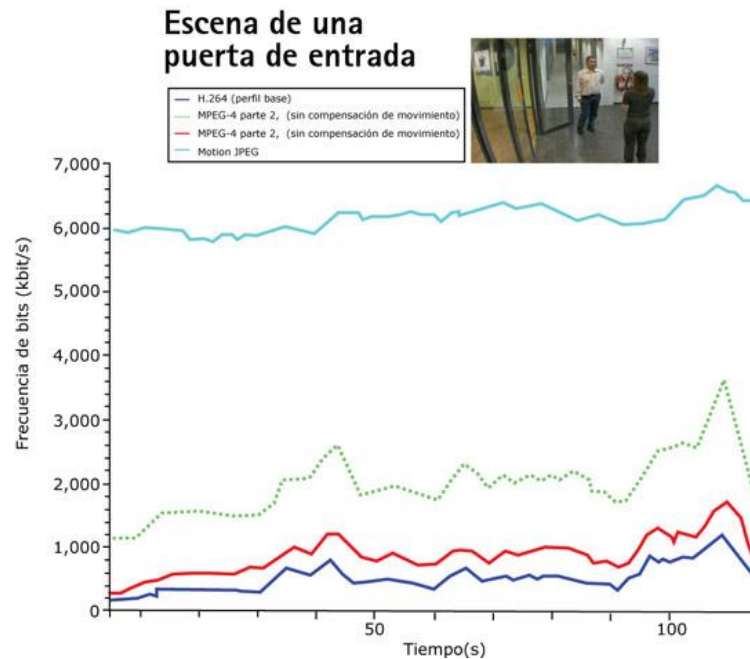


Fig. 14. Comparación de estándares.
Fuente: (Comparación de estándares, 2013)

Un codificador H.264 creó hasta un 50% menos bits por segundo para una secuencia de vídeo de muestra que un codificador MPEG-4 con compensación de movimiento. El codificador H.264 fue al menos tres veces más eficaz que un codificador MPEG-4 sin compensación de movimiento y al menos seis veces más eficaz que Motion JPEG. (Comparación de estándares, 2013)

2.3. VIDEO VIGILANCIA CCTV

Las siglas CCTV vienen del inglés “Closed Circuit Television” que traducido se conoce como “Circuito cerrado de televisión”. El objetivo de este sistema es la supervisión, el control y el eventual registro de la actividad física dentro de un local, espacio o ambiente en general. Se denomina circuito cerrado porque, a diferencia de la televisión tradicional, este solo permite un acceso limitado y restringido del contenido de las imágenes a los usuarios. (Axis Communications, 2013)

2.3.1. Evolución de los sistemas de vigilancia por vídeo

Los sistemas de vigilancia por vídeo existen desde hace 25 años. Empezaron siendo sistemas analógicos al 100% y paulatinamente se fueron digitalizando. Los sistemas de hoy en día han avanzado mucho desde la aparición de las primeras cámaras analógicas con tubo conectadas a VCR.

En la actualidad, estos sistemas utilizan cámaras y servidores de PC para la grabación de vídeo en un sistema completamente digitalizado. Sin embargo, entre los sistemas completamente analógicos y los sistemas completamente digitales existen diversas soluciones que son parcialmente digitales. Dichas soluciones incluyen un número de componentes digitales pero no constituyen sistemas completamente digitales.

2.3.1.1. Sistemas de circuito cerrado de TV analógicos usando VCR

Un sistema de circuito cerrado de TV (CCTV) analógico que utilice un VCR (grabador de vídeo) representa un sistema completamente analógico formado por cámaras analógicas con salida coaxial, conectadas al VCR para grabar.

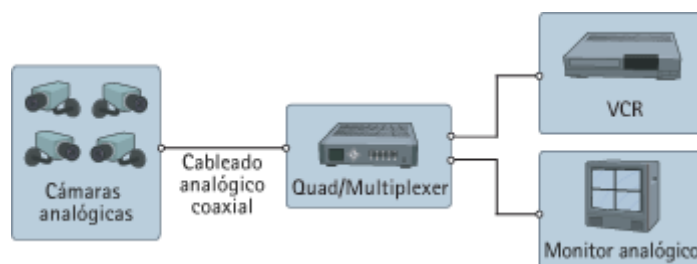


Fig. 15. Sistema de circuito cerrado de TV analógicos usando VCR.
Fuente: (La evolución de los sistemas de video vigilancia por video, 2013)

El VCR utiliza el mismo tipo de cintas que una grabadora doméstica. El vídeo no se comprime y, si se graba a una velocidad de imagen completa, una cinta durará como máximo 8 horas. En sistemas mayores, se puede conectar un quad o un multiplexor entre la cámara y el VCR. El quad/multiplexor permite grabar el vídeo procedente de varias cámaras en un solo grabador, pero con el inconveniente que tiene una menor velocidad de imagen. Para monitorizar el vídeo, es necesario un monitor analógico.

2.3.1.2. *Sistemas de circuito cerrado de TV analógicos usando DVR*

Un sistema de circuito cerrado de TV analógico usando un DVR (grabador de vídeo digital) es un sistema analógico con grabación digital. En un DVR, la cinta de vídeo se sustituye por discos duros para la grabación de vídeo, y es necesario que el vídeo se digitalice y comprima para almacenar la máxima cantidad de imágenes posible de un día.

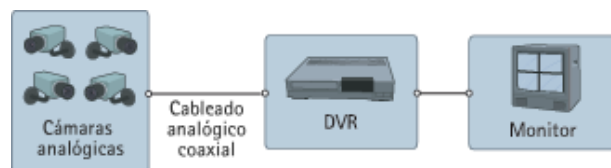


Fig. 16. Sistema de circuito cerrado de TV analógicos usando DVR.
Fuente: (La evolución de los sistemas de video vigilancia por video, 2013)

Con los primeros DVR, el espacio del disco duro era limitado, por tanto, la duración de la grabación era limitada, o debía usarse una velocidad de imagen inferior. El reciente desarrollo de los discos duros significa que el espacio deja de ser el principal problema. La mayoría de DVR disponen de varias entradas de vídeo, normalmente 4, 9 o 16, lo que significa que también incluyen la funcionalidad de los quads y multiplexores.

El sistema DVR añade las siguientes ventajas:

- No es necesario cambiar las cintas
- Calidad de imagen constante

2.3.1.3. *Sistemas de circuito cerrado de TV analógicos usando DVR de red*

Un sistema de circuito cerrado de TV analógico usando un DVR IP es un sistema parcialmente digital que incluye un DVR IP equipado con un puerto Ethernet para conectividad de red. Como el vídeo se digitaliza y comprime en el DVR, se puede transmitir a través de una red informática para que se monitorice en un PC en una ubicación remota.

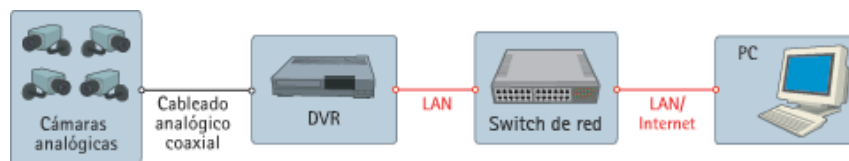


Fig. 17. Sistema de circuito cerrado de TV analógico usando DVR de red.
Fuente: (La evolución de los sistemas de video vigilancia por video, 2013)

Algunos sistemas pueden monitorizar tanto vídeo grabado como en directo, mientras otros sólo pueden monitorizar el vídeo grabado. Además, algunos sistemas exigen un cliente Windows especial para monitorizar el vídeo, mientras que otros utilizan un navegador web estándar, lo que flexibiliza la monitorización remota.

El sistema DVR IP añade las siguientes ventajas:

- Monitorización remota de vídeo a través de un PC
- Funcionamiento remoto del sistema

2.3.1.4. *Sistemas de vídeo IP que utilizan servidores de vídeo*

Un sistema de vídeo IP que utiliza servidores de vídeo incluye un servidor de vídeo, un conmutador de red y un PC con software de gestión de vídeo. La cámara analógica se conecta al servidor de vídeo, el cual digitaliza y comprime el vídeo. A continuación, el servidor de vídeo se conecta a una red y transmite el vídeo a través de un conmutador de red a un PC, donde se almacena en discos duros. Esto es un verdadero sistema de vídeo IP.

Un sistema de vídeo IP que utiliza servidores de vídeo añade las ventajas siguientes:

- Utilización de red estándar y hardware de servidor de PC para la grabación y gestión de vídeo
- El sistema es escalable en ampliaciones de una cámara cada vez
- Es posible la grabación fuera de las instalaciones
- Preparado para el futuro, ya que este sistema puede ampliarse fácilmente incorporando cámaras IP

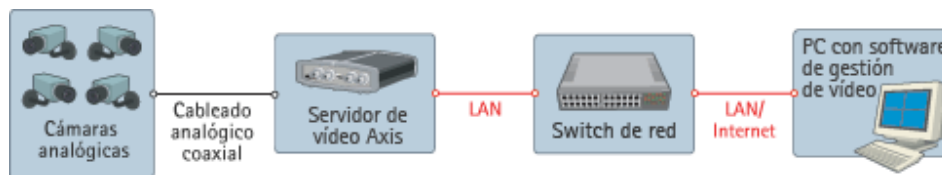


Fig. 18. Sistema de vídeo IP que utiliza servidor de vídeo.
Fuente: (La evolución de los sistemas de video vigilancia por video, 2013)

Este diagrama muestra un verdadero sistema de vídeo IP, donde la información del vídeo se transmite de forma continua a través de una red IP. Utiliza un servidor de vídeo como elemento clave para migrar el sistema analógico de seguridad a una solución de vídeo IP.

2.3.1.5. *Sistemas de vídeo IP que utilizan cámaras IP*

Una cámara IP combina una cámara y un ordenador en una unidad, lo que incluye la digitalización y la compresión del vídeo así como un conector de red. El vídeo se transmite a través de una red IP, mediante los conmutadores de red y se graba en un PC estándar con software de gestión de vídeo. Esto representa un verdadero sistema de vídeo IP donde no se utilizan componentes analógicos.

Un sistema de vídeo IP que utiliza cámaras IP añade las ventajas siguientes:

- Cámaras de alta resolución (megapíxel)
- Calidad de imagen constante
- Alimentación eléctrica a través de Ethernet y funcionalidad inalámbrica

- Funciones de Pan/tilt/zoom, audio, entradas y salidas digitales a través de IP, junto con el vídeo
- Flexibilidad y escalabilidad completas

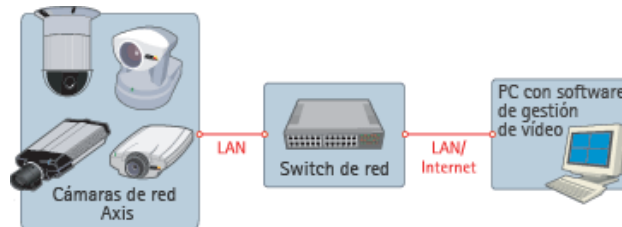


Fig. 19. Sistema de vídeo IP con cámaras IP.

Fuente: (La evolución de los sistemas de video vigilancia por video, 2013)

Este diagrama muestra un verdadero sistema de vídeo IP, donde la información del vídeo se transmite de forma continua a través de una red IP, utilizando cámaras IP. Este sistema saca el máximo partido de la tecnología digital y proporciona una calidad de imagen constante desde la cámara hasta el visualizador, dondequiera que estén. (Axis Communications, 2013)

2.3.2. Componentes de un sistema de cctv clásico

El sistema 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 requiera el usuario. Los componentes de este circuito pueden ser entonces: cámaras, conmutadores matriciales analógicos, grabadores digitales (Digital Video Record: DVR) o matrices de video (Video Matrix VMX).

Las cámaras se encuentran fijas en un lugar determinado. En un sistema moderno las cámaras que se utilizan pueden estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, inclinación y zoom. 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 Mata, 2011, pág. 11)

2.3.2.1. Cámaras analógicas

Una cámara de vigilancia análoga comienza con un sensor CCD y luego digitaliza la imagen para ser procesada posteriormente, pero antes de que el video sea enviado, deberá volver a convertirse en análogo para que pueda ser recibido por un equipo análogo como un monitor o grabador. Diferente a las cámaras IP, las cámaras análogas no tienen ningún tipo de servidor interno o codificadores y no requieren de mantenimiento técnico; estas funciones son implementadas en el equipo de control y grabación.

2.3.2.2. Monitores

La imagen creada y transmitida por la cámara analógica es transmitida a la posición de control y visualizada mediante monitores. Un monitor de CCTV es prácticamente el mismo que un receptor de televisión, un monitor analógico con entrada de antena. La característica que lo diferencia es la durabilidad de su pantalla.

2.3.2.3. Grabadoras

Las grabadoras de un sistema CCTV clásico sirven para poder ver, abalizar y hacer copias de seguridad de las cámaras. Normalmente han sido de cinta, pero en la actualidad y con el advenimiento de los sistemas IP, la grabación se lleva a cabo en discos duros, ya sea en un computador, o en equipos especializados para esta labor como los grabadores digitales autónomos.

2.3.2.4. Matriz de Video

Es un dispositivo que permite monitorear y conmutar muchas cámaras a un monitor de salida o múltiples monitores de salida, pudiendo desplegar cualquier imagen de sus cámaras de entrada en cualquiera de sus monitores de salida, ya sea a pantalla completa en forma intermitente o en secuencia preprogramada. La Matriz puede actuar como una interface entre las cámaras, los monitores y el puesto de control.

