



UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS,
ELECTRÓNICA E INDUSTRIAL
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y
COMUNICACIONES
SEMINARIO DE GRADUACIÓN

“Sistemas y de Redes de Comunicación Inalámbrica”

TEMA:

“SISTEMA DE VIDEO VIGILANCIA INALÁMBRICO PARA EL MEJORAMIENTO DE LA SEGURIDAD DEL EDIFICIO ADMINISTRATIVO DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO”

Trabajo de Grado Modalidad: Seminario de Graduación previo a la obtención del título de Ingeniera en Electrónica y Comunicaciones.

**AUTORA: Cifuentes Domínguez,
Gabriela Fernanda**

TUTOR: Ing. Geovanni Brito, Msc

AMBATO – ECUADOR

2012

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación, nombrado por el H. Consejo Superior de Pregrado de la Universidad Técnica de Ambato:

CERTIFICO:

Que el trabajo de investigación: “**Sistema de Video vigilancia Inalámbrico para el mejoramiento de la seguridad del edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato**”, presentado por la Srta. Gabriela Fernanda Cifuentes Domínguez, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato, Julio 2012

EL TUTOR

Ing. Geovanni Brito

AUTORÍA DEL TRABAJO DE GRADUACIÓN

El presente trabajo de investigación titulado: “**Sistema de Video vigilancia Inalámbrico para el mejoramiento de la seguridad del edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato**”. Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Julio del 2012

Gabriela Fernanda Cifuentes Domínguez

C.I. 1804066692

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docente Ing. M. Sc. Oswaldo Paredes, Ing. Julio Cuji, Ing. Juan Pablo Pallo, revisó y aprobó el Informe Final del trabajo de graduación titulado “SISTEMA DE VIDEO VIGILANCIA INALÁMBRICO PARA EL MEJORAMIENTO DE LA SEGURIDAD DEL EDIFICIO ADMINISTRATIVO DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO”, presentado por la Sra. Cifuentes Domínguez Gabriela Fernanda, de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ing. Oswaldo Paredes, M. Sc
PRESIDENTE DEL TRIBUNAL

Ing. Julio Cuji
DOCENTE CALIFICADOR

Ing. Juan Pablo Pallo
DOCENTE CALIFICADOR

DEDICATORIA

El presente trabajo está dedicado a Dios que ha guiado mi camino con esperanza, a mi tutor Ing. Geovanni Brito por su guía y ayuda para el desarrollo del proyecto, y a mi familia que me ha inspirado a ser mejor persona, con su amor, comprensión y dedicación.

Gabriela Cifuentes Domínguez

AGRADECIMIENTO

Mi agradecimiento profundo a mi mami que me ha brindado amor y apoyo incondicional a lo largo de mi vida, a mi papi por enseñarme el que el esfuerzo, la dedicación y constancia tienen buenos frutos, y a mi hermanita por ser mi guía, mi inspiración y brindarme su ayuda en todo momento.

A mis familiares, amigos, y demás personas que han convertido uno de mis sueños en realidad.

A las autoridades, y demás personal de la FISEI por darme la apertura para realizar mi proyecto, y al Ing. Geovanni Brito director del proyecto por brindarme su dedicación y tiempo.

Gabriela Cifuentes Domínguez

ÍNDICE GENERAL

Contenido	Página
PORTADA	ii
APROBACIÓN DEL TUTOR.....	iii
AUTORÍA DEL DEL TRABAJO DE GRADUACIÓN.....	iv
APROBACIÓN DE LA COMISIÓN CALIFICADORA.....	v
DEDICATORIA	vi
AGRADECIMIENTO	vii
ÍNDICE GENERAL	viii
ÍNDICE DE TABLAS	xii
ÍNDICE DE FIGURAS.....	xiv
RESUMEN EJECUTIVO	xvii
INTRODUCCIÓN	1
CAPÍTULO I	3
EL PROBLEMA DE INVESTIGACIÓN	3
1.1 Tema	3
1.2 Planteamiento del problema	3
1.2.1 Contextualización	3
1.2.2 Árbol del Problema	5
1.2.3 Análisis Crítico	5
1.2.4 Prognosis	6
1.2.5 Formulación del Problema	6
1.2.6 Preguntas Directrices	6
1.2.7 Delimitación del Problema	7
1.3 Justificación	7
1.4 Objetivos	8
1.4.1 Objetivo general	8
1.4.2 Objetivos específicos	8
CAPÍTULO II	10
MARCO TEÓRICO	10
2.1 Antecedentes investigativos	10
2.2 Fundamentación Legal	11

2.3 Figura de inclusión de las Categorías Fundamentales	12
2.3.1 Constelación de Ideas	13
2.4 Categorías Fundamentales	14
2.4.1 Sistema de vigilancia	14
2.4.2 Sistema de Vigilancia Física	14
2.4.3 Sistema de Vigilancia Electrónica	15
2.4.4 Sistema de Video vigilancia	16
2.4.5 Video Vigilancia IP	17
2.4.5.1 Cámaras de red	19
2.4.5.2 Codificadores de video	23
2.4.5.3 Sistemas de gestión de video	24
2.4.5.4 Video digital	27
2.4.5.5 Resolución	27
2.4.5.6 Técnicas de compresión	28
2.4.6 Redes de datos	30
2.4.7 Estándar IEEE 802.11 (Wi-Fi)	38
2.4.8 La seguridad en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial	40
2.4.8.1 Seguridad según el sector	41
2.4.8.2 Niveles de seguridad	42
2.4.8.3 Reglamentos de seguridad	44
2.5 Hipótesis	44
2.6 Señalamiento de variables	44
CAPÍTULO III	45
METODOLOGÍA	45
3.1 Enfoque de la investigación	45
3.2 Modalidad básica de investigación	45
3.3 Tipos de investigación	46
3.4 Población y Muestra	46
3.5 Operacionalización de variables	46
3.6 Técnicas e Instrumentos de Investigación	49
3.7 Recolección de la información	49
3.8 Procesamiento de la información	49
3.9 Análisis e interpretación de resultados	50
CAPÍTULO IV	51

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS	51
4.1 Encuesta	52
4.2 Ficha de Observación: Área Administrativa de la FISEI	58
4.3 Preguntas discriminantes	58
4.4 Situación actual de seguridad y vigilancia en la FISEI	59
CAPÍTULO V	67
CONCLUSIONES Y RECOMENDACIONES	67
5.1 Conclusiones	67
5.2 Recomendaciones	68
CAPÍTULO VI	70
PROPUESTA	70
6.1 Datos informativos	70
6.1.1 Título	70
6.1.2 Institución ejecutora	70
6.1.3 Tutor de tesis	70
6.1.4 Beneficiarios	71
6.1.5 Ubicación	71
6.1.6 Tiempo estipulado	71
6.1.7 Equipo técnico responsable	71
6.1.8 Costos	71
6.2 Antecedentes de la propuesta	71
6.3 Justificación	72
6.4 Objetivos	73
6.4.1 Objetivo general	73
6.4.2 Objetivos específicos	73
6.5 Análisis de Factibilidad	73
6.5.1 Factibilidad Técnica	74
6.5.2 Factibilidad Operativa	74
6.5.3 Factibilidad Económica	74
6.6 Fundamentación	75
6.6.1 Video Vigilancia IP Inalámbrico	75
6.6.1.1 Cámaras de red	75
6.6.1.2 Codificadores de video	77
6.6.1.3 Sistemas de gestión de video	77
6.6.1.4 Resolución	79

6.6.1.5 Técnicas de compresión	80
6.6.1.6 Soporte de Audio	83
6.6.2 Sistemas Inalámbricos	83
6.6.2.1 Topologías de un sistema inalámbrico	83
6.6.2.2 Seguridades de para un sistema inalámbrico	84
6.6.2.3 Estándar IEEE 802.11 (Wi-Fi)	85
6.7 Metodología	88
6.8 Diseño técnico del sistema	88
6.8.1 Introducción	88
6.8.2 Diseño físico	89
6.8.2.1 Topología física	90
6.8.3 Diseño lógico	115
6.8.3.1 Topología lógica	115
6.8.4 Requerimientos del sistema	118
6.8.5 Grabación y almacenamiento	131
6.8.6 Red WLAN	137
6.9 Presupuesto	139
6.10 Viabilidad de la propuesta	139
6.11 Conclusiones y Recomendaciones	142
BIBLIOGRAFÍA	144
LINKOGRAFÍA	144
GLOSARIO DE TÉRMINOS	146
ACRÓNIMOS	149
ANEXOS	151

ÍNDICE DE TABLAS

Contenido	Página
Tabla 3.1. Operacionalización de la variable independiente: Sistema de Vigilancia	47
Tabla 3.2. Operacionalización de la variable dependiente: Seguridad en el edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial	48
Tabla 3.3. Plan de recolección de información	49
Tabla 4.1. Tabulación Pregunta 1	52
Tabla 4.2. Tabulación Pregunta 2	53
Tabla 4.3. Tabulación Pregunta 3	54
Tabla 4.4. Tabulación Pregunta 4	55
Tabla 4.5. Tabulación Pregunta 5	56
Tabla 4.6. Tabulación Pregunta 6	57
Tabla 4.7. Ficha de observación	58
Tabla 6.1. Parámetros de ubicación de cámaras IP	99
Tabla 6.2. Radios de la Primera Zona de Fresnel	100
Tabla 6.3. Cálculos para Línea de Vista.....	100
Tabla 6.4. Atenuación en el Espacio Libre	101
Tabla 6.5. Intensidad de Campo eléctrico en recepción	102
Tabla 6.6. Potencia de recepción y Márgenes de desvanecimiento	103
Tabla 6.7. Tabla de Confiabilidad en base al Margen de Desvanecimiento	104
Tabla 6.8. Topología lógica de la red de Video Vigilancia	116
Tabla 6.9. Características de selección para el Switch Ethernet	120
Tabla 6.10. Características de selección para el Radio de comunicación inalámbrica	120
Tabla 6.11. Características de selección para Cámaras IP fijas	120
Tabla 6.12. Características de selección para Cámaras IP PTZ	121
Tabla 6.13. Características de selección para el servidor de video	121
Tabla 6.14. Características de selección para el software de gestión de video	121
Tabla 6.15. Comparación Switch Ethernet	122
Tabla 6.16. Comparación equipos inalámbricos	122