2.3.2.5. Líneas de transmisión

La señal de video que sale de la cámara debe llegar en las mejores condiciones posibles al monitor o monitores correspondientes, para lo cual se emplean las líneas de transmisión, que deben ser capaces de transportar la señal de video, que puede alcanzar frecuencias de 8MHz, con un mínimo de pérdidas. Usualmente el método de transmisión ha sido el cable coaxial, antecesor al cable UTP, usado en las modernas redes de video vigilancia IP.

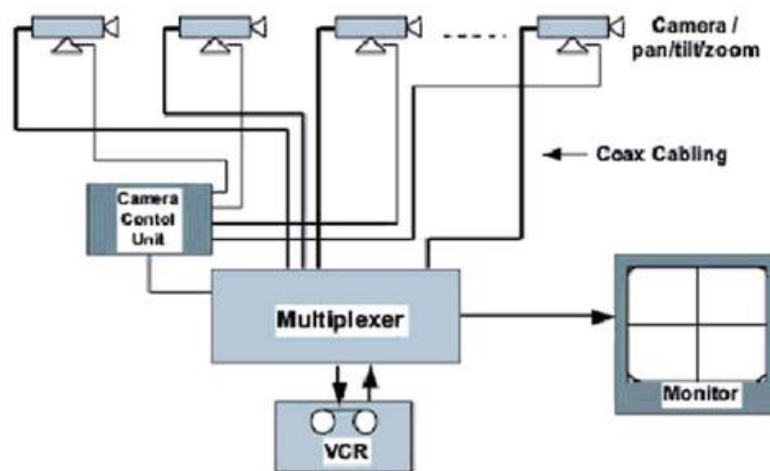


Fig. 20. Esquema básico de un sistema de CCTV analógico.
Fuente: (García Mata, 2011, pág. 13)

2.3.3. Descripción de los problemas comunes en los sistemas de video vigilancia tradicional o analógico

2.3.3.1. Resolución inadecuada de las cámaras

Las cámaras analógicas tienen una resolución ineficiente lo cual significa que en muchos de los casos no se puede identificar claramente el rostro de las personas.

Una cámara IP comprime la información de video mediante técnicas digitales, de esta manera, suprime redundancia, quita información que no es útil para el humano usa algoritmos avanzados para hacer cada vez más pequeña la cantidad de información para que las imágenes digitalizadas lleguen a su destino con buena resolución, velocidad y calidad, usando la mínima cantidad de recursos de la red de datos existente. Es decir usando el menor Ancho de Banda (BW) posible.

2.3.3.2. *Grabaciones inaudibles*

El registro de sonido es una parte fundamental dentro de la vigilancia especialmente en el área de juegos. Sin un registro de sonido no se puede tener evidencias de agresión o acoso verbal.

Las cámaras analógicas no pueden grabar sonido porque no tienen un micrófono incorporado a diferencia de las cámaras IP que incluso llegan a tener varias entradas de audio.

2.3.3.3. *Cámaras analógicas ubicadas sin un estudio previo*

Las cámaras deben ser ubicadas en lugares de difícil acceso para evitar que sean manipuladas por extraños y deben tener un buen ángulo de visión que permita vigilar las zonas conflictivas. Las cámaras analógicas del plantel tienen un ángulo de visión con muchos puntos ciegos además de estar ubicadas en puntos sin vigilancia lo cual hace que otras personas puedan acercarse a ellas sin ninguna restricción.

El tener una cámara en un lugar visible sirve para alertar a las personas de que están siendo vigiladas sin embargo si una persona sabe que está siendo grabada podría salir del campo de visión de la cámara, por esta razón el ángulo de grabación de la cámara es muy importante.

2.3.3.4. *Procedimiento de respaldos manual y deficiente*

El sistema de respaldos es fundamental en un sistema de video vigilancia, toda la información obtenida se debe almacenar en un lugar seguro en caso para tener acceso en caso de que se requiera ver la grabación.

En los sistemas analógicos de baja escalabilidad los respaldos se realizan mediante un dispositivo USB de manera manual.

Mediante el sistema de video vigilancia IP las grabaciones se almacenan automáticamente en el ordenador y mediante internet y una IP pública se pueden ver desde cualquier dispositivo con navegador web.

2.3.3.5. Sistema difícilmente escalable

El dispositivo DVR tradicional tiene una capacidad para controlar seis cámaras analógicas y si se requieren más cámaras se debe comprar completamente otro sistema.

Un solo software de video vigilancia IP tiene capacidad de integrar hasta 64 cámaras IP dependiendo de las características de la red, por lo tanto la escalabilidad presenta una de las ventajas más importantes sobre un sistema analógico.

2.3.3.6. Requerimientos de seguridad no son cubiertos por el sistema

Una cámara analógica no es más que un simple dispositivo que transmite video, el mismo que es capturado por un DVR. Una cámara IP incorpora funciones mejoradas como sensores de movimiento y utilizan internet para enviar avisos mediante correo electrónico.

2.3.4. VIDEO IP

El video IP o video vigilancia IP, al igual que muchos otros tipos de comunicaciones como son el correo electrónico, los servicios Web o la telefonía IP, se realiza a través de redes, ya sean cableadas o inalámbricas. Todo el flujo de audio/video se efectúa a través de la misma infraestructura de red común, lo cual conlleva multitud de ventajas sobre los sistemas CCTV tradicionales.

2.3.4.1. Aplicaciones de la Video vigilancia IP

El vídeo en red se puede utilizar en un número casi ilimitado de aplicaciones sin embargo, la mayoría de sus usos quedan dentro del ámbito de la vigilancia y seguridad o la supervisión remota de personas, lugares, propiedades y operaciones. Algunas posibilidades de aplicación habituales en sectores industriales clave son:

- Reconocimiento de matrículas.
- Monitorización de tráfico rodado.
- Monitorización de procesos industriales como Fundiciones o Cadenas de montaje.
- Vigilancia en condiciones de absoluta oscuridad, utilizando luz infrarroja.
- Vigilancia en vehículos de transporte público.
- Vigilancia del comportamiento de empleados.
- Vigilancia de los niños en el hogar, en la escuela, parques, guarderías
- Vigilancia de espacios públicos: aeropuertos, calles, estaciones, estadios.
- Vigilancia de espacios privados y negocios: hogares, comercios, hoteles, banca.
- Análisis facial para identificación de criminales en áreas públicas.
- Aplicaciones educativas.

2.3.4.2. *Arquitectura Básica de un sistema de video IP*

- Cámaras analógicas
- Cámaras de red IP
- Servidores de video (adaptan la señal de una cámara analógica a la red IP)
- Servidor de almacenamiento/gestión de video.
- Clientes de monitorización.
- Elementos de la red de datos (cableado, routers, switches, etc.)

Un sistema de video IP permite supervisar video y grabarlo desde cualquier lugar de la red, tanto si se trata por ejemplo de una red de área local (LAN) o de una red de área extensa (WAN) como internet. Esto permite una monitorización remota en tiempo real, centralizando las labores de monitorización, almacenamiento y gestión en una red de alarmas ubicada en un emplazamiento diferente al del espacio monitorizado. (García Mata, 2011, pág. 14)

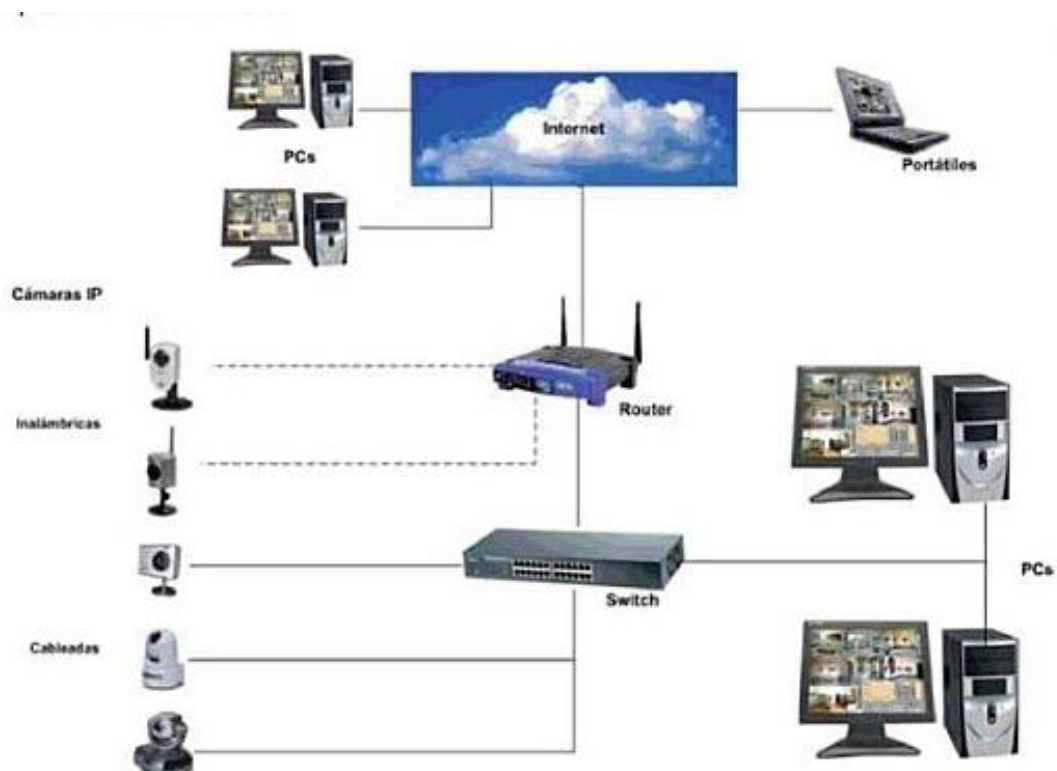


Fig. 21. Esquema básico de un sistema de video vigilancia IP.
Fuente: (Videovigilancia: CCTV usando vídeos IP, 2011, pág. 14)

2.3.4.3. Componentes de un sistema de cctv clásico

2.3.4.3.1. Cámara de red

Una cámara de red, también conocida como cámara de Internet, cámara IP o una cámara de vídeo de Internet, es un dispositivo que capta y transmite una señal de audio/vídeo digital través de una red IP estándar a otros dispositivos de red, tales como un PC o un teléfono 3G. Mediante el uso de una dirección IP dedicada, un servidor web y protocolos de streaming de vídeo, los usuarios pueden visualizar, almacenar y gestionar vídeo de forma local o remota, en tiempo real. Para ello podrán usarse tanto software cliente dedicado como navegadores web tales como Explorer, Firefox, Mozilla y Opera. (García Mata, 2011)

La versatilidad de las redes IP permite al usuario la visualización en directo de diferentes dispositivos de red. Además, los clientes pueden controlar y gestionar múltiples cámaras al mismo tiempo desde cualquier lugar donde haya una conexión de red. Por lo tanto, un sistema de vigilancia IP es más fácil, más cómodo y ofrece muchas más prestaciones en comparación con un sistema de CCTV clásico

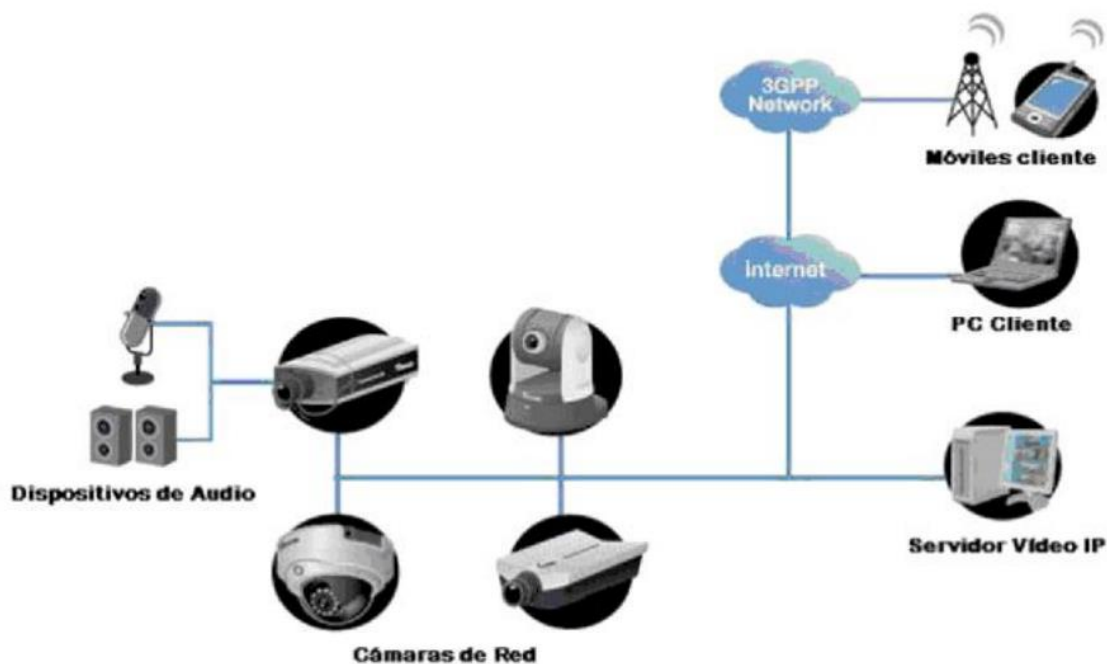


Fig. 22. Ubicación de las cámaras de red en un sistema de video vigilancia IP.

Fuente: (Videovigilancia: CCTV usando vídeos IP, 2011, pág. 18)

Una cámara de red se compone principalmente de una lente, un sensor de imágenes, un procesador de imagen, un chip de compresión de vídeo y un chip Ethernet que ofrece conectividad de red para la transmisión de datos

Cuando la luz pasa a través de la lente al sensor, se convierte en señales digitales que son luego procesadas Procesador Digital de Señal (DSP) integrado en la cámara. El flujo de vídeo es posteriormente comprimido para poder transmitirlo por la red IP a una velocidad de transmisión óptima. Por último, las imágenes de vídeo se envían a través de Internet a los dispositivos de back-end para permitir la visualización y almacenamiento de las mismas.

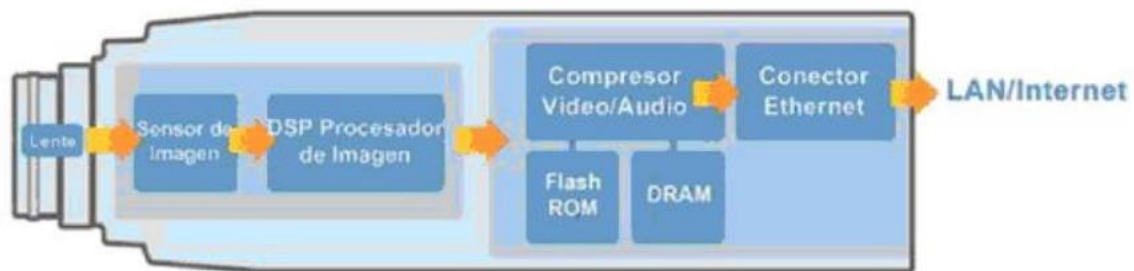


Fig. 23. Esquema básico de una cámara de red.

Fuente: (Videovigilancia: CCTV usando vídeos IP, 2011, pág. 19)

Las cámaras de red se pueden clasificar en función de si están diseñadas únicamente para su uso en interiores o para su uso en interiores-exteriores. Las cámaras de red para exteriores suelen tener un objetivo con iris automático para regular la cantidad de luz a la que se expone el sensor de imagen. Una cámara de exteriores también necesitará una carcasa de protección externa, salvo que su diseño ya incorpore un cerramiento de protección. Las carcasas también están disponibles para cámaras para interiores que requieren protección frente a entornos adversos como polvo y humedad y frente a riesgo de vandalismo o manipulación.

Las cámaras de red, diseñadas para su uso en interiores o exteriores, pueden clasificarse en cámaras de red fijas, domo fijas, PTZ (Pan-Tilt-Zoom) y domo PTZ.

2.3.4.3.1.1. Cámaras de red fijas

Una cámara de red fija, que puede entregarse con un objetivo fijo o varifocal, es una cámara que dispone de un campo de vista fijo (normal/telefoto/ gran angular) una vez montada. Este tipo de cámara es la mejor opción en aplicaciones en las que resulta útil que la cámara esté bien visible. Normalmente, las cámaras fijas permiten que se cambien sus objetivos. Pueden instalarse en carcasas diseñadas para su uso en instalaciones interiores o exteriores.



Fig. 24. Cámara de red fija.

Fuente: (Videovigilancia: CCTV usando vídeos IP, 2011, pág. 20)

2.3.4.3.1.2. Cámaras de red domo fijas

Una cámara domo fija, también conocida como mini domo, consta básicamente de una cámara fija preinstalada en una pequeña carcasa domo. La cámara puede enfocar el punto seleccionado en cualquier dirección. La ventaja principal radica en su discreto y disimulado diseño, así como en la dificultad de ver hacia qué dirección apunta la cámara. Asimismo, es resistente a las manipulaciones.

Las cámaras de domo fijas están diseñadas con diferentes tipos de cerramientos, a prueba de vandalismo y/o con clasificación de protección IP66 cuyo valor significa, IP índice de protección, el primer dígito 6 protección completa contra personas y entrada de polvo, el segundo dígito 6 protección contra fuertes chorros de agua de todas direcciones, incluido olas. Generalmente, las cámaras domo fijas se instalan en la pared o en el techo.



Fig. 25. Cámara de red de domo fija.
Fuente: (Videovigilancia: CCTV usando vídeos IP, 2011, pág. 21)

2.3.4.3.1.3. Cámara de red PTZ

Las cámaras PTZ (Pan-Tilt-Zoom) son cámaras que pueden moverse horizontalmente o verticalmente y disponen de un zoom ajustable dentro de un área, de forma tanto manual como automática. Son ideales para su uso en ubicaciones en áreas amplias y pueden ser usadas remotamente.

Las cámaras PTZ pueden incorporar las siguientes funciones:

Estabilización electrónica de imagen (EIS): en instalaciones exteriores, las cámaras domo PTZ con factores de zoom superiores a los 20X son sensibles a las vibraciones y al movimiento causados por el tráfico o el viento. La estabilización electrónica de la imagen (EIS) ayuda a reducir el efecto de la vibración en un video. Además de obtener videos más útiles, EIS reducirá el tamaño del archivo de la imagen comprimida, de modo que se ahorrará un valioso espacio de almacenamiento.

Máscara de privacidad: La máscara de privacidad permite bloquear o enmascarar determinadas áreas de la escena frente a visualización o grabación para que en esa área no grave y aparezca en el video solo una franja blanca.

Posiciones predefinidas: Muchas cámaras PTZ permiten programar posiciones predefinidas, normalmente entre 20 y 100 posiciones. Una vez las posiciones predefinidas se han configurado en la cámara, el operador puede cambiar de una posición a la otra de forma muy rápida.

E-flip: En caso de que una cámara PTZ se monte en el techo y se utilice para realizar el seguimiento de una persona, por ejemplo en unos grandes almacenes, se producirán situaciones en las que el individuo en cuestión pasará justo por

debajo de la cámara. Sin la funcionalidad E-flip, las imágenes de dicho seguimiento se verían del revés. En estos casos, E-flip gira las imágenes 180°.

Auto-flip: Generalmente, las cámaras PTZ, a diferencia de las cámaras domo PTZ, no disponen de un movimiento vertical completo de 360 grados debido a una parada mecánica que evita que las cámaras hagan un movimiento circular continuo. Sin embargo, gracias a la función Auto-flip, una cámara de red PTZ puede girar al instante 180 grados su cabezal y seguir realizando el movimiento horizontal más allá de su punto cero. De este modo, la cámara puede continuar siguiendo el objeto o la persona en cualquier dirección.

Auto seguimiento: función de video inteligente que detecta automáticamente el movimiento de una persona o vehículo y lo sigue dentro de la zona de cobertura de la cámara. Esta función resulta especialmente útil en situaciones de video vigilancia no controlada humanamente en las que la presencia ocasional de personas o vehículos requiere especial atención. La funcionalidad recorta notablemente el coste de un sistema de supervisión, puesto que se necesitan menos cámaras para cubrir una escena. Asimismo, aumenta la efectividad de la solución debido a que permite que las cámaras PTZ graben áreas de una escena en actividad.



Fig. 26. Cámara de red PTZ.
Fuente: (Videovigilancia: CCTV usando vídeos IP, 2011, pág. 22)

Podemos distinguir las cámaras PTZ entre cámaras mecánicas y no mecánicas.

Las cámaras de red PTZ mecánicas se utilizan principalmente en interiores y en aplicaciones donde se emplea un operador. El zoom óptico en cámaras PTZ varía normalmente entre 10X y 26x. Una cámara PTZ se puede instalar en el techo o en la pared.

Las cámaras de red PTZ no mecánicas, ofrecen capacidades de movimiento horizontal, vertical y zoom sin partes móviles, de forma que no existe desgaste de potencia por lo que no existen motores para que realicen el movimiento. Con un objetivo gran angular, ofrecen un campo de visión más completo que las cámaras de red PTZ mecánicas.

Una cámara de red PTZ no mecánica utiliza un sensor de imagen megapíxel y permite que el operador aleje o acerque, de forma instantánea, cualquier parte de la escena sin que se produzca ninguna pérdida en la resolución de la imagen. Esto se consigue presentando una imagen de visión general en resolución VGA (640x480 píxeles) aunque la cámara capture una imagen de resolución mucho más elevada. Cuando se da la orden a la cámara de acercar o alejar cualquier parte de la imagen de visión completa, el dispositivo utiliza la resolución megapíxel original para proporcionar una relación completa, en resolución VGA.

2.3.4.3.1.4. Cámara de red Domo PTZ

Las cámaras de red domo PTZ pueden cubrir una amplia área al permitir una mayor flexibilidad en las funciones de movimiento horizontal, vertical y zoom. Asimismo, permiten un movimiento horizontal continuo de 360 grados y un movimiento vertical de normalmente 180 grados.

Debido a su diseño, montaje y dificultad de identificación del ángulo de visión de la cámara (el cristal de las cubiertas de la cúpula puede ser transparente o ahumado), las cámaras de red domo PTZ resultan idóneas para su uso en instalaciones discretas.

Las cámaras de red domo PTZ también proporcionan solidez mecánica para operación continua en el modo ronda de vigilancia, en el que la cámara se mueve automáticamente de una posición predefinida a la siguiente de forma predeterminada o aleatoriamente. Normalmente, pueden configurarse y activarse hasta 20 rondas de vigilancia durante distintas horas del día. En el modo ronda de vigilancia, una cámara de red domo PTZ puede cubrir un área en el que se necesitarían 10 cámaras de red fijas ya que se pueden configurar para que vigilen en diferentes puntos es decir que no solo graba el entorno total sino también

puede grabar distintos puntos configurados. El principal inconveniente de este tipo de cámara es que sólo se puede supervisar una ubicación en un momento concreto, dejando así las otras nueve posiciones sin supervisar.

El zoom óptico de las cámaras domo PTZ se mueve, generalmente, entre valores de 10X y 35x. Las cámaras domo PTZ se utilizan con frecuencia en situaciones en las que se emplea un operador. En caso de que se utilice en interiores, este tipo de cámara se instala en el techo o en un poste o esquina para instalaciones exteriores.



Fig. 27. Cámara de red de domo PTZ.

Fuente: (Videovigilancia: CCTV usando vídeos IP, 2011, pág. 24)

Aunque las cámaras PTZ y domo PTZ comparten funciones similares, existen algunas diferencias entre ellas:

Las cámaras de red PTZ no disponen de un movimiento horizontal de 360° debido a la existencia de un tope mecánico. Esto significa que la cámara no puede seguir a una persona caminando de forma continua en un círculo completo alrededor del dispositivo.

Algunas cámaras de red PTZ no están diseñadas para la operación automática continua o las llamadas rondas de vigilancia, en las que la cámara se mueve automáticamente de una posición predefinida a la siguiente.

2.3.4.3.2. Servidor De Vídeo

Un servidor de vídeo es un dispositivo que permite la integración de un sistema de video vigilancia analógico CCTV existente en un sistema de vídeo en red IP. Básicamente, es una pasarela entre la tecnología coaxial de los sistemas analógicos, y la tecnología IP, que permite al software de gestión del sistema de

video vigilancia considerar las cámaras analógicas como cámaras IP. (García Mata, 2011, pág. 24)

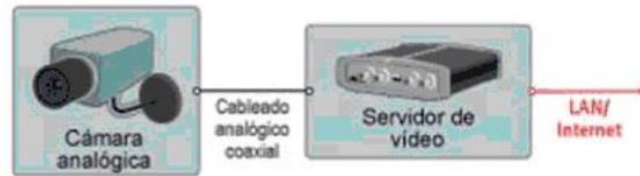


Fig. 28. Servidor de video.

Fuente: (Videovigilancia: CCTV usando vídeos IP, 2011)

Los servidores de vídeo desempeñan un papel significativo en aquellas instalaciones en las que se deben mantener muchas cámaras analógicas. Un servidor de vídeo permite migrar un sistema CCTV analógico a un sistema de vídeo en red. De este modo, los usuarios pueden beneficiarse de las ventajas del vídeo en red sin tener que descartar los equipos analógicos existentes, como cámaras analógicas CCTV y cableado coaxial. El servidor de vídeo se conecta a la cámara analógica a través de un cable coaxial y convierte las señales de vídeo analógicas en secuencias de vídeo digitales que luego se envían a través de una red basada en IP {p. ej., LAN, WLAN o Internet}. Para visualizar y/o grabar el vídeo digital se pueden utilizar monitores de ordenador y PC en lugar de DVR o VCR y monitores analógicos. El servidor de vídeo puede también transmitir y recibir audio, así como las señales de control que se envían a las cámaras (control de movimiento, zoom, gestión de eventos, alarmas, etc.).

Dependiendo de la configuración, el número de cámaras, el tipo de cámara y de si se encuentra o no instalado el cableado coaxial, podrán utilizarse distintos tipos de servidores de vídeo:

2.3.4.3.2.1. Servidores de vídeo montados en rack

La mayoría de las empresas usan una sala de control exclusiva en la que ubican el servidor y en la que controlan de forma eficiente las operaciones. Esto implica que todo el cableado coaxial instalado partirá de cada una de las cámaras hasta la sala de control. De esta manera, el servidor de vídeo se configura como un

equipo modular al cual se le van insertando tarjetas de interfaz de cable coaxial que permite que un gran número de servidores de vídeo funcionando en paralelo en un rack, todos administrados de forma centralizada.