Tabla 6.17.	Comparación cámaras IP fijas	123
Tabla 6.18.	Comparación cámaras IP PTZ	123
Tabla 6.19.	Comparación servidores de video	124
Tabla 6.20.	Relación entre la compresión y la resolución	132
Tabla 6.21.	Cálculo para la capacidad de almacenamiento	136
Tabla 6.22.	Presupuesto total	139
Tabla 6.23.	Tabla de gastos para Vigilancia física	140
Tabla 6.24.	Tabla de gastos para Vigilancia IP	141
Tabla 6.25.	Costo de funcionamiento del sistema de Vigilancia IP	141

ÍNDICE DE FIGURAS

Contenido	Página
Figura N° 1.1. Árbol del problema	5
Figura N° 2.1. Categoría Fundamental Variable Independiente	12
Figura N° 2.2. Categoría Fundamental Variable Dependiente	12
Figura N° 2.3. Constelación de ideas de la variable independiente	13
Figura N° 2.4. Constelación de ideas de la variable dependiente	13
Figura N° 2.5. Sistemas de seguridad contra incendios	15
Figura N° 2.6. Sistema de Video vigilancia IP	16
Figura N° 2.7. Marcas de componentes de Vigilancia IP	17
Figura N° 2.8. Integración de un sistema analógico de vigilancia a un sistema de Video IP	18
Figura N° 2.9. Ventajas de la Vigilancia IP	18
Figura N° 2.10. Vigilancia IP en universidades	19
Figura N° 2.11. Componentes de una cámara IP	20
Figura N° 2.12. Definición de 1lux	20
Figura N° 2.13. Clases de cámaras de red	22
Figura N° 2.14. Decodificador para Vigilancia IP	24
Figura N° 2.15. Sistema de gestión de video	24
Figura N° 2.16. Plataforma NVR marca QNAP	25
Figura N° 2.17. Uso de la Resolución analógica alrededor del mundo	27
Figura N° 2.18. Formatos de compresión utilizados en cámaras de red	28
Figura N° 2.19. Comparación entre los formatos de compresión más Utilizados	30
Figura N° 2.20. Tipos de Medios guiados	31
Figura N° 2.21. Tipos de Fibra óptica	32
Figura N° 2.22. Diferentes Medios No guiados	33
Figura N° 2.23. Servicios y procesos en los dispositivos de una red IP	34
Figura N° 2.24. Capas de modelos de red	34
Figura N° 2.25. Diferentes Topologías físicas	36
Figura N° 2.26. Red alámbrica	37
Figura N° 2.27. Red híbrida	38
Figura N° 2.28. Comparación entre los diferentes estándares Wi-Fi	39
Figura N° 2.29. Edificio principal de la FISEI	41

Figura N° 2.30.	Edificio secundario de la FISEI	41
Figura N° 2.31.	Diagrama de relación Riesgos-Reglamentos de seguridad	43
Figura N° 4.1.	Pregunta 1	52
Figura N° 4.2.	Pregunta 2	53
Figura N° 4.3.	Pregunta 3	54
Figura N° 4.4.	Pregunta 4	55
Figura N° 4.5.	Pregunta 5	56
Figura N° 4.6.	Pregunta 6	57
Figura N° 4.7.	Sensor de movimiento Administración de Redes	61
Figura N° 4.8.	Sensor de movimiento LAB N° 1	62
Figura N° 4.9.	Sensor de movimiento Secretaría de Carrera	62
Figura N° 4.10.	Sirena ubicada en el edificio principal de la facultad	63
Figura N° 4.11.	Tablero de control	63
Figura N° 4.12.	Central telefónica	64
Figura N° 4.13.	Teléfono interconectado a la Central telefónica	64
Figura N° 4.14.	Electrocerradura de la puerta principal del área administrativa	65
Figura N° 4.15.	Botón para desactivación de la electrocerradura	65
Figura N° 6.1.	Cámara Fija	76
Figura N° 6.2.	Cámara Domo Fija	76
Figura N° 6.3.	Cámara PTZ	77
Figura N° 6.4.	Codificador de video	77
Figura N° 6.5.	Servidor HP Proliant ML350 G6	78
Figura N° 6.6.	Software de Gestión de cámaras IP D-Link	79
Figura N° 6.7.	Soporte de audio y video	83
Figura N° 6.8.	Topología Punto – Multipunto	84
Figura N° 6.9.	Arquitectura de un Sistema inalámbrico	86
Figura N° 6.10.	Diagrama físico del la red	91
Figura N° 6.11.	Simbología del diagrama físico de red	92
Figura N° 6.12.	Campo visual de una cámara de red	94
Figura N° 6.13.	Campo visual de la cámara 1	94
Figura N° 6.14.	Campo visual de la cámara 2	95
Figura N° 6.15.	Campo visual de la cámara 3	95
Figura N° 6.16.	Campo visual de la cámara 4	96
Figura N° 6.17.	Campo visual de la cámara 5	96

Figura N° 6.18.	Campo visual de la cámara 6	97
Figura N° 6.19.	Campo visual de la cámara 7	97
Figura N° 6.20.	Campo visual de la cámara 8	98
Figura N° 6.21.	Campo visual de la cámara 9	98
Figura N° 6.22.	Cámara 1 ubicada en la oficina de Secretaria de Carrera	105
Figura N° 6.23.	Cámara 3 ubicada en las escaleras del primer piso	105
Figura N° 6.24.	Cámara 2 ubicada en la entrada al ágora del edificio Principal	106
Figura N° 6.25.	Cámara 6 ubicada en la entrada secundaria al edificio principal	106
Figura N° 6.26.	Cámara 4 ubicada en la oficina de Secretaria Subdecanato	107
Figura N° 6.27.	Cámara 7 ubicada en el segundo piso frente a la Biblioteca	107
Figura N° 6.28.	Cámara 8 ubicada en el segundo piso frente al Ágora	108
Figura N° 6.29.	Radio 1 localizado en el segundo piso frente a Administración de Redes	108
Figura N° 6.30.	Cámara 5 localizada en la oficina de Asistente de Secretaria General	109
Figura N° 6.31.	Radio 2 ubicado en la primera planta	109
Figura N° 6.32.	Cámara 9 ubicada en la primera planta del nuevo Edificio	110
Figura N° 6.33.	Primera planta del edificio principal con cámaras IP	111
Figura N° 6.34.	Segunda planta del edificio principal con cámaras IP	112
Figura N° 6.35.	Tercera planta del edificio principal con cámaras IP	113
Figura N° 6.36.	Primera planta del nuevo edificio con cámaras IP	114
Figura N° 6.37.	Diagrama lógico del la red IP	117
Figura N° 6.38.	Pantalla principal del software de gestión D-ViewCam de D-Link	127
Figura N° 6.39.	Pantalla principal del modo de Configuración Experto	129

RESUMEN EJECUTIVO

El presente proyecto tiene como tema: “Sistema de Video vigilancia Inalámbrico para el mejoramiento de la seguridad del edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato”.

El Capítulo I contiene el Problema de Investigación, que enfoca los problemas que afectan a los niveles de seguridad en el edificio administrativo de la FISEI.

El Capítulo II se refiere al Marco Teórico, que presenta un estudio técnico sobre vigilancia IP, sus principios de operación, componentes, estándares y formatos de video digital; un análisis sobre el estándar IEEE 802.11, sus componentes, estructuras y formas de seguridad, finalmente normas y reglamentos de seguridad.

El Capítulo III contiene la Metodología, que se aplica al trabajo, para determinar los procedimientos para elaborar la propuesta, el tipo de enfoque que se dio a la investigación, la modalidad y el tipo de investigación utilizada.

El Capítulo IV se sujeta al Análisis e Interpretación de Resultados, posterior a la recolección de información en base a las técnicas e instrumentos de investigación, los datos obtenidos fueron tabulados, analizados sistemáticamente e interpretados de conformidad a las preguntas planteadas.

El Capítulo V narra las Conclusiones y Recomendaciones, que se han obtenido del análisis de los resultados de la recolección de información lo cual ayudará a la realización de la propuesta.

El Capítulo VI contiene la Propuesta, que consiste en la realización del diseño de un Sistema de Video vigilancia Inalámbrico utilizando tecnología y equipos IP.

INTRODUCCIÓN

Actualmente las instalaciones que comprenden la Facultad de Ingeniería en Sistema, Electrónica e Industrial no tienen un eficiente sistema de seguridad y vigilancia, ya que el sistema con el que se cuenta es un sistema de vigilancia físico que no cubre las necesidades que seguridad de una institución educativa, del personal, de las y los estudiantes, del equipamiento e información, que son necesarias para la enseñanza de las diferentes ciencias.

El presente proyecto tiene como finalidad resolver los problemas relacionados a la seguridad que afectan al edificio administrativo, a través del diseño de un sistema de vigilancia electrónico.

Los sistemas de video vigilancia se han convertido en una de las aplicaciones de vigilancia electrónica más utilizadas e implementadas en la sociedad, en áreas como la Educación, el Comercio, la Salud, entre otras; por brindar ventajas como la flexibilidad, convergencia y escalabilidad.

Lo que se busca es salvaguardar la integridad de los empleados y personas que visitan las instalaciones, controlar y disminuir hechos delictivos como robos, pérdida de información y daño a las instalaciones, con equipamiento como cámaras de red las cuales permiten capturar y enviar video en tiempo real a través de una red IP, permitiendo el acceso y visualización del video por medio de un software de gestión en cualquier equipo local o remotamente conectado a la red.

La propuesta de la investigación surge por la necesidad de mejorar los niveles de seguridad del área administrativa de la FISEI, debió a la pérdida de equipos suscitada en las oficinas de las autoridades, y otros incidentes que han influenciado negativamente a la imagen de la facultad.

Con el diseño de un sistema de Video vigilancia Inalámbrica para el edificio administrativo (y áreas que requieren vigilancia y mejor seguridad), los

responsables del área de seguridad tendrán una solución integral que satisface los requerimientos de seguridad, y al mismo tiempo se reducirán costos operativos, de fácil administración, y almacenamiento continuo de información para ser utilizada cuando sea necesario.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 Tema

“Sistema de video vigilancia inalámbrico para el mejoramiento de la seguridad del edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial (FISEI) de la Universidad Técnica De Ambato.”

1.2 Planteamiento del problema

1.2.1 Contextualización

En estas últimas décadas el mundo entero ha estado inmerso en cambios en lo que concierne a aspectos económicos, culturales y sociales, por el hecho mismo de la globalización; las barreras entre países cada vez se hacen más pequeñas, permitiendo la ampliación de oportunidades para el desarrollo humano.

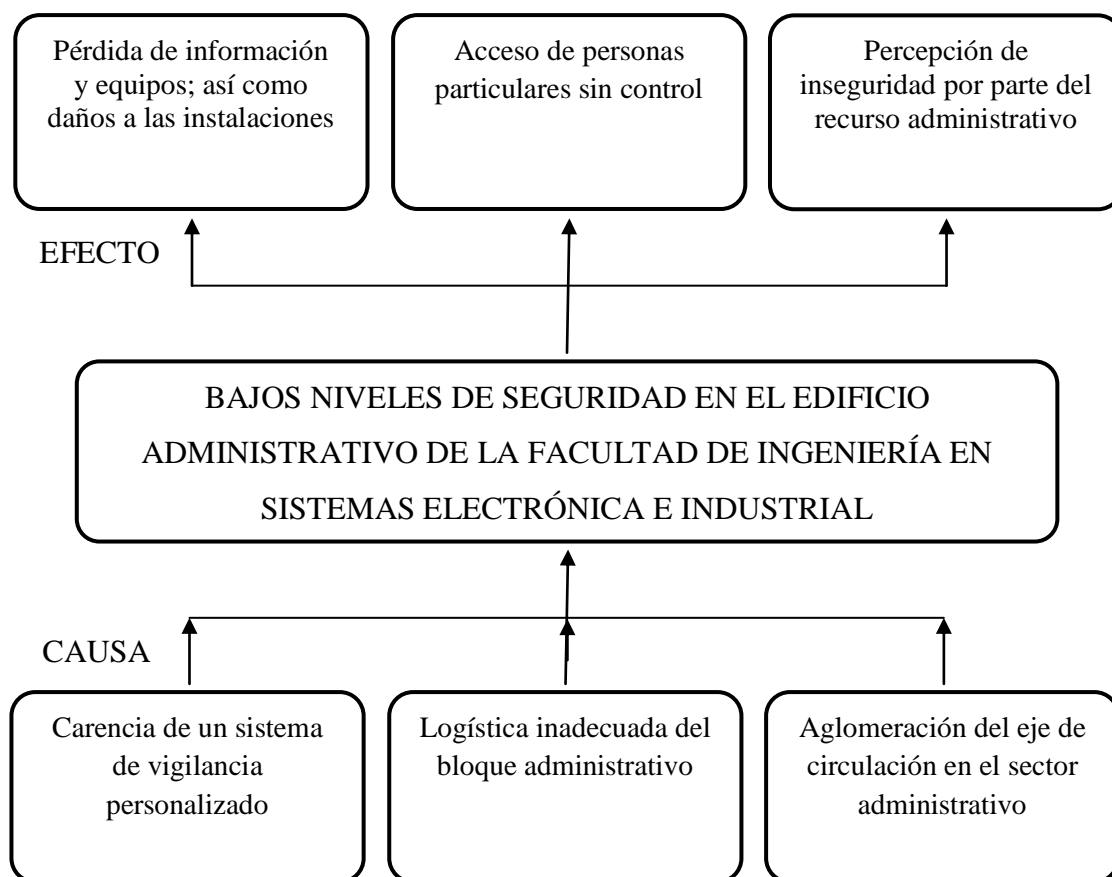
En nuestro país en materia de seguridad el presente gobierno ha implementado programas para mejorar la seguridad nacional y la seguridad ciudadana, como por ejemplo “El Plan de Seguridad Integral”, “Plan Nacional del Buen Vivir

(SumakKawsay)”, los cuales están enfocados en el ser humano, y en su bienestar, respondiendo a las necesidades de planificación y a los objetivos del Gobierno Nacional en la reestructura de todos los niveles institucionales que tienen que ver con Seguridad; pero en la realidad la inseguridad, la corrupción y otros males sociales siguen siendo un problema latente dentro de la vida diaria de los ecuatorianos, como puede evidenciarse en los encabezados de periódicos nacionales que publican: La inseguridad, el gran problema/Editorial de El Comercio, Seguridad: Otra reforma/Editorial de El Comercio, Inseguridad crucial/Carlos Jaramillo Abarca, Quito registra un promedio de 20 muertes violentas al mes desde 2009. El gran problema de la seguridad no solo abarca niveles nacionales, sino internacionales que han surgido en gran parte debido a diversas problemáticas que afectan a la sociedad, la familia y la falta de respeto a la propiedad ajena.

Ambato conocida como la Ciudad Cosmopolita, la cual cuenta con 309.000 habitantes en el área urbana, ha buscado como solución a esta problemática el uso de sistemas de seguridad física y tecnológica, en donde esta última debido al gran auge de las tecnología IP ha sido aplicada en hogares, pequeñas tiendas de barrio, centros educativos y grandes industrias, para salvaguardar las instalaciones, equipos y lo más importante el personal humano.

La Facultad de Ingeniería Sistemas, Electrónica e Industrial al ser un ente de educación dentro de la provincia cuenta con equipamiento e información académica para el estudio de las diferentes ciencias, y requiere un mejor sistema de seguridad y vigilancia; ya que en años pasados se han producido robos dentro de oficinas y laboratorios, debido a que no se cuenta con personal de seguridad exclusivo para el área administrativa, de laboratorios y demás sectores que comprenden los predios de la facultad.

1.2.2 Árbol del Problema



*Figura N° 1.1 Árbol del problema
Elaborado por: La Investigadora*

1.2.3 Análisis Crítico

El problema de inseguridad que ha afectado a la FISEI es inherente a la realidad del país y del mundo entero, actualmente se cuenta con un sistema de vigilancia compuesto por algunos guardias que al no tener una cobertura total de las instalaciones no han podido brindar una seguridad tanto preventiva, como ejecutora al cien por ciento, dando lugar al daño o destrucción de equipos, herramientas, daño a las instalaciones y usos inadecuados de las mismas; debido a la falta de vigilancia, al poco interés de estudiantes, docentes y autoridades; y a la

falta de recursos que deberían ser destinados para precautelar posibles riesgos o accidentes.

Entre otros factores que han afectado la percepción de seguridad dentro del bloque administrativo se encuentra el deficiente control de acceso, y aglomeración en la sección de oficinas en horas pico, lo que ha traído consigo malestar a las personas que allí laboran y a las que visitan las instalaciones.

1.2.4 Prognosis

Al no solucionar el tipo de vigilancia del edificio administrativo de la FISEI de la ciudad de Ambato, atentará a la seguridad de las personas que diariamente trabajan o visitan dichas instalaciones, al igual que la pérdida de información y al equipamiento del área administrativa, además perjudicará a la imagen de institución de educación superior líder en la provincia.

1.2.5 Formulación del Problema

¿Cómo incide el sistema de vigilancia en los niveles de seguridad en el edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato?

1.2.6 Preguntas Directrices

¿Qué sistemas de vigilancia se aplican en el edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato?

¿Los niveles de seguridad que dispone el edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial son adecuados y garantizan el resguardo de los bienes e información que reposan en el mismo?

¿Se pueden mejorar los niveles de seguridad del edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial mediante una propuesta de diseño de un sistema de video vigilancia inalámbrico?

1.2.7 Delimitación del Problema

CAMPO: Ingeniería Electrónica y Comunicaciones

ÁREA: Redes de Comunicaciones

ASPECTO: Sistema de video vigilancia

DELIMITACIÓN ESPACIAL: Edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, ubicado entre la Av. de los Chasquis y Río Guayllabamba, sector Huachi.

DELIMITACIÓN TEMPORAL: Seis meses a partir de la aprobación por parte del Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.3 Justificación

La FISEI se ha convertido en una de las facultades más importantes de la Universidad Técnica de Ambato, por su calidad de enseñanza y el ser proactivos en el desarrollo de proyectos educativos; por estas razones debe contar con un ambiente que propicie el mejoramiento personal y educativo. Áreas como la administrativa deben ser resguardadas con un sistema de seguridad que tenga una

visión global, y permita almacenar imágenes para que en caso de suceder algún delito o inconveniente permita aclarar los hechos.

El uso de la Tecnología digital ha influido en varias áreas permitiendo el desarrollo de nuevas aplicaciones debido a sus características, pudiendo citar entre ellas: rentabilidad, escalabilidad, y convergencia; lo que ha permitido mejorar la calidad de vida de las personas en general. Es por eso que la implementación de sistemas de video vigilancia con Tecnología IP es más común cada día, debido a que un sistema de vigilancia persigue garantizar la protección de los bienes y del personal, permitiendo el acceso remoto y brindando un mejor desempeño que los sistemas análogos. El presente proyecto denominado “Sistema de video vigilancia inalámbrico para el mejoramiento de la seguridad del edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato” tiene como objetivo diseñar un sistema integral de seguridad que permita el adecuado desarrollo de las actividades propias del edificio, mejorando la atención al público en general, y brindando una adecuada vigilancia y seguridad, para así generar confianza en el personal que allí trabaja y frecuenta las instalaciones, y para el equipamiento que conforma el área administrativa.