2.3.4.3.2.2. Servidores de vídeo independientes

En un sistema de vigilancia donde se han realizado inversiones en cámaras analógicas pero aún no se ha instalado el cableado coaxial, resulta útil conectar un servidor de vídeo independiente anexa a cada cámara, de manera que las comunicaciones hacia el resto del sistema se harían a través de red IP. La ventaja de hacer esto, además del reducido coste de cableado para transmitir el vídeo, consiste en no disminuir la calidad de la imagen debido a la distancia, que es lo que ocurre con el cableado coaxial en el cual la calidad de la imagen se reduce en distancias mayores. Un servidor de vídeo produce imágenes digitales, por tanto la calidad no se ve reducida a causa de la distancia.

2.3.4.3.2.3. Servidores de vídeo con cámaras PTZ y domo

Las cámaras PTZ pueden conectarse a servidores de vídeo independientes así como a servidores de vídeo montados en rack, usando el puerto serie (RS232/422/485) integrado en los servidores de vídeo. En los casos en los que se utiliza un servidor de vídeo de un solo puerto con la cámara, se añade el beneficio de no tener que instalar cableado serie independiente para controlar el mecanismo PTZ. También ofrece la función de realizar un control PTZ a lo largo de grandes distancias a través de Internet. Deberá estar disponible un controlador específico en el servidor de vídeo para controlar una cámara PTZ determinada.

2.3.4.3.3. Software de gestión de vídeo

En términos simplificados, un software de gestión de vídeo es un software diseñado para atender a la visualización, gestión y grabación de un gran número de cámaras. Los sistemas de vídeo vigilancia de hoy pueden llegar a tener a menudo cientos o miles de cámaras de seguridad. Con tales magnitudes sería imposible asignar un monitor a cada cámara o asignar un circuito dedicado a cada una. (García Mata, 2011, pág. 26)

Sin embargo, usando la tecnología IP podemos conectar todas las cámaras a una misma red, y usando ese software instalado en un servidor dedicado, podemos hacer una selección de las cámaras que queremos monitorizar en cada momento, y podemos implementar todas las prestaciones o aplicaciones que creamos útiles en nuestro sistema de video vigilancia. Ejemplo:

- Visualización simultánea y grabación de vídeo en directo desde múltiples cámaras.
- Diversos modos de grabación: continua, programada, por alarma y por detección de movimiento.
- Capacidad para manejar altas velocidades de imagen y gran cantidad de datos.
- Múltiples funciones de búsqueda para eventos grabados.
- Acceso remoto a través de un navegador web, software cliente e incluso cliente PDA. o Control de cámaras PTZ y domos.
- Funciones de gestión de alarmas (notificación de alarma, ventanas desplegadas o correo electrónico).
- Soporte de sistema de audio en tiempo real, full dúplex. De esta manera, tendríamos un sistema completamente automatizado, con una disponibilidad 24/7, con capacidad de memoria ilimitada y con acceso global.



Fig. 29. Aplicación de gestión de vídeo.

Fuente: (Videovigilancia: CCTV usando vídeos IP, 2011, pág. 27)

2.3.4.3.3.1. Criterios para la selección de un sistema de gestión de vídeo

En primer lugar, los requisitos que debe cumplir el sistema de gestión de vídeo deben ser verificados en la fase de planificación. Idealmente, el software incluido con la grabadora digital debe satisfacer los criterios de aplicación necesarios. Algunos programas de software contienen herramientas de control y gestión íntegra de un sistema de video vigilancia IP.

Otra opción sería utilizar una grabación y una plataforma de análisis de imagen que cuente con funciones avanzadas de gestión.

Si el objeto del sistema es tener un gran número de cámaras de vigilancia y es previsible su expansión futura, las soluciones óptimas se basarán en arquitecturas de cliente/servidor.

2.3.4.3.3.1.1. Uso de arquitecturas software abiertas

Las soluciones cliente/servidor son ideales para su uso en arquitecturas de red basadas en la arquitectura TCP/IP, independientemente de si trabajamos en entornos LAN o WAN. Las aplicaciones software del sistema definen todas las funciones requeridas para la video vigilancia (vigilancia en directo, grabación, control de alarmas y análisis de imagen). Una vez están especificadas todas las funciones, el sistema de gestión tomaría el control del centro de control de vídeo y funcionaría automáticamente. Este sistema de gestión podría incluir interfaces

que facilitarían la integración con otros sistemas de seguridad u otras aplicaciones.

Adicionalmente, los usuarios debe ser capaces de acceder a las imágenes generadas por el sistema de video vigilancia IP desde cualquier ubicación utilizando simplemente un navegador. Para poder hacer esto habrá que tener en cuenta aspectos de seguridad (encriptar bien los datos, trabajar en una red privada virtual).

2.3.4.3.3.1.2. Uso de arquitecturas cliente/servidor

La arquitectura cliente/servidor y la estructura modular de los sistemas de gestión de vídeo deben permitir su adaptación flexible a los diferentes escenarios de aplicación. Las plataformas deben permitir la expansión del sistema en función de la demanda de fuentes de vídeo adicionales y por lo tanto deben permitir la máxima flexibilidad, con un diseño de sistemas orientado a la aplicación estructurada sobre un número de entradas de vídeo activas. Esto es así porque las cámaras analógicas de seguridad también se pueden conectar, además de los componentes básicos de un sistema de video vigilancia IP.

Los sistemas deben poderse ampliar con módulos de software partiendo de la base del uso de un sistema modular. Los sistemas deben poder instalarse en servidores Windows o Linux, al igual que los clientes, comunicándose todos mediante TCP/ IP.

Las soluciones de vigilancia basadas en plataforma Linux ofrecen las ventajas de que el sistema operativo es gratuito y de que la estabilidad del sistema está asegurada. Las plataformas Windows mencionadas pueden también ser utilizadas por el cliente, y también los sistemas operativos como Mac OS en función de qué programas se ejecutan. Algunos programas de software de gestión de vídeo también permiten que se utilicen independientemente del sistema operativo que se esté utilizando. Los clientes, por el contrario, pueden utilizar todos los sistemas operativos que soporten Java. Los requisitos de hardware dependen de la aplicación requerida con la regla general: cuanto más, mejor.

2.3.4.3.3.1.3. Integración con proveedores externos y uso de interfaces estándar

El uso de interfaces estandarizados y la capacidad de integración con otros proveedores son características que identificarían a una plataforma de gestión de Video vigilancia IP de calidad. Así se permitiría la integración de todos los módulos del sistema de gestión, como sistemas de puntos de venta, de reconocimiento de matrícula, de contabilización de personas, alarma de incendio, etc. Si bien las alarmas de incendio o los sistemas de detección de intrusos pueden conectar a través de interfaces OPC o de las API' s de la aplicación, algunos sistemas incluso dar acceso a la funcionalidad completa en un interfaz HTTP/LME. Esto permite el intercambio de datos de imágenes en vivo y archivados y eventos, así como 105 datos y la integración con aplicaciones externas de control y sistemas (centro de control, acceso, alarmas, sistemas de punto de venta, etc.).

La selección del software de vídeo ideal para nuestro propósito no es fácil y depende de la arquitectura de red y de otros factores adicionales. Los criterios más importantes de cara a tomar dicha decisión son por un lado la flexibilidad en un entorno de arquitectura abierta del sistema y por otro una modularidad que permita al sistema expandirse y adaptarse a nuevas condiciones. Igualmente importante son las "características inteligentes" tales como detección de movimiento para la grabación de movimiento y la activación automática de alarmas. Adicionalmente, funciones como el almacenamiento de imágenes y análisis de vídeo son de vital importancia.

2.3.4.4. Ventajas de la video vigilancia IP respecto a los sistemas analógicos

Un sistema de video vigilancia IP ofrece toda una serie de ventajas y funcionalidades avanzadas que no puede proporcionar un sistema de video vigilancia analógico.

Entre las ventajas se incluyen la accesibilidad remota, la alta calidad de imagen, la gestión de eventos y las capacidades de video inteligente, así como las posibilidades de una integración sencilla y una escalabilidad, flexibilidad y rentabilidad mejoradas.

2.3.4.4.1. Accesibilidad remota

Se pueden configurar las cámaras de red y los servidores de video para acceder a ellos de forma remota, lo que permite a diferentes usuarios autorizados visualizar video en vivo y grabado en cualquier momento y desde prácticamente cualquier ubicación de red del mundo. Esto resulta ventajoso si los usuarios quisieran que otra empresa, por ejemplo una de seguridad, tuviera también acceso al video. En un sistema CCTV analógico tradicional, los usuarios necesitarían encontrarse en su centro de control para ver y gestionar el video, y el acceso al video fuera del centro no sería posible sin un equipo como un servidor de video o un grabador de video digital (DVR) de red. Un DVR es el sustituto digital de la grabadora de cintas de video.

2.3.4.4.2. Calidad de imagen

En una aplicación de video vigilancia IP, es indispensable contar con una alta calidad de imagen para poder capturar con claridad un incidente en curso e identificar a las personas u objetos implicados. Con las tecnologías de barrido progresivo y megapíxel, una cámara de red puede producir una mejor calidad de imagen y una resolución más alta que con una cámara CCTV analógica. De igual manera, la calidad de imagen se puede mantener más fácilmente en un sistema de video en red que en uno de vigilancia analógica. Con los sistemas de video analógicos que utilizan un DVR como medio de grabación, se realizan muchas conversiones analógicas a digitales y después otra vez a analógicas para su transporte; después las señales analógicas se digitalizan para su grabación. Las imágenes capturadas se degradan con cada conversión entre los formatos analógico y digital, así como con la distancia de los cables. Cuanto más lejos tienen que viajar las señales de video, tanto más débiles se vuelven. En un sistema de vigilancia IP digital completo, las imágenes de una cámara de red 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. Además, las imágenes digitales se pueden almacenar y recuperar más fácilmente que en los casos en los que se utiliza video analógico.

2.3.4.4.3. Gestión de eventos y video inteligente

Es muy común la existencia de demasiado material de vídeo grabado y una falta de tiempo suficiente para analizarlo adecuadamente. Las cámaras de red y los servidores de vídeo avanzados con inteligencia o análisis integrado pueden ocuparse de este problema al reducir la cantidad de grabaciones sin interés y permitir respuestas programadas. Este tipo de funcionalidad no está disponible en un sistema analógico. Por otro lado, el usar la tecnología IP posibilita la utilización de software inteligente que puede facilitar el uso de incluyen funciones integradas como la detección de movimiento por vídeo, alarma de detección de audio, alarma anti manipulación activa, conexiones de entrada y salida (E/S) y funcionalidades de gestión de alarmas y eventos.

Las funcionalidades de gestión de eventos se pueden configurar mediante la interfaz de usuario del producto de vídeo en red o a través de un programa de software de gestión de vídeo. Los usuarios pueden definir las alarmas o eventos configurando el tipo de activadores que se utilizarán así como en qué momento. Asimismo, se pueden configurar las respuestas (por ejemplo, la grabación en uno o varios sitios, tanto si es local como si es fuera del centro por motivos de seguridad; la activación de dispositivos externos como alarmas, luces y puertas; y el envío de mensajes a los usuarios).

2.3.4.4.4. Estandarización

Los productos de vídeo 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, además del software de gestión de vídeo y de la aplicación. Por ejemplo, el vídeo de una cámara de red se puede integrar en un sistema de punto de venta o en un sistema de gestión de edificios.

2.3.4.4.5. Escalabilidad y flexibilidad

Un sistema de vídeo en red puede crecer a la vez que las necesidades del usuario. Los sistemas basados en IP ofrecen a muchas cámaras de red y servidores de vídeo, así como a otros tipos de aplicaciones, una manera de compartir la misma red inalámbrica o con cable para la comunicación de datos;

de este modo, se puede añadir al sistema cualquier cantidad de productos de vídeo en red sin que ello suponga cambios significativos o costosos para la infraestructura de red. Esto no sucede con un sistema analógico. En un sistema de vídeo analógico, se debe extender un cable coaxial directamente desde cada cámara a un puesto de visualización o grabación. Asimismo, se deben usar cables de audio independientes si se requiere audio. Los productos de vídeo en red también se pueden implementar y utilizar en red desde prácticamente cualquier lugar, y el sistema puede ser tan abierto o cerrado como se necesite.

2.3.4.4.6. Rol (Rentabilidad de la inversión)

Un sistema de vigilancia IP tiene normalmente un coste total inferior al de un sistema CCTV analógico tradicional. La infraestructura de red a menudo ya está implementada y se utiliza para otras aplicaciones dentro de una organización, por lo que una aplicación de vídeo en red puede aprovechar la infraestructura existente. Las redes basadas en IP y las opciones inalámbricas constituyen además alternativas mucho menos caras que el cableado coaxial y de fibra tradicionales utilizados por un sistema CCTV analógico.

Por otro lado, las transmisiones de vídeo digitales se pueden encaminar por todo el mundo mediante una gran variedad de infraestructuras interoperativas. Los costes de gestión y equipos también son menores ya que las aplicaciones back-end y el almacenamiento se ejecutan en servidores basados en sistemas abiertos, de estándar industrial, no en hardware propietario como un DVR en el caso de un sistema CCTV analógico.