1.4 Objetivos

1.4.1 Objetivo general:

Diseñar un sistema de video vigilancia inalámbrico para el mejoramiento de los niveles de seguridad en el edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

1.4.2 Objetivos específicos:

1. Analizar los sistemas de vigilancia aplicados actualmente en la facultad.

2. Determinar los niveles de seguridad en el área administrativa de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

3. Proponer un sistema de video vigilancia inalámbrico con tecnología IP que permita mejorar los niveles de seguridad en el edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la ciudad de Ambato.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes investigativos

Revisando diversas fuentes bibliográficas como la biblioteca de la FISEI e Internet se ha encontrado los siguientes trabajos relacionados al tema propuesto, entre ellos se menciona:

“ESTUDIO Y DISEÑO DE UN SISTEMA DE VIGILANCIA Y MONITOREO DE VIDEO EN TIEMPO REAL, SOBRE UNA RED IP, PARA UN TERMINAL DE DESPACHO Y BOMBEO DE COMBUSTIBLE DE LA GERENCIA REGIONAL SUR DE PETROCOMERCIAL”. Realizado por Kléber Palacios. Año 2006. Y que entre sus principales conclusiones están:

- Establecer las bases del funcionamiento de un sistema de video vigilancia sobre una red IP como un servicio de seguridad y detección de intrusos que se implementan en un terminal de despacho y bombeo de combustible de la regional sur de PETROCOMERCIAL.

“SISTEMA DE VIDEO VIGILANCIA PARA LA BRIGADA DE CABALLERÍA BLINDADA NÚMERO 11 “GALÁPAGOS” EN LA CIUDAD DE RIOBAMBA”. Realizado por: Washington Ibarra. Año 2008. En donde se han llegado a las siguientes conclusiones:

- El CCTV es uno de los sistemas más prácticos y rentables en materia de seguridad. Además que es un sistema que funciona en tiempo real.
- La migración hacia la tecnología de video digital, es importante debido a sus ventajas respecto a la tecnología digital sobre la tecnología analógica.

2.2 Fundamentación Legal

El presente proyecto se basó en las normativas que regulan el funcionamiento de la Universidad Técnica de Ambato relacionadas a Seguridad y Vigilancia, al igual que las leyes de la actual Constitución del Ecuador relacionadas a Comunicación e Información, Educación Superior, y Propiedad intelectual.

La Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato (FISEI), abrió sus puertas en Octubre de 1991. Su creación fue una respuesta a los retos del avance de la ciencia y la tecnología. Se vencieron obstáculos de local y de presupuesto. H. Consejo Universitario, presidido por el Ing. Víctor Hugo Jaramillo, aprobó su funcionamiento. La Facultad nació en los predios de Ingahurco, junto a la Facultad de Ciencias Humanas y de la Educación, con 120 estudiantes, siendo su primer decano el Ing. Washington Medina.

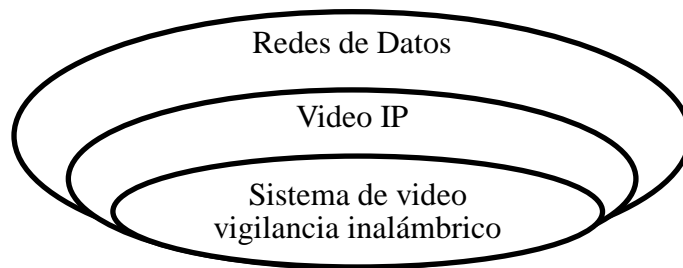
Con el paso del tiempo la Facultad creció en estudiantes, profesores y empleados; se ve la necesidad de un edificio propio y es así como en el año de 1992 se inicia la construcción de la Facultad en los predios de Huachi.

El crecimiento de los estudiantes ha sido notable, pese a que las autoridades han tenido que restringir el ingreso para no sobrepasar el límite de la infraestructura

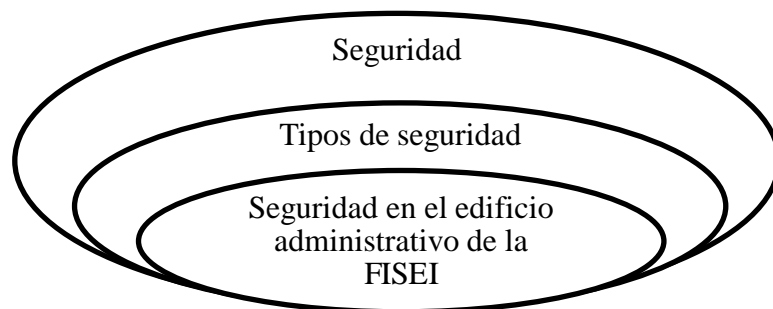
física, actualmente tenemos 1000 estudiantes en la modalidad presencial, se cuenta con tres especialidades: Sistemas, Electrónica e Industrial.

Más importante ha sido el desarrollo académico manifestado en la seriedad científica, que los propios estudiantes han aceptado de buen grado; el perfil profesional garantiza expertos para el mundo laboral. Todo esto responde al esfuerzo de profesores, trabajadores, estudiantes y a la dedicación de las autoridades que han dirigido a la Facultad.

2.3 Figura de inclusión de las Categorías Fundamentales



*Figura N° 2.1. Categoría Fundamental Variable Independiente
Elaborado por: La Investigadora*



*Figura N° 2.2. Categoría Fundamental Variable Dependiente
Elaborado por: La Investigadora*

2.3.1 Constelación de Ideas

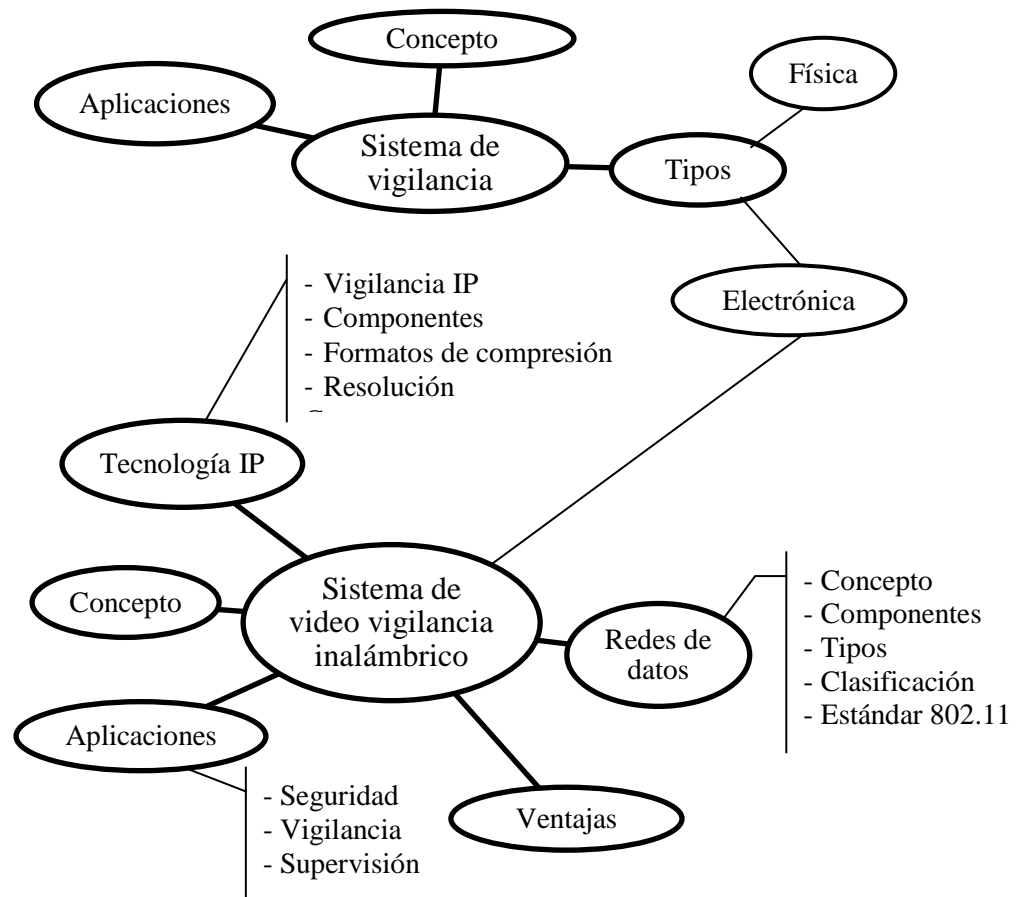


Figura N°2.3. Constelación de ideas de la variable independiente
Elaborado por: La Investigadora

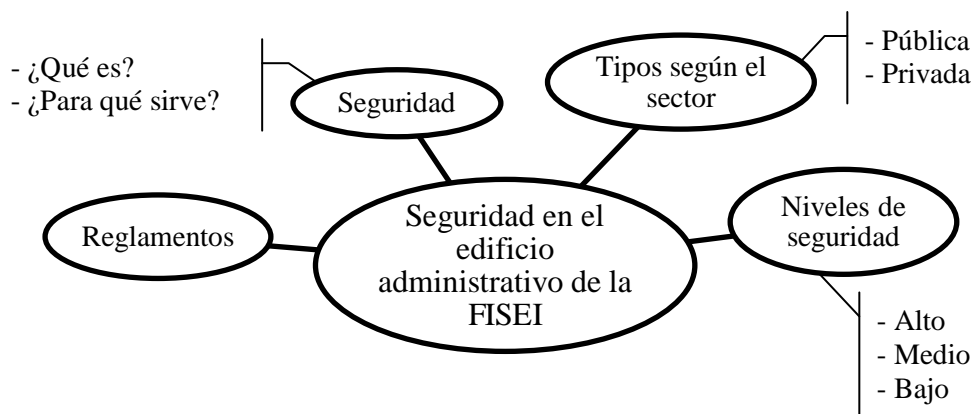


Figura N° 2.4. Constelación de ideas de la variable dependiente
Elaborado por: La Investigadora

2.4 Categorías Fundamentales

2.4.1 Sistema de vigilancia

Un sistema de vigilancia es un conjunto de medios o dispositivos tecnológicos, que se encargan del monitoreo, y observación de no solo personas, sino también de objetos o procesos para la conformidad de normas esperadas o deseadas dentro de la sociedad.

Después de un análisis bibliográfico y práctico sobre la temática la investigadora concibe como sistema de vigilancia a una serie de procesos mediante el uso de la tecnología para captar información, para así proteger el presente y el futuro de ataques de cualquier índole.

Entre las características que favorecen un sistema de vigilancia se encuentran: visualización y/o vigilancia con ayuda técnica, prevención de incidentes como hurto, vandalismo, y sensación de inseguridad.

2.4.2 Sistema de Vigilancia Física

Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información de organizaciones.

El objetivo de la Seguridad Física es resguardar la seguridad patrimonial de las personas, comunidades y organizaciones. El personal de vigilancia o guardias representan el elemento clave de todo sistema de seguridad. Requieren una formación y entrenamiento para prevenir robos y daños, proteger y generar un ambiente seguro y comfortable.

2.4.3 Sistema de Vigilancia Electrónica

La aparición de la electrónica nos ha permitido un rápido progreso en lo que se refiere al concepto de seguridad, ya que nos proporciona una variedad de posibilidades en los sistemas de seguridad, cada día más amplia y eliminando de esta forma viejos conceptos y formas de vida.

Características de importancia de este tipo de seguridad se mencionan en *Internet (¿Qué es Seguridad electrónica?, http://www.slideshare.net/martinn2/que-es-seguridad-electrnica, 5, octubre, 2011; 14:00 h)* como “La importancia de los Sistemas de Seguridad Electrónica, radica en que se sustenta en el uso de alta tecnología aplicada a la seguridad y soportada en un adecuado diseño, instalación e interconexión, de modo tal, que permita obtener una alerta temprana de los eventos generados en las instalaciones, en el momento en que están siendo vulneradas por personas no ajenas a la organización”.

Al hablar de seguridad electrónica nos referimos a aquellos sistemas como los de monitoreo satelital, sistemas de alarmas y software de seguridad que podamos utilizar para proteger no solo nuestra propiedad sino también nuestros bienes. Como ejemplos de aplicación tenemos: Seguridad en la vivienda, Seguridad en los establecimientos, Seguridad activa contra incendios, entre otros.



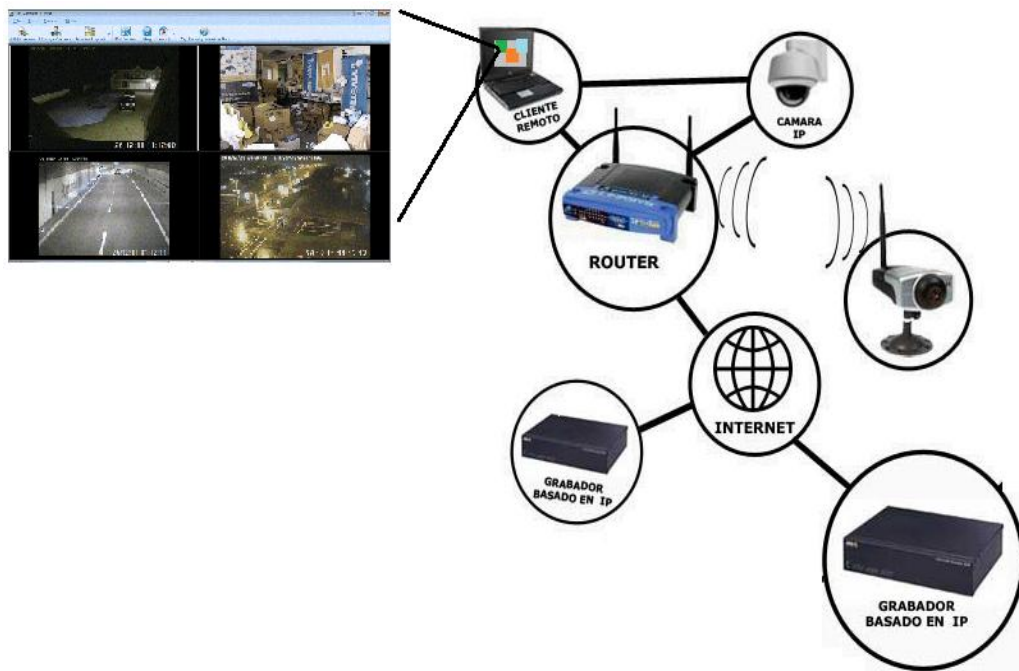
Figura N° 2.5. *Sistemas de seguridad contra incendios*
Fuente: <http://www.ico-ecuador.com/icoecua.php?c=1272>

En la *figura N° 2.5* se puede apreciar un conjunto de medios activos que permiten la detección, alerta y señalización de posibles incendios dentro de una institución, en la actualidad este tipo de sistemas son un requisito indispensable dentro de la infraestructura de un edificio.

2.4.4 Sistema de Video vigilancia

En general podemos definir a un sistema de seguridad, como el conjunto de elementos e instalaciones necesarios para proporcionar a las personas y bienes materiales existentes en un local determinado, protección frente a agresiones, tales como robo, atraco o sabotaje e incendio.

La *figura N° 2.6*, muestra un sistema completo de vigilancia IP; con el cual se puede brindar seguridad y vigilancia las 24 horas del día, en varias locaciones en tiempo real, desde un software de gestión de video propio de la cámara IP.



*Figura N° 2.6. Sistema de Video vigilancia IP
Elaborado por: La Investigadora*

2.4.5 Video Vigilancia IP

El manual técnico de *AXIS-Guía técnica de vídeo IP (2009, pág. 7)* menciona como característica de la vigilancia IP que “El video en red o vigilancia IP, utiliza una red IP inalámbrica o con cable para transportar video y audio digital, y otros datos”.

Un sistema de video en red permite supervisar video y grabarlo desde cualquier lugar de la red, tanto si se trata por ejemplo de una red LAN o de una red WAN como Internet.

Existen varios fabricantes a nivel mundial que desarrollan componentes de calidad para sistemas de video vigilancia, entre esas marcas encontramos a las mencionadas en la *figura N° 2.7*, las cuales tienen sucursales en el Ecuador pudiendo ser adquiridas.



*Figura N° 2.7. Marcas de componentes de Vigilancia IP
Elaborado por: La Investigadora*

- Componentes

Los componentes básicos de un sistema de video en red son: la cámara de red, el codificador de video (para la conexión a cámaras analógicas), la red, el servidor y el almacenamiento, así como el software de gestión de video.

- Ventajas

El sistema de video vigilancia de red digital ofrece toda una serie de ventajas a diferencia de los sistemas analógicos, como por ejemplo:

- Accesibilidad remota.
- Alta calidad de imagen.
- Gestión de eventos.
- Capacidades de video inteligente, así como la posibilidad de una integración sencilla entre sistemas con tecnología analógica y sistemas con tecnología IP (la *figura N° 2.8* muestra una de las características más importantes de la vigilancia IP, a través de la implementación de un codificador de video para integrar cámaras analógicas y equipamiento con tecnología IP), escalabilidad, flexibilidad y rentabilidad mejoradas.

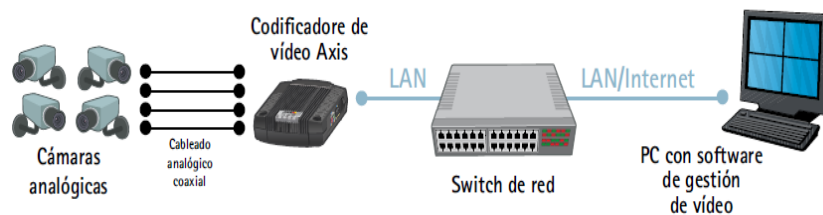


Figura N° 2.8. Integración de un sistema analógico de vigilancia a un sistema de Video IP

Fuente: AXIS COMMUNICATIONS, *El acceso más fácil al vídeo en red* (2009, pág. 16)

Las ventajas de combinar la tecnología digital, es decir Redes IP y Medios Digitales nos dan como resultado características que hacen que un sistema de Vigilancia IP sea un sistema integral, eficiente y eficaz.

Entre las ventajas se mencionan las siguientes en la *figura N° 2.9*.

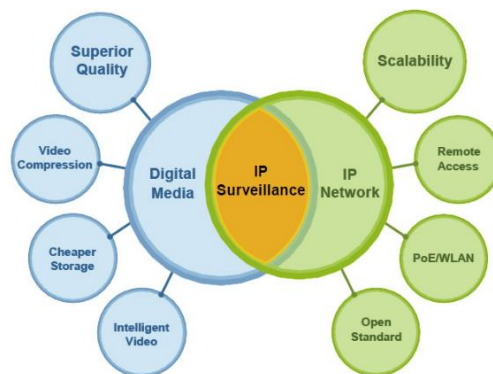


Figura N° 2.9. Ventajas de la Vigilancia IP

Fuente: <http://www.deseecom.com/es>

- **Aplicaciones**

Dentro del ámbito de seguridad, vigilancia, supervisión del personal, operaciones, y propiedades:

Entre las principales aplicaciones el manual de *AXIS-Vigilancia IP inalámbrica para aplicaciones de seguridad (2003, pág. 8)* menciona “En el transporte, Educación, en la Industria, Vigilancia urbana, Seguridad ciudadana, Asistencia sanitaria, Banca y finanzas”.



Figura N° 2.10. Vigilancia IP en universidades

Fuente: http://hualaralnoticias.blogspot.com/2010_10_09_archive.html

Detalle de los componentes:

2.4.5.1 Cámaras de red

La evolución de la tecnología ha permitido la implementación de nuevos dispositivos a redes IP, este es el caso de las cámaras IP. Estas cámaras a partir de su localización permiten ver al usuario lo que está sucediendo en tiempo real, desde cualquier punto dentro de una red o de la Internet.

Cada cámara tiene su propio direccionamiento IP y características propias de ordenador para gestionar la comunicación en la red. Además de capturar video, algunas cámaras cuentan con características extras como detección de movimiento, detección de audio, puertos E/S, entre otras.

Los componentes de una cámara de red, necesarios para capturar y transmitir imágenes al sistema de gestión de video, independiente de la marca de cámara se detallan en la *figura N° 2.11*.