Además, la tecnología PoE (Alimentación a través de Ethernet), que no se puede aplicar a un sistema de vídeo analógico, se puede utilizar en un sistema de vídeo en red. PoE permite a los dispositivos en red recibir alimentación de un conmutador compatible con PoE a través del mismo cable Ethernet que transporta los datos (vídeo). Ofrece un ahorro sustancial en los costes de instalación y puede aumentar la fiabilidad del sistema. (García Mata, 2011)

CAPITULO III

3. ANÁLISIS DE LA SITUACIÓN ACTUAL

En este capítulo se describen las zonas con mayores requerimientos de vigilancia, además se presenta el estudio y comparación de equipos en el mercado, finalmente se describe la solución más adecuada para el sistema.

3.1. ANTECEDENTES

El Centro de Desarrollo Infantil “Angelitos Juguetones” no cuenta con monitoreo de las actividades realizadas en las instalaciones; así como el registro de eventos conflictivos en las zonas con mayores de requerimientos de vigilancia. No existe un registro del comportamiento e interacción entre docentes, niños y padres de familia que concurren diariamente al centro.

3.2. PLANO DEL ÁREA A CONTROLAR

La implementación de cámaras de vigilancia IP para el Centro de Desarrollo Infantil “Angelitos Juguetones” será en las zonas con mayores requerimientos de supervisión identificadas previamente por las autoridades del plantel, de tal forma que se mejore la seguridad de la institución, el control y prevención de riesgos de accidentes en los estudiantes y personal docente, así como el aseguramiento del uso adecuado de los recursos de la institución como son el área de juegos y el patio.

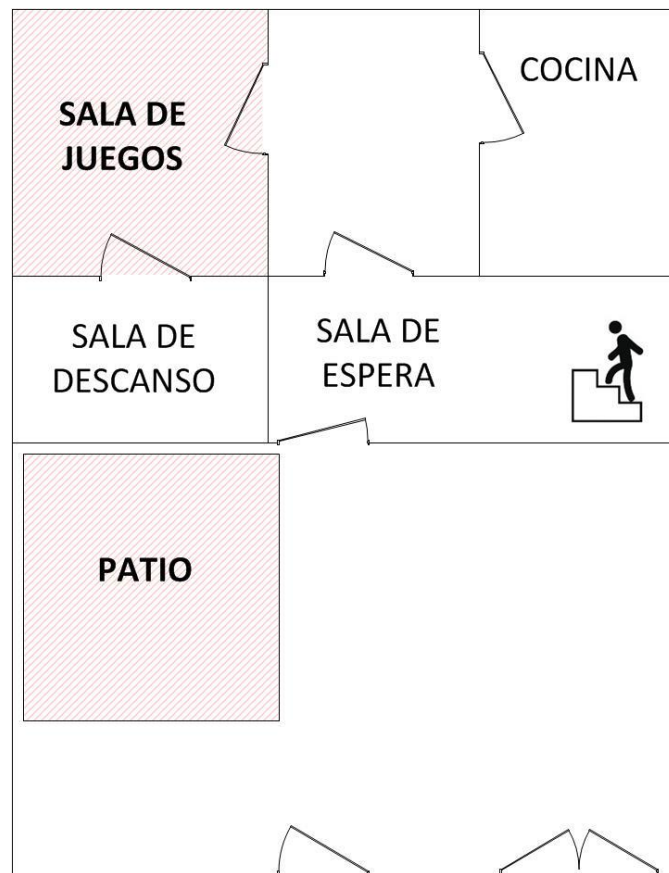


Fig. 30. Plano del área a controlar

3.2.1. Descripción de las áreas a controlar

3.2.1.1. ZONA A

Esta zona comprende una parte del patio de la institución y el acceso vehicular y peatonal principal en la avenida 12 de octubre, dicha zona posee elevados requerimientos de vigilancia debido a la concentración de alumnos y padres de familia en las horas de entrada/salida. Se establece como objetivo el control del comportamiento de los niños, así como de las personas y vehículos que utilicen este acceso a la institución. Se implementará una cámara IP exterior para esta zona.

3.2.1.2. ZONA B

Esta zona comprende el área de juegos de la institución. Se establece como objetivo el control de la interacción entre los docentes y los niños. Se implementara una cámara IP interior en esta zona.

3.3. ESTUDIO DE EQUIPOS DE VIDEO VIGILANCIA

3.3.1. CÁMARAS IP INTERIORES

3.3.1.1. Cámara IP FOSCAM FI9826W



Fig. 31. Cámara IP FOSCAM FI9826w

Fuente: (Foscam Intelligent Technology, <http://www.foscam.es/FI9826W/>)

3.3.1.1.1. Descripción

Posee amplia capacidad de movimiento vertical y horizontal. Equipada con visión nocturna en completa oscuridad, gracias a sus led infrarrojos, muy potente y con prestaciones casi profesionales para el usuario doméstico, de pequeño comercio u oficina, muy sencilla de instalar y con grandes posibilidades, debido a su sistema de grabación interna, en tarjeta microSD (hasta 32Gb), que le permitirá funcionar de forma totalmente autónoma. Software incorporado, por lo que se puede ver lo que está ocurriendo vía remota, con un ordenador o desde cualquier dispositivo móvil, Dispone de software gratuito, que permite desde un ordenador planificar las grabaciones y alarmas, así como elegir los eventos a realizar en caso de alarma. Puede integrarse fácilmente con otros modelos FOSCAM.

3.3.1.1.2. Características Principales

- Cámara de 1.3 megapíxeles, con un tamaño máximo de imagen de 1280x960 píxeles.
- ZOOM óptico de 3X.
- Compresión H264.

- Incorpora detección de movimiento.

3.3.1.1.3. Especificaciones Técnicas

Especificaciones Técnicas - Cámara FOSCAM FI9826w	
Sensor de imagen	Sensor: High Definition Color CMOS Sensor
	Resolución: 960P (1280 x 960 Pixels 1.3 Megapíxel), VGA, QVGA
	Iluminación: 0 Lux mínimo (con iluminación infrarroja incorporada)
	Controles: Control de brillo, contraste y frecuencia de luz. Automáticos y manuales
Lentes	<p>Cristal: Lentes IR-infrarrojas de visión nocturna; rosca estándar S-Mount para intercambio de objetivos.</p> <p>f: 4-9 mm, 35-70° ángulo de visión (zoom óptico 2.25X = estándar comercial 3X)</p>

Especificaciones Técnicas - Cámara FOSCAM FI9826w	
Audio	Entrada: Micrófono incorporado
	Salida: Altavoz incorporado
	Conexión externa: Conexión jack 3.5 mm para opción de micro y altavoz externo
	Compresión audio: PCM/G.726
Vídeo	Compresión vídeo: H.264
	Stream: Triple stream
	Imágenes/seg: 30 fps máx. (ajustable a valores inferiores)
	Resolución: 960P (1280 x 960 Pixels 1.3 Megapíxel), VGA, QVGA
	Volteo imagen: Vertical / Horizontal
	Frecuencia luz: 50Hz, 60Hz o Exterior
	Modo infrarrojo: Automático y Manual
	Ajustes vídeo: Brillo, Contraste, Saturación, Agudeza

Especificaciones Técnicas - Cámara FOSCAM FI9826w	
Comunicación	Red Ethernet: 10/100 Mbps RJ-45
	Protocolos: HTTP, FTP, TCP/IP, UDP, SMTP, DHCP, PPPoE, DDNS, UPnP, GPRS
	Wi-Fi: IEEE 802.11 b/g/n
	Velocidad datos: 802.11b: 11Mbps (Max.), 802.11g: 54Mbps (Max.), 802.11n: 150 Mbps (Max.)
	WPS: Soporte de WPS (conexión Wi-Fi con pulsar un botón)
	Seguridad Wi-Fi: Encriptación WEP, WPA, WPA2
Sistemas compatibles	Sistema operativo: Windows 2000/XP, Vista, 7, 8; MacOS, iOS, Android
	Navegador: IE, Firefox, Chrome, Safari
Datos físicos	<p>Movimiento horizontal: 300°.</p> <p>Movimiento vertical: 120°.</p>
Datos físicos	Luz infrarroja: 8 IR LEDs, Alcance nocturno hasta 8 m
	Dimensiones(mm): 115,8 (La) x 103,2 (An) x 118,6 (Al)
	Peso: 720 gr (accesorios incluidos). Cámara sola con antena: 350 gr

Especificaciones Técnicas - Cámara FOSCAM FI9826w	
Datos físicos	Luz infrarroja: 8 IR LEDs, Alcance nocturno hasta 8 m
	Dimensiones(mm): 115,8 (La) x 103,2 (An) x 118,6 (Al)
	Peso: 720 gr (accesorios incluidos). Cámara sola con antena: 350 gr
Alimentación	Alimentación: Adaptador DC 5V/2.0A (incluido). El cable mide 1,5 m.
	Consumo: 9 W máximo
Entorno	Temperatura: 0° ~ 40°C (operativa) / -10°C ~ 60°(almacenamiento)
	Humedad: 20% ~ 85% sin condensación (operativa) / 0% ~ 90% sin condensación (almacenamiento)

Tabla 1. Especificaciones Técnicas – Cámara FOSCAM FI9826W

3.3.1.2. Cámara IP Apexis APM-HP803-MPC-WS



Fig. 32. Cámara IP Apexis APM-HP803-MPC-WS
Fuente: (APEXIS, <http://www.apexis.es/productos/interior/apm-hp803-mpc-ws>)

3.3.1.2.1. Descripción

Cámara IP Wi-Fi H.264 de alta resolución con movimiento remoto, altavoz y micrófono integrados, salida-entrada de alarma I/O, salida y entrada de audio, infrarrojos, LED de estado, lector de tarjetas SD y conexión punto a punto P2P.

3.3.1.2.2. Características Principales

- Incluye función "IR CUT", para brindar alta nitidez.
- Envío de imágenes vía correo electrónico cuando se active la función de "Detección de Movimiento".
- Configuración de acceso hasta de 8 usuarios con diferentes privilegios.
- Monitoreo desde una página en Internet en donde se puede mover la cámara vía remota en cualquier dirección.

3.3.1.2.3. *Especificaciones Técnicas*

Especificaciones Técnicas - Cámara IP Apexis APM-HP803-MPC-WS	
Sensor de imagen	Sensor: CMOS Color de 1/4"
	Resolución: (1280x720 Pixels 1.0 Megapíxel)
	Iluminación: 0 Lux mínimo
	Controles: modificaciones del brillo, contraste, color y nitidez.
Lentes	Cristal: 3.6 mm, alcance de leds infrarrojos 16/10 m.
	Angulo de visión: 59° Horizontal / 32° Vertical.
Audio	Modos de audio: dúplex completo.
	Micrófono: mini jack 3.5 mm
	Altavoz: mini jack 3.5 mm
Video	Compresión de video: H.264
	Imágenes por segundo: 30 fps (1280x720)
	Inversión de imagen: Vertical/Horizontal
	Frecuencia de Luz: 50 Hz, 60Hz, exteriores

Especificaciones Técnicas - Cámara IP Apexis APM-HP803-MPC-WS	
Comunicación	Interfaz de sistema: Ethernet 10 Base-T/100 Base-TX. Conexión P2P.
	Frecuencia de bits: VBR / CBR 128Kbps~4Mbps
	Protocolos soportados: TCP/IP, DHCP, SMTP, HTTP, DDNS, UPnP, PPPoE, FTP, DNS, UDP, GPRS, ARP/RARP, NFS, RTP, RTCP, SSL, TFTP, NTP.
	LAN Inalámbrica: Wi-Fi b/g/n, IEEE 802.11 b/g/n
	Encriptación: WPA/WPA2: TKIP/AES
Sistemas compatibles	Sistema operativo: Microsoft Windows 98/ME/2000/XP, Vista, 7, 8.
	Navegador: IE, Firefox, Chrome, Safari
Datos físicos	Movimiento horizontal: 300°.
	Movimiento vertical: 120°.
	Dimensiones (mm): 130 Al, 96 An, 130 Fo.
	Peso: 360 g.
Alimentación	Alimentación: Transformador de corriente externo 5V DC/2 ^a .

	Consumo: 7w (máximo)
Especificaciones Técnicas - Cámara IP Apexis APM-HP803-MPC-WS	
Entorno	Temperatura: ~30°C ~ 55°C
	Humedad: 20% - 85% sin condensación

Tabla 2. Especificaciones Técnicas - Cámara IP Apexis APM-HP803-MPC-WS

3.3.1.3. Cámara IP D-Link DCS-930L



Fig. 33. Cámara IP D-Link DCS-930L
Fuente: (Dlink Corporation, <http://www.dlinkla.com.ec/dcs-930l>)

3.3.1.3.1. Descripción

La cámara DCS-930L constituye una solución única y versátil para el hogar o pequeña oficina. A diferencia de las cámaras web estándar, la DCS-930L es un sistema completo que incorpora una CPU y un servidor web capaz de transmitir imágenes de vídeo de alta calidad.

Se puede acceder a la cámara DCS-930L de forma remota y controlarla desde cualquier PC o equipo portátil de la red local, o bien por Internet a través de un explorador web. La sencillez del proceso de instalación y el carácter intuitivo de la interfaz basada en web aseguran una fácil integración con la red Ethernet/Fast Ethernet existente o la red inalámbrica 802.11n/g. La cámara DCS-930L también incluye funciones de monitorización remota y de detección de movimiento, que la convierten en una solución de seguridad doméstica completa y rentable.