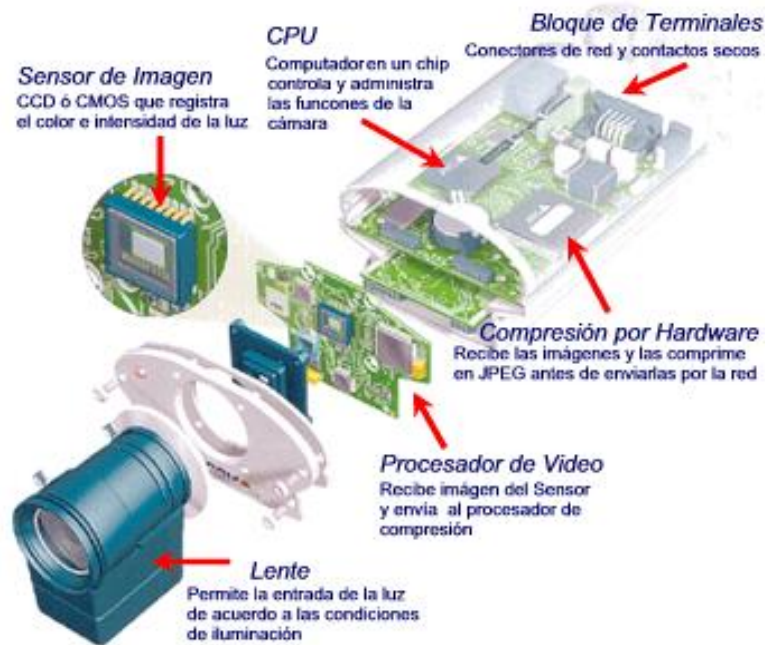


Figura N° 2.11. Componentes de una cámara IP
Fuente: <http://www.gscsoftware.com/teccamaraip.htm>

a) Elementos de una cámara IP

- **Sensibilidad lumínica:** Especificada en términos de *lux*, que es el nivel de iluminación en el que una cámara produce una imagen aceptable.

Cuanto menor sea la especificación de lux, mejor será la sensibilidad lumínica de la cámara.

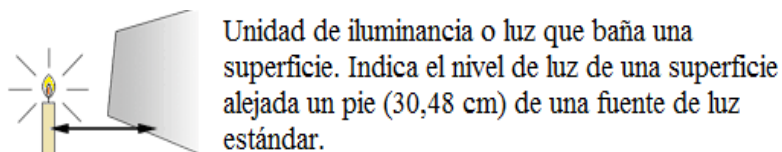


Figura N° 2.12. Definición de *lux*
Elaborado por: La Investigadora

- ***Tipos de objetivo:*** Existen tres tipos de objetivo principales:

Objetivo fijo: ofrece solamente un campo de visión.

Objetivo de óptica variable: ofrece diferentes campos de visión.

Objetivo con zoom: se parecen a los objetivos de óptica variable en el permitir la selección de los campos de visión.

- ***Procesamiento de la imagen:***

Características para mejorar la calidad de imagen:

Compensación de contraluz: un contraluz intenso puede provocar que los objetos en primer plano aparezcan oscuros. Las cámaras de red con compensación de contraluz intentan ignorar áreas limitadas con mucha iluminación.

Alcance amplio y dinámico

b) Tipos de cámaras de red

Las cámaras de red, diseñadas para su uso en interiores o exteriores, pueden clasificarse en cámaras de red fijas, domo fijas, PTZ y domo PTZ.

- **Cámaras de red fijas:** Es una cámara que dispone de un campo de vista fijo una vez montada. Este tipo de cámara es la mejor opción en aplicaciones en las que resulta útil que la cámara este bien visible.

- **Cámaras de red domo fijas:** También conocidas como mini domo, constan 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 diseño, y la dificultad de ver hacia qué dirección apunta la cámara.

- **Cámaras PTZ y cámaras domo PTZ**

Las cámaras PTZ y domo PTZ pueden moverse horizontalmente, verticalmente y acercarse o alejarse de un área o un objeto de forma manual o automática. Todos

los comandos PTZ se envían a través del mismo cable de red que la transmisión de video.

Las cámaras de red PTZ no disponen de un movimiento horizontal de 360 grados debido a la existencia de un tope mecánico. Mientras que las cámaras de red domo PTZ permiten un movimiento horizontal continuo de 360 grados y un movimiento vertical de normalmente 180 grados.

En la *figura N° 2.13*, se muestran gráficamente las diferentes clases de cámaras de red que existen en el mercado, las cuales en base a sus componentes y funcionalidades brindan distintos beneficios.



***Figura N° 2.13. Clases de cámaras de red
Elaborado por: La Investigadora***

c) Cámaras de red con visión diurna/nocturna

Las cámaras con visión diurna y nocturna están diseñadas para su uso en instalaciones exteriores o en entornos interiores con poca iluminación.

Proporcionan imágenes a color a lo largo del día, pero cuando la luz disminuye bajo un nivel determinado, la cámara puede cambiar automáticamente al modo nocturno para utilizar la luz prácticamente infrarroja para proporcionar imágenes de alta calidad en blanco y negro.

d) Criterios para seleccionar una cámara de red

- *Definir el objetivo de video vigilancia:*

El objetivo de vigilancia determinara el campo de visión, la ubicación de la cámara y el tipo de cámara.

- *Zona de cobertura:*

La zona de cobertura determinara el tipo y el número de cámaras que se utilizaran.

- *Entorno interior o exterior:*

Para exteriores se debe tener en cuenta la sensibilidad lumínica y condiciones lumínicas, carcasa

- *Vigilancia visible u oculta.*

- *Del manual técnico de AXIS-Guía técnica de vídeo IP (2009, pág. 24) se detalla que “Otras características con las que debe contar una cámara son: calidad de imagen, resolución, compresión, audio, funcionalidades de red, aplicaciones de software, selección del proveedor de productos de video en red”.*

2.4.5.2 Codificadores de video

Permiten la integración de un sistema de video vigilancia analógico CCTV existente a un sistema de video en red.

Para FULUSHIMA, Sergio (2009) “Las señales de la cámara analógica al pasar por el codificador de video son convertidas en secuencias de video digitales para luego ser enviadas a través de la red IP, para la visualización y/o grabación del video digital se puede utilizar el monitor del computador, monitores analógicos, y computadores en lugar de DVR ó VCR”.

- **Decodificador de vídeo**

Se encarga de descodificar video digital y audio procedente de una cámara IP o de un codificador de video, para luego visualizar la señal en monitores analógicos.

La *figura N° 2.14*, muestra un equipo decodificador de video, el cual funciona de forma inversa a un codificador de video para vigilancia IP. Este tipo de equipos son muy útiles porque permiten integrar la tecnología Digital y Analógica, sin tener que prescindir de instalaciones previas.



Figura N° 2.14. Decodificador para Vigilancia IP

Fuente: <http://cirview.circontrol.com/cirview/videovigilancia-ip-profesional-en-red/video-servidores-y-decodificadores-ip-para-cctv-concencional-analogico/codecs-d--0>

2.4.5.3 Sistemas de gestión de video

Un sistema de gestión de video se encarga de la visualización, grabación, reproducción y almacenamiento en directo del video.

En el caso que el sistema esté formado por una o pocas cámaras, la visualización y la grabación de video es gestionada a través de la interfaz Web incorporada de las cámaras IP y los codificadores de video.

Cuando el sistema consta de más cámaras, es recomendable usar un sistema de gestión de video en red.

Los aspectos a tomar en cuenta son la elección de plataforma de hardware, la plataforma de software, y características del sistema.



Figura N° 2.15. Sistema de gestión de video
Elaborado por: La Investigadora

En la *figura N° 2.15* se muestra los componentes (plataformas) de un sistema de gestión de video de un Sistema de Vigilancia IP.

a) Plataformas de hardware

Existen dos tipos para un sistema de gestión de video en red:

- Plataforma de servidor de PC

El manual técnico de *AXIS-Guía técnica de vídeo IP (2009, pág. 91)* conceptualiza que “Un sistema de gestión de video basado en una plataforma de servidor de PC incluye servidores de PC y equipos de almacenamiento para el mejor rendimiento de un sistema”.

- Plataforma NVR

Un grabador de video en red es un hardware con funcionalidades de gestión de video preinstaladas.

El NVR es diseñado para la gestión de video, teniendo como tareas la grabación, análisis y reproducción de video en red y normalmente no permite que ninguna otra aplicación se conecte a este.

La *figura N° 2.16* muestra un servidor NVR marca QNAP, el cual presta servicios de monitoreo de video y audio en tiempo real, además playback de múltiples cámaras IP.



Figura N° 2.16. Plataforma NVR marca QNAP

Fuente: <http://www.qnap.com/index.asp>

b) Plataformas de software

Se pueden utilizar plataformas de software diferentes para gestionar video.

- Funcionalidad incorporada

Se puede acceder a las cámaras de red y los codificadores de video por medio de una red introduciendo la dirección IP del producto en el campo Dirección/Ubicación de un navegador Web de un ordenador. La interfaz Web ofrece funciones de grabación simples.

- Software basado en cliente de Windows

Con un programa basado en cliente de Windows, primero se debe instalar el software de gestión de video en el servidor de grabación. Después, se puede instalar un programa de software de cliente de visualización en el mismo servidor de grabación o en cualquier PC.

- Software basado en Web

Primero se debe instalar un programa de software de gestión de video basado en Web en un servidor de PC que sirva tanto de servidor Web como de grabación, permitiendo a los usuarios de cualquier parte del mundo y con cualquier tipo de ordenador conectado a la red acceder al servidor de gestión de video y a los productos de video en red que gestiona.

c) Características del sistema

Un sistema de gestión de video debe tener las siguientes características:

- Visualización simultanea de video desde varias cámaras
- Grabación de video y audio
- Funciones de gestión de eventos con video inteligente
- Administración y gestión de cámaras
- Seguridad

2.4.5.4 Video digital

Video digital es la reproducción en forma secuencial de imágenes, que al verse con una determinada velocidad y continuidad dan la sensación al ojo humano de apreciar el movimiento natural. Junto con la imagen, el otro componente es el sonido. Se almacenan en un determinado formato digital de video.

2.4.5.5 Resolución

La resolución de video define el máximo detalle que se puede obtener en una imagen.

- Para *video analógico*, una imagen consta de líneas de TV. Se aplican las dos siguientes resoluciones:

a) NTSC (Comité Nacional de Sistemas de Televisión): tiene una resolución de 480 líneas y utiliza una frecuencia de actualización de 60 campos entrelazados por segundo.

b) PAL (Línea de Alternancia de Fase): tiene una resolución de 576 líneas y utiliza una frecuencia de actualización de 50 campos entrelazados por segundo.

Como se puede apreciar en la *figura N° 2.17*, el uso de los formatos de resolución de video analógico varía según el país.

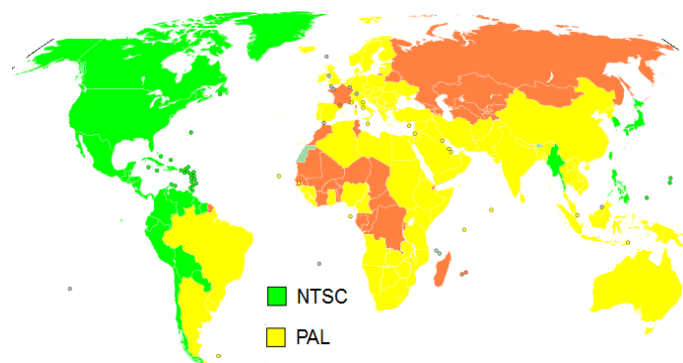


Figura N° 2.17. Uso de la Resolución analógica alrededor del mundo

Fuente: <http://es.wikipedia.org/wiki/NTSC>

- En el video digital, un sistema digital una imagen está formada por pixeles cuadrados. Se aplican los siguientes tres tipos de resoluciones:

a) **VGA** (Tabla de Gráficos de Video) es un sistema de pantalla de gráficos para PC. Tiene una resolución de 640 x 480 pixeles, ideal para cámaras de red.

b) **Resolución megapíxel**, una cámara de red que ofrece este tipo de resolución si cuenta con un sensor megapíxel, mientras más pixeles tenga el sensor, mayor será la resolución de la imagen.

c) **Resolución de televisión de alta definición (HDTV)**, proporciona una resolución hasta cinco veces más alta que la televisión analógica estándar, debido a que se basa en pixeles cuadrados.

2.4.5.6 Técnicas de compresión

En el manual de AXIS-*Guía técnica de vídeo IP (2009, pág. 55)* se conceptualiza a la *compresión* como “La compresión consiste en reducir y eliminar datos redundantes del video para que el archivo de video digital se pueda enviar por la red y ser almacenado”.

La *figura N° 2.18* muestra los formatos de compresión más utilizados en cámaras de red, para transmitir audio y video en tiempo real hacia en software y hardware de gestión del sistema de vigilancia hacia cualquier punto que se encuentre dentro de la red IP.

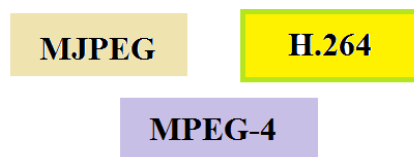


Figura N° 2.18. *Formatos de compresión utilizados en cámaras de red*
Elaborado por: La investigadora

a) Formatos de compresión

- **Formato MJPEG (Motion-JPEG es una versión extendida del algoritmo JPEG).**

Trata al video digital como una secuencia de imágenes estáticas independientes a las que se aplica el proceso de compresión del algoritmo JPEG una y otra vez para cada imagen de la secuencia de video.

- **Formato MPEG (Grupo de Expertos en Imágenes en movimiento)**

Es un estándar internacional, para la compresión de imágenes en movimiento y audio asociado, orientado a medios de almacenamiento digital.

El algoritmo que utiliza además de comprimir imágenes estáticas compara los fotogramas presentes con los anteriores y los futuros para almacenar sólo las partes que cambian. La señal incluye sonido en calidad digital. Existen diferentes opciones dependiendo del uso:

MPEG-1 guarda una imagen, la compara con la siguiente y almacena sólo las diferencias.

MPEG-2, transmite video digital comprimido con velocidades de hasta de 20 Mbps aproximadamente. *MPEG-2* cubre imágenes más grandes y de mayor calidad.

Para VELLACOTT, Oliver (2010, pág. 80) *MPEG4*, “es un estándar orientado inicialmente a las videoconferencias, y para Internet”. Es rápido codificando el video de alta calidad, para contenidos en tiempo real y bajo demanda.

- **Formato H; H.261, 263, 321, 324, entre otros.**

Estándares recomendados por la *ITU*. Conjunto de normas diseñadas para video conferencia, aunque se emplean en algunas ocasiones con cámaras de red. Producen imágenes de muy baja calidad.

H.264 es un estándar de compresión de video más actual y eficaz.

Puede reducir el tamaño de un archivo de video digital, requiriendo menos ancho de banda y espacio de almacenamiento para los archivos de video.

Como se puede apreciar en la siguiente figura (*figura N° 2.19*) el formato H.264 presenta mejores características de compresión a comparación de los otros dos formatos existentes; la compresión la realiza sin comprometer el ancho de banda de la red al momento de realizar la grabación de video, al igual que el espacio de almacenamiento.

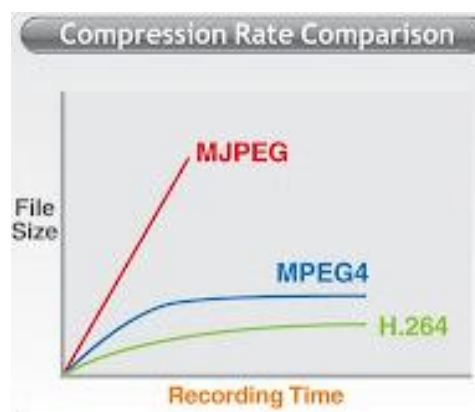


Figura N° 2.19. Comparación entre los formatos de compresión más utilizados
Fuente: <http://ecomspain.blogspot.com/2010/05/video-grabador-ip.html>

2.4.6 Redes de datos

Una red es sencillamente la unión por diversos medios de dos o más computadoras personales o hosts, con el objetivo de compartir recursos con los cuales cuente cada una de ellas, así como para expandir sus capacidades.

- Componentes de una red

a) Los *dispositivos y los medios* son los *elementos físicos* o hardware de la red.

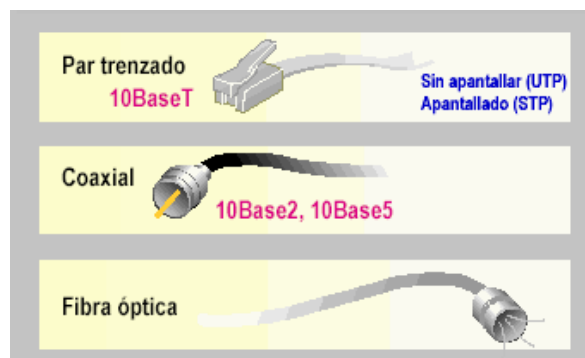
- Los **dispositivos finales** o host son los dispositivos con los que trabajan directamente las personas, y constituyen el origen o destino de un mensaje transmitido a través de la red.

- Los **dispositivos intermedios** proporcionan conectividad y garantizan que los datos fluyan a través de la red.

- Los **medios** de red transportan los datos que permiten la comunicación por una red. Las redes usan tres tipos de medios para interconectar los dispositivos. Estos medios son:

Hilos metálicos dentro de cables: Par trenzado (UTP, STP), Coaxial.

La *figura N° 2.20*, muestra los medios guiados que son utilizados para la implementación de una red.



*Figura N° 2.20. Tipos de Medios guiados
Elaborado por: La Investigadora*

- *Cable de Par trenzado*

Es un medio de conexión compuesto por hilos de cobre, trenzados entre sí.

Entre los tipos más comunes se encuentran: UTP (Cable par trenzado no apantallado), STP (Cable de par trenzado apantallado).

- *Coaxial*

De una fuente de *Internet (Medios de transmisión, www.wiener.edu.pe/manuales2/4to-ciclo/...1/Manual-Redes.pdf, 2, octubre, 2011; 8:30 h)* se mencionan características del cable coaxial como: “Es un conductor cilíndrico exterior que rodea un solo conductor interior, ambos conductores están

aislados entre sí. En el centro del cable hay un único hilo de cobre o alguna aleación conductiva, rodeado por un aislante flexible. Sobre este aislante, una pantalla de cobre trenzado actúa como segundo conductor. Finalmente una cubierta aislante recubre el conjunto”.

- *Fibras de vidrio o plástico (cable de fibra óptica).*

Es un medio capaz de conducir transmisiones de luz modulada. No es susceptible de interferencias ya que a diferencia del resto de cables no usa pulsos eléctricos, sino de luz. Este cable es utilizado para grandes distancias y alta capacidad de aplicaciones de comunicación.

Existen dos tipos de fibra:

Para PALLO, Juan P (2010, pág. 24) la fibra óptica se clasifica en “*Monomodo*”: En esta fibra la luz viaja por el eje del cable. Este modo es mucho más rápido, ya que el núcleo no permite la dispersión del haz.

Multimodo: Las ondas de luz entran en la fibra con distintos ángulos y viajan rebotando entre las paredes del núcleo. Su precio es más barato”.

En la *figura N° 2.21*, se puede apreciar los diferentes tipos de fibra óptica que son usados en base a factores como: distancia, costo, índices de refracción y tipo de aplicación.

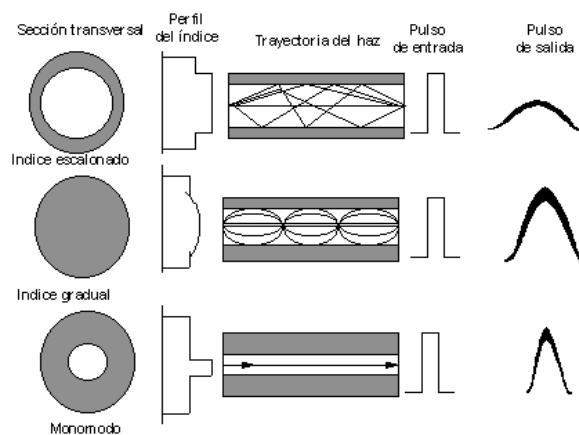


Figura N° 2.21. Tipos de Fibra óptica

Fuente: <http://www.mitecnologico.com/Main/MediosGuiados>

- *Transmisión inalámbrica: Por aire.*

Los medios inalámbricos transportan señales electromagnéticas mediante frecuencias de microondas y radiofrecuencias que representan los dígitos binarios de las comunicaciones de datos. El medio inalámbrico también es susceptible a la interferencia y puede distorsionarse.

Entre los diferentes tipos, se mencionan los siguientes:

Microondas terrestres: La transmisión de estas señales es de líneas de visión; esto es, la señal de radio viaja en línea recta de una estación repetidora a la siguiente hasta llegar a su destino.