3.3.1.3.2. Características Principales

- Utilidad de monitorización remota.
- Compatibilidad con varias plataformas.
- Preparado para mydlink: monitorización fácil de su hogar, desde cualquier lugar.
- Incluye detección de movimiento y alertas por correo electrónico a través de la interfaz de usuario.

3.3.1.3.3. Especificaciones Técnicas

Especificaciones Técnicas - Cámara D-Link DCS-930L	
Sensor de imagen	Sensor: CMOS VGA 1/5 pulgadas.
	Resolución: 160 x 120 con hasta 30 fps.
	Iluminación: 1 lux @ F2.8.
	Controles: tamaño y calidad de la imagen ajustables.
Lentes	Distancia focal: 5,01 mm, F2.8
	Zoom Digital: hasta 4x
	Angulo de visión: horizontal: 45,3° Vertical: 34,5° Diagonal: 54,9°

Especificaciones Técnicas - Cámara D-Link DCS-930L	
Audio	Micrófono integrado
Video	Compresión de video: MJPEG. JPEG para imágenes fijas.
Comunicación	Protocolos de conexión en red: IPV4, ARP, TCP, UDP, ICMP, Cliente DHCP, Cliente NTP (D-Link), Cliente DNS, Cliente DDNS (Dyndns y D-Link), Cliente SMTP, Cliente FTP, Servidor HTTP, PPPoE, Direccionamiento de puerto UPnP.
	Interfaz de red integrada: Fast Ethernet 10/100BASE-TX/ WLAN 802.11
	Conectividad inalámbrica: 802.11b/g/n con seguridad WEP
Sistemas compatibles	Sistema operativo: Microsoft Windows XP, Vista, Windows 7.
	Navegador: IE 6 o superior, Firefox 3.5 o superior, Safari 4.
Datos físicos	Movimiento: Sin movimiento
	Dimensiones (mm): 27,2 x 60 x 96 mm.
	Peso: 76,9 g (sin la base ni el soporte).

Especificaciones Técnicas - Cámara D-Link DCS-930L	
Alimentación	Alimentación: a: 100-240 V CA, 50/60 Hz.
	Consumo: 2 W.
Entorno	Temperatura: 0 °C a 40 °C
	Humedad: 20-80% RH, sin condensación.

Tabla 3. Especificaciones Técnicas - Cámara D-Link DCS-930L

3.3.1.4. Comparación de Cámaras IP Interiores

Categoría	Especificación	D-Link DCS-930L	FOSCAM FI9826w	Apexis APM-HP803
Sensor de imagen	Sensor	CMOS VGA 1/5 pulgadas.	Color. CMOS Sensor	1/4" Color CMOS Sensor
	Resolución	640 x 480	1280 x 960	1280 x 720
	Iluminación	1 lux @ F2.8.	0 Lux mínimo	0 Lux mínimo
	Controles	Tamaño y calidad de la imagen ajustables.	Automáticos y manuales	Automáticos y manuales
Lentes	Lente	5,01 mm, F2.8	3.6mm	4-9 mm
Audio	Entrada	Micrófono incorporado	Micrófono incorporado	Micrófono incorporado
	Salida	No especificado	Altavoz incorporado	Altavoz incorporado
	Compresión audio	No especificado	PCM/G.726	ADPCM

Categoría	Especificación	D-Link DCS-930L	FOSCAM FI9826w	Apexis APM-HP803
Vídeo	Compresión vídeo	MJPEG	H.264	H.264, MJPEG
	Imágenes/seg.	30 fps máx.	30 fps máx.	30 fps máx.
	Resolución	1280 x 960	640x480	1280*720
	Volteo imagen	Vertical/ Horizontal	Vertical/ Horizontal	Vertical/ Horizontal
	Frecuencia luz	No especificado	50Hz, 60Hz, Outdoor	50Hz, 60Hz, Outdoor
	Ajustes vídeo	brillo, contraste	brillo, contraste, saturación, agudeza	brillo, Contraste, Saturación, Agudeza
Comunicación	Red Ethernet	10/100 Mbps RJ-45	10/100 Mbps RJ-45	10/100 Mbps RJ-45
	Wi-Fi	IEEE 802.11b/g/n	IEEE 802.11b/g/n	IEEE 802.11b/g/n

Categoría	Especificación	D-Link DCS-930L	FOSCAM FI9826w	Apexis APM-HP803
Comunicación	Seguridad Wi-Fi	Encriptación WEP, WPA, WPA2	Encriptación WEP, WPA, WPA2	Encriptación WEP, WPA, WPA2
Sistemas compatibles	Sistema operativo	Windows 2000/XP, Vista, 7, 8; MacOS, iOS, Android	Windows 2000/XP, Vista, 7, 8; MacOS, iOS, Android	Windows 2000/XP, Vista, 7, 8; MacOS, iOS, Android
	Navegador	IE, Firefox, Chrome, Safari	IE, Firefox, Chrome, Safari	IE, Firefox, Chrome, Safari
Datos físicos	Movimiento	Sin movimiento	h: 300° v: 120°	h:320° v: 120°
	Luz infrarroja	No especificado	8 IR LEDs Alcance nocturno hasta 8 m	16 IR Alcance Nocturno de 12- 18 metros
	Dimensiones (mm: la, an, al)	27.2x60x96	116x104 x119	105x98x130
	Peso (g)	76.9	350	360

Categoría	Especificación	D-Link DCS-930L	FOSCAM FI9826w	Apexis APM-HP803
Alimentación	Alimentación	5V	5V	5V
	Consumo	2W	9 W	7W
Entorno	Temperatura (operativa)	0° a 40° C	0° ~ 40°C	-30°C ~ 55°C
	Humedad (operativa/sin condensación)	20 a 80%	20% ~ 85%	20% ~ 85%
Precio		130+I.V.A	140+I.V.A	145+I.V.A

Tabla 4. Comparación de Cámaras IP Interiores

3.3.1.5. Conclusión del Estudio de Cámaras IP Interiores

Al finalizar el estudio y comparación de características técnicas, se observa que la cámara IP Apexis APM-HP803 presenta similares características que las cámaras D-Link DCS-930L y FOSCAM FI9826w. Sin embargo; la principal especificación por la que se eligió esta cámara es que presenta mejor resolución en ambientes baja intensidad de luz; así como su amplia capacidad de movimiento.

3.3.2. CÁMARAS IP EXTERIORES

3.3.2.1. Cámara EasyN F-M1BF



Fig. 34. Cámara EasyN F-M1BF

Fuente: (EasyN, <http://www.easyn.com.es/ProductsShow.aspx?id=497#.U-5uhf15OSp>)

3.3.2.1.1. Descripción

Es un dispositivo de vigilancia y seguridad de uso amplio, que combina la tecnología inalámbrica Wi-Fi y cámara CCTV en uno solo. Motorizado para girarse horizontal y verticalmente.

Posee un estándar de compresión MJPEG. El sensor CMOS presenta un balance automático de blancos y de la luz de fondo. Compatible con navegador Internet Explorer, navegadores móviles y la gestión a través de la interfaz de monitor centralizado.

En general, la cámara IP EasyN F-M1BF tiene funciones como simplex y dúplex de audio, puerto de infrarrojos, cable, inalámbrico, POE, PZT, almacenamiento local.

3.3.2.1.2. Características Principales

- Acceso monitoreo desde cualquier ordenador y la mayoría de los smartphones en el mercado (tales como Android, iPhone).
- Ofrecer software especial para iPhone o móvil Android.
- Sistema de DDNS incorporado gratis, como <http://demo.easyn.hk>.
- Software de gestión de multi-ventanas de EasyN, grabación remota.
- Admite cuenta de tres niveles de jerarquía, contraseña, gestión de autoridad de multi-niveles para usuarios.

3.3.2.1.3. Especificaciones Técnicas

Especificaciones Técnicas - Cámara EasyN F-M1BF	
Sensor de imagen	Sensor: 3.6mm SBC lente. CMOS
	Resolución: VGA(640*480),QVGA(320*240) ,QQVGA(160*120)
	Iluminación: 0.3LUX/F1.2
	Controles: Corte de infrarrojos incorporado, con interruptor automático, sin dominante de color.
Lentes	Zoom Digital: 3x óptico
	Angulo de visión: Horizontal:355°, vertical: 90°

Especificaciones Técnicas - Cámara EasyN F-M1BF	
Audio	Formato de compresión: G.711/G.726
	Entrada: micrófono incorporado
Video	Compresión de video: Motion-JPEG
	Fotogramas por segundo: 25fps
Comunicación	Protocolos: HTTP, UDP, SMTP, FTP, DHCP, DNS, DDNS, NTP, UPNP
	Interfaz de red integrada: RJ-45 10/100Mb auto-adaptable Ethernet
	Conectividad inalámbrica: Wifi802.11 b/g/n
Sistemas compatibles	Sistema operativo: Microsoft Win98 SE/ME/2000/XP, Vista, Win7.
	Navegador: Internet Explorer 8.0 o superior.
Datos físicos	Movimiento: rotación horizontal: 355°, rotación vertical: 90°.
	Dimensiones (mm): 200 x 160 x 180mm (L*W*H)
	Peso: 1370 g.

Especificaciones Técnicas - Cámara EasyN F-M1BF	
Alimentación	Alimentación: 12V 1A
	Consumo: No especificado.
Entorno	Temperatura: -10~50°C
	Humedad: 10%~90%RH.

Tabla 5. Especificaciones Técnicas - Cámara EasyN F-M1BF

3.3.2.2. Cámara IP FOSCAM FI9804W



Fig. 35. Cámara IP FOSCAM FI9804W
Fuente: (FOSCAM, <http://www.foscam.es/FI9804W/>)

3.3.2.2.1. Descripción

Cámara IP perfecta para su casa o negocio, puede colocarse, por sus reducidas dimensiones, tanto en el interior como en el exterior, además, cuenta con una perfecta visión nocturna de hasta 30 metros, con una calidad mejorada debido a su filtro, que posibilita mayor nitidez y menos destellos blancos en la visión. Esta cámara además es muy estética, y pasa fácilmente desapercibida. Este modelo es anti vandálico, por lo que se puede colocar con total seguridad de que no se romperá fácilmente.

3.3.2.2.2. Especificaciones Técnicas

Especificaciones técnicas - Cámara IP modelo FI9804W	
Sensor de imagen	Sensor: High Definition Color CMOS Sensor
	Resolución: 720P (1280 x 720 Pixeles 1 Megapíxel), VGA, QVGA

Especificaciones técnicas - Cámara IP modelo FI9804W	
Sensor de imagen	Iluminación: 0 Lux mínimo
	Controles: control de brillo, contraste y frecuencia de luz.
Lentes	Cristal; Lentes IR-infrarrojas de visión nocturna; rosca estándar CS-Mount para intercambio de objetivos. f: 2.8 mm, 70° ángulo de visión
Vídeo	Compresión vídeo: H.264
	Stream: Triple stream
	Imágenes/seg.: 30 fps máx. (ajustable a valores inferiores)
	Resolución: 720P (1280 x 720 Pixeles 1 Megapíxel), VGA, QVGA
	Ajustes vídeo: brillo, contraste
Sonido	Entrada/Salida: Conectores jack estándares 3.5 mm para entrada/salida de audio. Compresión PCM/G.726
Comunicación	Red Ethernet: 10/100 Mbps RJ-45
	Protocolos: HTTP, FTP, TCP/IP, UDP, SMTP, DHCP, PPPoE, DDNS, UPnP, GPRS

Especificaciones técnicas - Cámara IP modelo FI9804W	
Comunicación	Wi-Fi: IEEE 802.11 b/g/n
	Seguridad Wi-Fi: Encriptación WEP, WPA, WPA2
Sistemas compatibles	Sistema operativo: Windows 2000/XP, Vista, 7, 8; MacOS, iOS, Android
	Navegador: IE, Firefox, Chrome, Safari
Datos Físicos	Dimensiones (mm): 173,3 (La) x 87,4 (An) x 83 (Al)
	Peso: 1186 gr (accesorios incluidos). Cámara sola con antena: 870 gr
Alimentación	Alimentación: adaptador DC 12V/2.0A.
	Consumo: 5,5 W máximo
Entorno	Temperatura: -20° ~ 55°C (operativa)/-20°C ~ 60°(almacenamiento)
	Humedad: 20% ~ 85% sin condensación (óptima operativa)/0% ~ 90% sin condensación (almacenamiento)

Tabla 6. Especificaciones Técnicas - Cámara IP modelo FI9804W

3.3.2.3. Cámara IP Apexis APM-HP602-MPC-WS



Fig. 36. Cámara IP Apexis APM-HP602-MPC-WS
Fuente: (Apexis, <http://www.apexis.es/productos/exterior/apm-hp602-mpc-ws>)

3.3.2.3.1. Descripción

Cámara IP Wi-Fi H.264 de alta resolución resistente al agua con salida-entrada de alarma I/O, salida y entrada de audio RCA, infrarrojos de gran alcance, lector de tarjetas micro-SD y conexión punto a punto P2P.

3.3.2.3.2. Características Principales

- Sensor de imagen CMOS de 1/3" (frente al de 1/4" de la gama tradicional)
- Resolución megapíxel de 1280x720 (frente a la resolución VGA de 640x480 de la gama tradicional)
- Compresión de vídeo H.264 (frente a la MJPEG de la gama tradicional)
- Capacidad de conexión punto a punto, P2P, que elimina la necesidad de abrir los puertos del router (frente a la obligatoriedad que presenta la gama tradicional de tener que configurar los parámetros internos del router si queremos conectarnos a la cámara IP desde WAN).

3.3.2.3.3. *Especificaciones Técnicas*

Especificaciones técnicas - Cámara IP Apexis APM-HP602-MPC-WS	
Sensor de imagen	Sensor: 1/3" Color CMOS Sensor
	Iluminación: 0.5Lux mínimo.
	Controles: control de brillo, contraste, color y nitidez
Lentes	f : 6 mm, F:2.0 (IR Lens)
Vídeo	Compresión vídeo: H.264, MJPEG
	Imágenes/seg.: 30fps(VGA),30fps(QVGA)
	Resolución: 640*480(VGA), 320*240(QVGA)
Audio	Modos de audio: dúplex completo.
	Micrófono: no / Altavoz: no
Comunicación	Protocolos de conexión en red: TCP/IP HTTP DNS DHCP PPPoE SMTP FTP SSL TFTP NTP ARP/RARP NFS RTSP RTP RTCP.
	Interfaz de red integrada: 10/100Mbps,Auto MDI/MDIX , RJ-45
	Conectividad inalámbrica: IEEE 802.11b/g/n. WEP & WPA WPA2.

Especificaciones técnicas - Cámara IP Apexis APM-HP602-MPC-WS	
Sistemas compatibles	Sistema operativo: Microsoft Windows 2000/XP/7/Vista
	Navegador: IE6.0/7.0/8.0/Firefox/Safari/Chrome.
Datos físicos	Movimiento: sin movimiento.
	Dimensiones (mm): 175 (L) x98(W) x98mm(H)
	Peso: 1200g aprox. (incluido los accesorios)
Alimentación	Alimentación: DC12V/2.0A
	Consumo: 9Watts (máx.)
Entorno	Temperatura: -30° ~ 55°C (-22°F ~ 131°F) operación /-30°C ~ 60° (-2°F ~ 140°F) almacenamiento.
	Humedad: 20% ~ 85% operación. 0% ~ 90% almacenamiento.

Tabla 7. Especificaciones técnicas - Cámara IP Apexis APM-HP602-MPC-WS

3.3.2.4. Comparación de Cámaras IP Exteriores

Categoría	Especificación	EasyN F-M1BF	FOSCAM FI9804W	Apexis APM-HP602
Sensor de imagen	Sensor	CMOS	Color CMOS Sensor	1/4" Color CMOS Sensor
	Resolución	640 x 480	1280 x 720	640 x 480
	Iluminación	0.3LUX	0 Lux mínimo	0 Lux mínimo
	Controles	Tamaño y calidad de la imagen ajustables.	Automáticos y manuales	Automáticos y manuales
Lentes	Lente	5-15mm	2.8 mm	6 mm
Audio	Entrada	Micrófono incorporado	Micrófono incorporado	No especificado
	Salida	No especificado	No especificado	No especificado
	Compresión audio	G.711/G.726	PCM/G.726	No especificado

Categoría	Especificación	EasyN F-M1BF	FOSCAM FI9804W	Apexis APM-HP602
Vídeo	Compresión vídeo	Motion-JPEG	Motion-JPEG	H.264, MJPEG
	Imágenes/seg.	25 fps máx.	30 fps máx.	30 fps máx.
	Resolución	640x480	1280x720	640*480
	Volteo imagen	Vertical / Horizontal	Vertical / Horizontal	Vertical / Horizontal
	Frecuencia luz	No especificado	50Hz, 60Hz, Outdoor	50Hz, 60Hz, Outdoor
	Ajustes vídeo	brillo, contraste	brillo, contraste	brillo, contraste saturación, agudeza
Comunicación	Red Ethernet	10/100 Mbps RJ-45	10/100 Mbps RJ-45	10/100 Mbps RJ-45
	Wi-Fi	IEEE 802.11b/g	IEEE 802.11b/g/n	IEEE 802.11b/g/n
	Seguridad Wi-Fi	No especificado	Encriptación WEP, WPA, WPA2	Encriptación WEP, WPA, WPA2

Categoría	Especificación	EasyN F-M1BF	FOSCAM FI9804W	Apexis APM-HP602
Sistemas compatibles	Sistema operativo	Windows 2000/XP, Vista, 7, 8; MacOS, iOS, Android	Windows 2000/XP, Vista, 7, 8; MacOS, iOS, Android	Windows 2000/XP, Vista, 7, 8; MacOS, iOS, Android
	Navegador	IE, Firefox, Chrome, Safari	IE, Firefox, Chrome, Safari	IE, Firefox, Chrome, Safari
Datos físicos	Movimiento	h:355 v: 90°	NO	NO
	Luz infrarroja	20 m	20 m	35 m
Alimentación	Alimentación	12V	12V	12V
	Consumo	No especificado	5,5 W	9 W
Entorno	Temperatura (operativa)	-10~50°C	0° ~ 40°C	-30° ~ 55°C
	Humedad (operativa/ sin condensación)	10%~90%	20% ~ 85%	20% ~ 85%

	EasyN F-M1BF	FOSCAM FI9804W	Apexis APM-HP602
Precio	190+I.V.A	160+I.V.A	160+I.V.A

Tabla 8. Comparación de Cámaras IP Exteriores

3.3.2.5. *Conclusión del Estudio de Cámaras IP Exteriores*

Al finalizar el estudio y comparación de características técnicas, se observa que la cámara Apexis APM-HP602 presenta similares características que las cámaras EasyN F-M1BF y FOSCAM FI9804W. Sin embargo; la principal especificación por la que se eligió esta cámara es que presenta mejor resolución en ambientes nocturnos; así como mejor capacidad de resistencia al entorno físico.

CAPITULO IV

4. IMPLEMENTACIÓN

Luego del planteamiento de requerimientos y del estudio de dispositivos disponibles en el mercado se procede con la implementación de la cámara IP Apexis APM-HP602 para exteriores en la zona A y la cámara Apexis APM-HP803 para interiores en la zona B.

Como parte de la implementación del sistema de video vigilancia se realiza la instalación del software de gestión de los dispositivos, así como su respectiva configuración de acuerdo a los requerimientos de seguridad de las autoridades de la institución.

Es importante mencionar que una de las características más relevantes de las cámaras elegidas es la posibilidad de gestionar la vigilancia mediante dispositivos móviles.

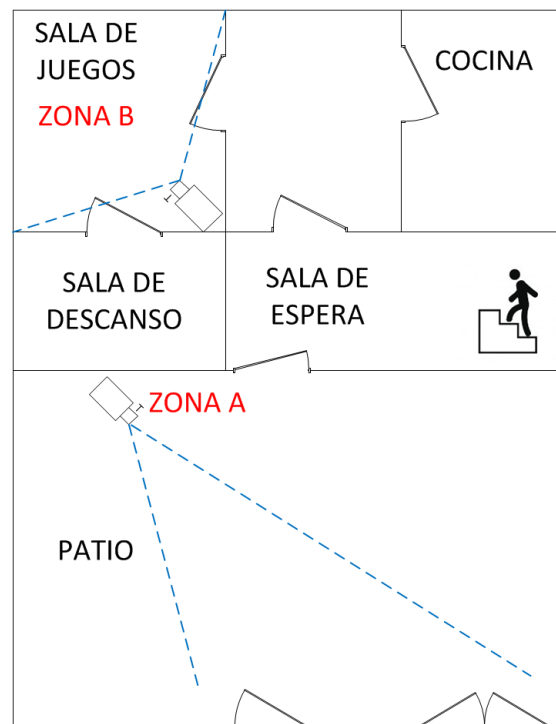


Fig. 37. Plano con ubicación de las cámaras y alcance de visión

4.1.1. Monitoreo de cámaras IP

Mediante la instalación del software gestor de cámaras IpCamClient, se pueden administrar hasta 64 cámaras simultáneamente.

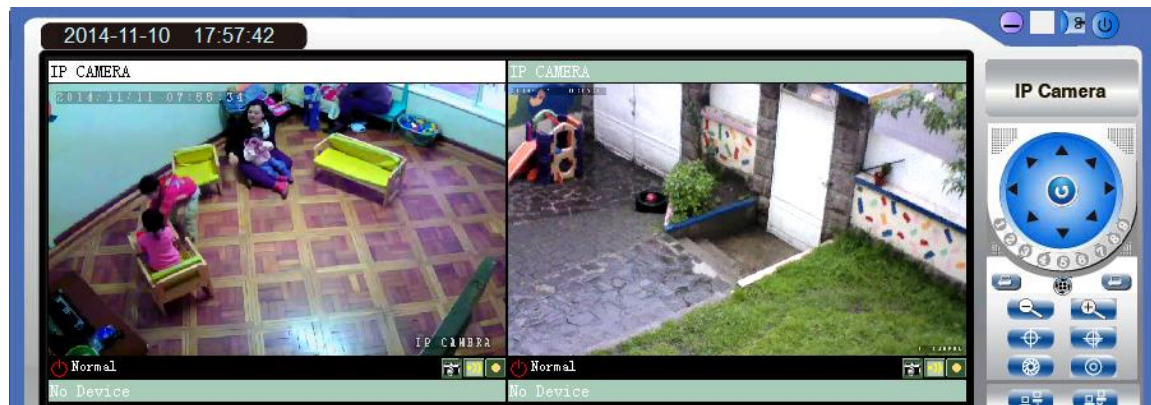


Fig. 38. Software de Gestión de Cámaras (IpCamClient) mostrando las vistas de los dos dispositivos instalados.

Con el acceso al router proporcionado por el proveedor de internet, se puede configurar el monitoreo a las cámaras mediante internet e incluso por aplicaciones móviles como TinyCam monitor.

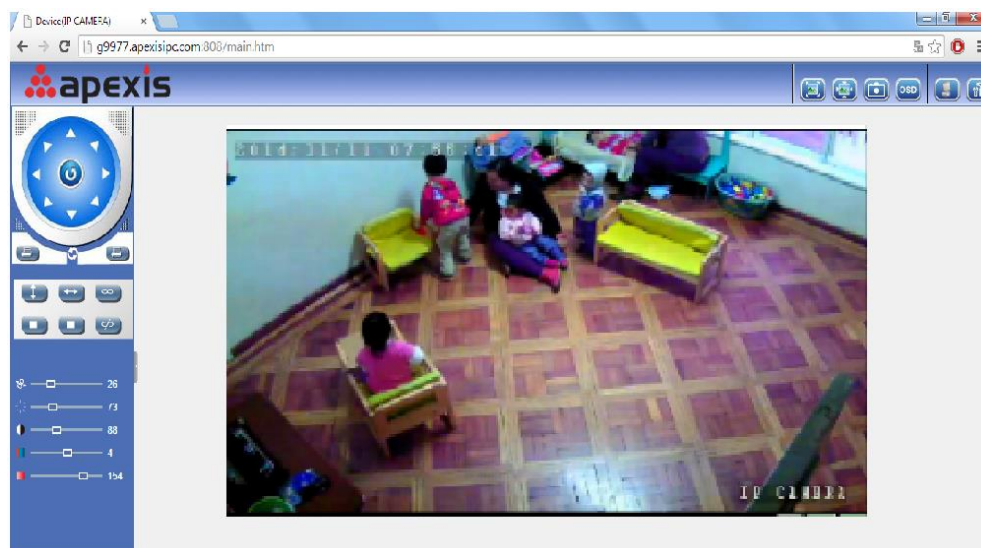


Fig. 39. Interfaz Web mediante DDNS

4.1.2. Cámara de la Zona A

El dispositivo implementado en esta zona permitirá monitorear la concentración de alumnos y padres de familia en las horas de entrada/salida. Así como el comportamiento de los niños, personas y vehículos que utilicen este acceso a la institución.



Fig. 40. Cámara IP - Zona A

La cámara IP de la zona A puede soportar lluvias, bajas temperaturas y calor intenso, características necesarias para soportar los cambios constantes en el clima de Quito. La configuración de la cámara permite almacenar grabaciones de video durante las 24 horas del día, posee LEDs infrarrojos que se activan automáticamente proporcionando así una imagen nítida en la oscuridad.

La figura 39, muestra el alcance de visión de la cámara IP de la zona A mediante el programa IP CAM CLIENT instalado en el computador de la oficina del centro infantil.



Fig. 41. Alcance de visión - Cámara Zona A

Esta cámara puede monitorearse remotamente; sin embargo no tiene la funcionalidad de orientación remota por lo que se realizó la instalación en un ángulo que permita mayor visibilidad y está situada en el segundo piso del centro infantil para protegerla de la delincuencia.

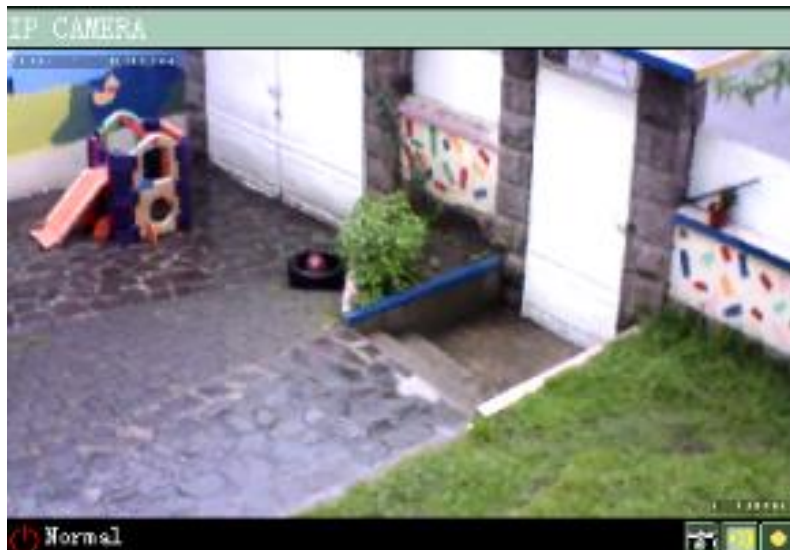


Fig. 42. Vista del patio principal - Cámara Zona A

Las cámaras Apexis instaladas en el Centro de Desarrollo Infantil “Angelitos Juguetones” pueden ser monitoreadas por medio de cualquier dispositivo móvil desde aplicaciones descargadas directamente de Google Play Store o Apple Store.

4.1.3. Cámara de la Zona B

El dispositivo implementado en el área de juegos de la institución permite controlar de la interacción y comportamiento de los docentes y niños. Así como monitorear el uso adecuado de los bienes que se ubican en esta zona.



Fig. 43. Cámara IP - Zona B

Esta cámara es ideal para vigilar remotamente las actividades diarias de los niños. Se puede acceder a su visualización (o gestión) mediante internet cuando se requiera. Podrá visualizar la cámara en tiempo real o cambiar su posición. Dispone de un filtro automático que permite obtener durante el día una imagen con colores nítidos y reales. Tiene también audio bidireccional. El sonido se transmite desde la cámara por medio de un micrófono integrado que se activa desde el programa IpCamClient.

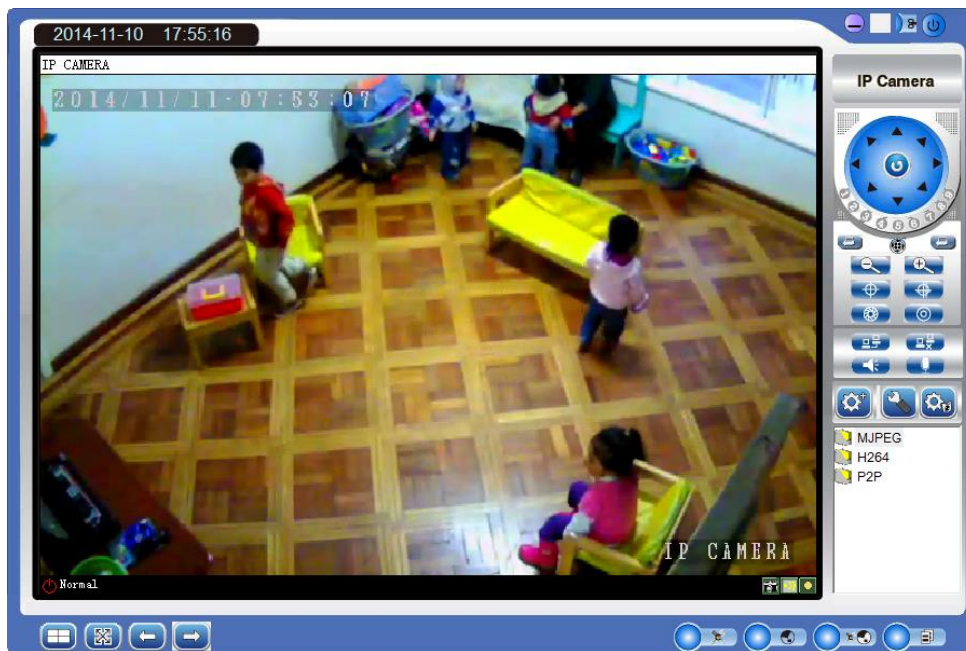


Fig. 44. IpCamClient - Zona B

El dispositivo de la zona B muestra la sala de juegos del centro infantil. Desde el software gestor de cámaras, su interfaz web, o desde una aplicación móvil se puede controlar el movimiento remoto.

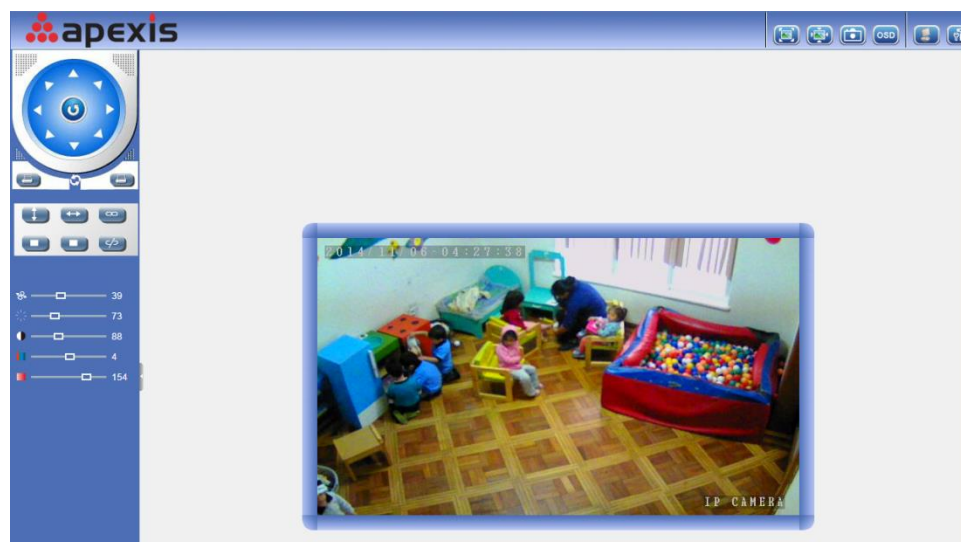


Fig. 45. Interfaz Web - Cámara Zona B

La cámara fue configurada para grabar automáticamente en el horario de atención del Centro de Desarrollo Infantil es decir desde las 08:00 hasta las 18:00 y para seguridad de los bienes de la institución se configuró la funcionalidad de

detección de movimiento en el horario de 18:00 hasta 08:00, de esta manera se cubren las 24 horas del día.

4.1.4. Red Cableada

Los dispositivos pueden conectarse a la red por medio de cable UTP o Wi-Fi. Se resolvió colocar cable UTP para no intervenir con la red Wi-Fi ya que el mayor tráfico de red se produce por este medio.

Todo el cableado interno tiene canaletas para cumplir con las normas de seguridad del Centro de Desarrollo Infantil además de contribuir con el ornato de la institución.



Fig. 46. Red Cableada - Canaletas

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- En términos de escalabilidad, el presente proyecto demuestra la amplia capacidad de los sistemas de video vigilancia IP de agregar varios dispositivos en red sin necesidad de adquirir un equipo adicional para gestionarlos.
- La implementación del sistema de video vigilancia con cámaras IP, representó una mejora significativa con respecto a la seguridad del plantel, puesto que se mantiene un registro del comportamiento y actividades realizadas en los espacios con mayores requerimientos de vigilancia; así como asegurar el uso adecuado de los recursos de la institución.
- El sistema cubre la necesidad de los padres de familia de visualizar la interacción entre los docentes y niños.
- Las investigaciones realizadas durante el desarrollo de este proyecto demuestran que en las configuraciones de sistemas con más de 32 cámaras, el costo inicial de un sistema de vigilancia basado en cámaras de red es incluso inferior si se compara con las opciones analógicas.
- Las cámaras IP representan una solución más confiable con respecto a las cámaras analógicas debido a que con una cámara analógica, la señal de vídeo se transporta por un cable coaxial sin ningún cifrado ni autenticación y cualquier individuo con conocimientos adecuados puede interceptar el vídeo o cambiar la señal de una cámara por otra señal de vídeo. A diferencia de la cámara IP que puede cifrar el vídeo que se envía a través de la red para asegurarse de que no pueda visualizarse ni interferirse por personal ajeno o fuera de la institución.

- La finalización de este proyecto nos permitió afianzar los conocimientos adquiridos en nuestros años de estudios, así como la comprensión de los aspectos teóricos y prácticos de los sistemas de video vigilancia IP.
- El sistema de video vigilancia IP instalado mejora significativamente la seguridad en la institución; sin embargo las cámaras no pueden hacer el trabajo solas. La vigilancia solo es vigilancia, la cámara no podría detener a un intruso y detenerlo en caso de robo, así que se recomienda no descuidar el monitoreo de los dispositivos.

5.2. RECOMENDACIONES

- Se recomienda que la contraseña de acceso al software de configuración en modo Super Administrador se maneje únicamente por la autoridad de la institución, para evitar cambios que afecten el funcionamiento normal de los dispositivos.
- Se recomienda el uso del gestor de usuarios para asignar de roles de interacción con el software, así se evitarían daños en los dispositivos causados por configuraciones erróneas.
- En la función de detección de movimiento de los dispositivos se recomienda configurar el nivel de sensibilidad en medio (o inferior), puesto que un nivel alto de sensibilidad podría causar un evento de falsa alarma.
- Se recomienda realizar un estudio previo a la colocación de cámaras adicionales pues deben ser ubicadas en lugares de difícil acceso para evitar que sean manipuladas por extraños y deben tener un buen ángulo de visión que permita vigilar las zonas conflictivas.
- Si se presenta alguna inquietud sobre el dispositivo y su configuración que no se pueda resolver mediante el manual entregado al usuario, se recomienda ponerse en contacto con el equipo de soporte técnico de Apexis, mediante la página web <http://www.apexis.com.cn/>.

BIBLIOGRAFÍA

- Apexis. (2012). *Apexis*. Recuperado el 18 de Agosto de 2014, de APM-HP602-MPC-WS: <http://www.apexis.es/productos/exterior/apm-hp602-mpc-WS>
- Apexis. (2012). *Apexis*. Recuperado el 12 de Agosto de 2014, de APM-HP803-MPC-WS: <http://www.apexis.es/productos/interior/apm-hp803-mpc-WS>
- Axis Communications. (2013). *Comparación de estándares*. Recuperado el 21 de Abril de 2014, de http://www.axis.com/es/products/video/about_networkvideo/compression_compare.htm
- Axis Communications. (2013). *Compresión de video*. Recuperado el 21 de Abril de 2014, de http://www.axis.com/es/products/video/about_networkvideo/compression.htm
- Axis Communications. (2013). *Formatos de compresión*. Recuperado el 21 de Abril de 2014, de http://www.axis.com/es/products/video/about_networkvideo/compression_formats.htm
- Axis Communications. (2013). *Frecuencia de bits variable y constante*. Recuperado el 21 de Abril de 2014, de http://www.axis.com/es/products/video/about_networkvideo/compression_bitrates.htm
- Axis Communications. (2013). *La evolución de los sistemas de video vigilancia por video*. Recuperado el 25 de Abril de 2014, de http://www.axis.com/es/products/video/about_networkvideo/evolution.htm#analog

- *Definicion.de.* (2008). Recuperado el 26 de Marzo de 2014, de <http://definicion.de/protocolo-de-red/>
- DLink. (2012). *Videovigilancia IP.* Recuperado el 26 de Agosto de 2014, de <http://www.dlink.com/es/es/business-solutions/ip-surveillance>
- Dlink Corporation. (s.f.). *DLink.* Recuperado el 12 de Agosto de 2014, de DCS-930L: <http://www.dlinkla.com.ec/dcs-930l>
- EasyN. (s.f.). *EasyN.* Recuperado el 26 de Julio de 2014, de Cámara F-M1BF: <http://www.easyn.com.es/ProductsShow.aspx?id=497#.U-5uhfl5OSp>
- FOSCAM. (s.f.). *Foscam Intelligent Technology.* Recuperado el 14 de Julio de 2014, de Cámara IP FI9826W: <http://www.foscam.es/FI9826W/>
- FOSCAM. (s.f.). *Foscam Intelligent Technology.* Recuperado el 18 de Agosto de 2014, de <http://www.foscam.es/FI9804W/>
- García Mata, F. J. (2011). *Videovigilancia: CCTV usando vídeos IP.* Málaga: Vértice.
- Garrido, F., Reascos, I., & Rivadeneira, J. (01 de Febrero de 2013). *Metodología para la implementación de Intranets.* Recuperado el 01 de Abril de 2014, de Capítulo II-TCP/IP: <http://repositorio.utn.edu.ec/handle/123456789/1096>
- Gómez, J. A. (2011). *Redes Locales.* Madrid: Editorial Editex, S.A.
- Maryem Aliria Ruiz, Luis Daniel Patiño. (s.f.). Recuperado el 24 de Marzo de 2014, de <http://fundamentosderedes.jimdo.com/2-protocolos-arquitectura-de-redes-y-modelo-osi-iso/arquitectura-de-redes/>
- Oracle. (2010). *Capítulo I-Conjunto de protocolos TCP/IP.* Recuperado el 01 de Abril de 2014, de <http://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0r9/index.html>

- Tanenbaum, A., & Wetherall, D. (2012). *Redes de Computadoras*. México: Pearson.
- *Textos Científicos*. (s.f.). Recuperado el 31 de Marzo de 2014, de <http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi>
- Universidad de Buenos Aires. (s.f.). *Redes*. Recuperado el 21 de Marzo de 2014, de http://www.econ.uba.ar/www/departamentos/sistemas/plan97/tecn_informatica/briano/seoane/tp/2002_1/redes.htm
- *Universidad del Azuay*. (s.f.). Recuperado el 20 de Marzo de 2014, de *Redes de Datos LAN:* http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan.pdf