Ondas de radio: Ondas omnidireccionales, que no necesitan de antenas parabólicas. Las ondas electromagnéticas poseen distintas propiedades y usos, dependiendo de su longitud.

Microondas satelital: Un satélite actúa como una estación repetidora. Los beneficios de la comunicación por satélite desde el punto de vista de comunicaciones de datos son: transferencia de información a altas velocidades, ideal para comunicaciones en puntos distantes y no fácilmente accesibles geográficamente.

Según el tipo de aplicación y el alcance que ésta requiere se utilizan los medios no guiados que se visualizan en la *figura N° 2.22*.

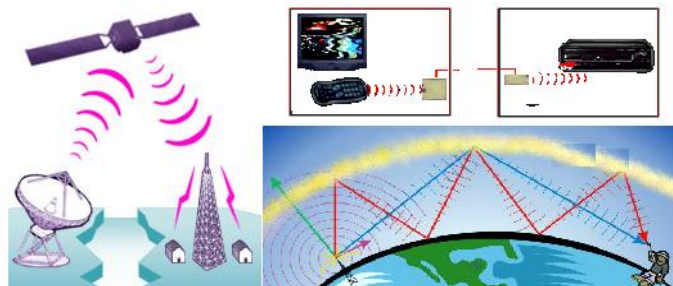


Figura N° 2.22. Diferentes Medios No guiados
Elaborado por: La Investigadora

b) Los *servicios y procesos* son los programas de comunicación, llamados software, que se ejecutan en los dispositivos conectados a la red.

La *figura N° 2.23*, muestra los servicios más utilizados en una red IP, como son: videoconferencia, correo electrónico, y descarga de archivos.



Figura N° 2.23. Servicios y procesos en los dispositivos de una red IP
Elaborado por: La Investigadora

c) *Protocolos de red*, son el conjunto de reglas predeterminadas, que rigen la forma en cómo los dispositivos de una red se comunican entre sí.

Entre los protocolos necesarios para el funcionamiento de una red encontramos los listados en la siguiente figura (*figura N° 2.24*), estos protocolos se los utiliza en base a las funcionalidades de las diferentes capas que conforman un modelo de red.

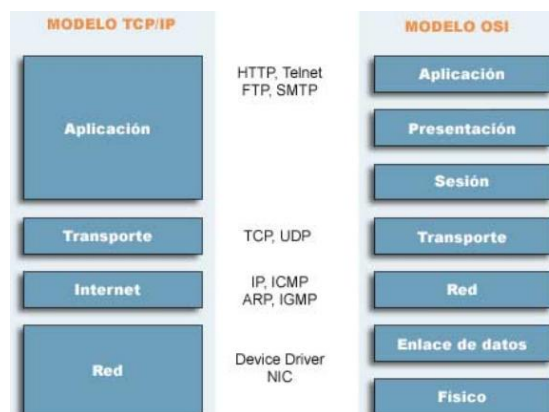


Figura N° 2.24. Capas de modelos de red
Fuente: <http://n4jredes1.blogspot.com/p/protocolos-de-red.html>

- **Tipos de redes según la cobertura física**

- **Redes LAN o Red de Área Local:** Conjunto de computadoras que pueden compartir datos, aplicaciones y recursos. Las computadoras de una red de área local están separadas por distancias de hasta unos pocos kilómetros.

- **Redes WAN o Red de Área Extendida:** Son redes que se extienden a larga distancia, conectando varias redes LAN separadas geográficamente. Las WAN utilizan dispositivos de red diseñados específicamente para realizar las interconexiones entre las LAN.

- **Topología de red**

La topología de red define la estructura de una red. La topología se divide en física y lógica.

- La *topología física* es la disposición real de los cables o medios. Entre los principales tipos están:

Topología bus, usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.

Topología de anillo, conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.

Topología en estrella, conecta todos los cables con un punto central de concentración.

Topología en estrella extendida, conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.

Topología de malla, se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio.

El uso de una determinada topología afecta la forma en cómo se comunica la información entre los diferentes componentes de una red de datos.

La *figura N° 2.25* enlista los tipos de topologías físicas existentes, que se pueden usar para la disposición de los medios físicos en una red IP. Dentro de las topologías más utilizadas se encuentran la topología estrella, y estrella extendida; por su característica de escalabilidad.

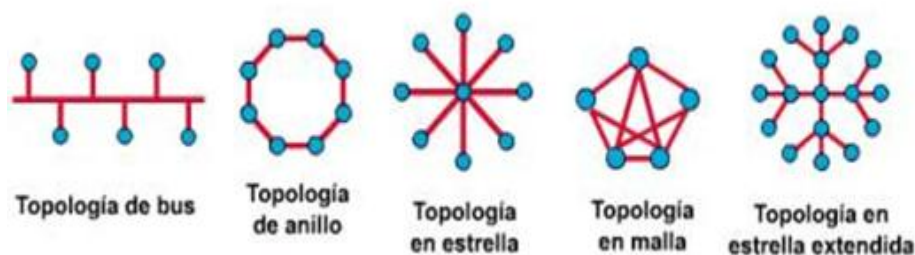


Figura N° 2.25. Diferentes Topologías físicas

Fuente: <http://culturacion.com/2009/10/topologias-de-red/>

- Mientras que la *topología lógica* define la forma en que los hosts acceden a los medios para enviar datos; los tipos más comunes son:

a) *Broadcast*, cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red.

b) *Transmisión de tokens*, se controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial.

- **Clasificación de redes según el medio de transmisión por el que se propaga la información**

a) **Red alámbrica:** Son redes que se comunican a través de cables de datos (como cables de red de Ethernet), permitiendo a los usuarios una buena seguridad y mayor tasa de transferencia de datos de manera rápida y efectiva.

Una red alámbrica ofrece la ventaja de transmitir grandes cantidades de información a altas velocidades, mediante tecnología Ethernet y medios Ethernet.

La *figura N° 2.26* muestra la estructura de red de un ISP, el cual consta de un servidor, varios dispositivos intermediarios, y usuarios finales; los cuales están distribuidos en diferentes partes del mundo.

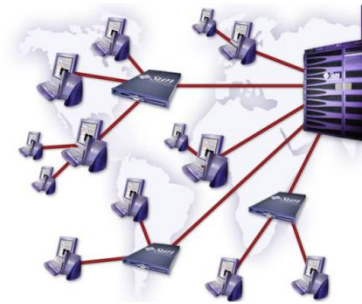


Figura N° 2.26. Red alámbrica

Fuente: <http://darmolano.blogspot.com/2008/07/red-alambrica-e-inalambrica.html>

b) Red inalámbrica: Las redes inalámbricas no utilizan un medio físico de conexión, su principal medio de transmisión son las ondas electromagnéticas que viajan a través del aire en forma de microondas, se utilizan antenas y satélites como elementos de interconexión; tienen un alcance global y local, son de uso privado.

Esta clase de redes tiene como objetivo proporcionar al usuario una gran movilidad sin perder conectividad, son de facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado.

Los principales estándares para la comunicación de datos que se aplican a los medios inalámbricos son:

- IEEE estándar 802.11 (Wi-Fi)
- IEEE estándar 802.16 (WiMAX).
- IEEE estándar 802.15.1 (Bluetooth).

La mayoría de redes que se utilizan en cualquier tipo de ambiente son del tipo híbrida, ya que permite combinar las características que ofrecen la tecnología inalámbrica y la seguridad que brindan los medios guiados.

La *figura N° 2.27* muestra un esquema de red híbrida.

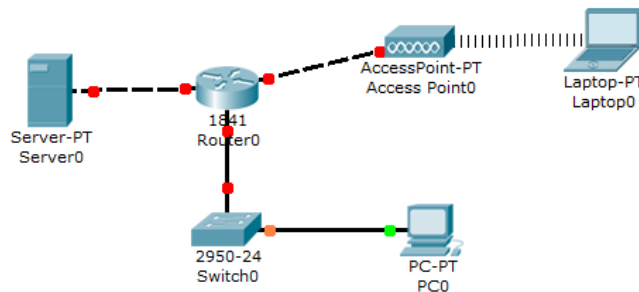


Figura N° 2.27. Red híbrida
Elaborado por: La investigadora

2.4.7 Estándar IEEE 802.11 (Wi-Fi)

De una fuente bibliográfica de *Internet (802.11: Wireless LANs, www.standards.ieee.org/about/get/802/802.11.html, 3, octubre, 2011; 11:10 h)* se obtienen definiciones del estándar Wi-Fi, como por ejemplo: “Estándar que define el protocolo y compatibilidad de interconexión de los equipos de comunicación de datos a través del “aire”, de radio o infrarrojo, en un área local (LAN)”.

a) Características

- En la banda de los 2.4 GHz presenta velocidades de 1 Mbps hasta 2 Mbps.
- Con Wi-Fi se pueden crear redes de área local inalámbricas de alta velocidad siempre y cuando el equipo que se vaya a conectar no esté muy alejado del punto de acceso.
- Para brindar seguridad utiliza protocolos de cifrado de datos como WEP, WPA, o WPA2; los cuales codifican la información a ser transmitida brindando cierta confidencialidad.

b) Componentes de la arquitectura

La norma 802.11 LAN está basada en una arquitectura celular, donde el sistema es subdividido en células, cada célula (BSS – Basic Service Set) es controlada por una estación base (AP- Access Point).

c) Comparación de estándares de la norma IEEE 802.11

La norma posee varios estándares desarrollados por diferentes grupos de trabajo, los cuales son identificados por la letra tras la última cifra. Existen 18 estándares (a, b, d, e, f, g, h, i, k, m, n, p, r, s, t, u, v, w) pero los estándares más relevantes son:

802.11a, con una frecuencia de 5 GHz, y una velocidad de 54 Mbps.

802.11b, con una frecuencia de 2.4 GHz, y una velocidad de 11 Mbps.

802.11g, con una frecuencia de 2.4 GHz, y una velocidad de 54 Mbps.

802.11n, con una frecuencia de 2.4 y 5.8 GHz, y una velocidad de hasta 600 Mbps.

En la *figura N° 2.28*, se muestra un cuadro comparativo de velocidades entre los estándares Wi-Fi más utilizados.

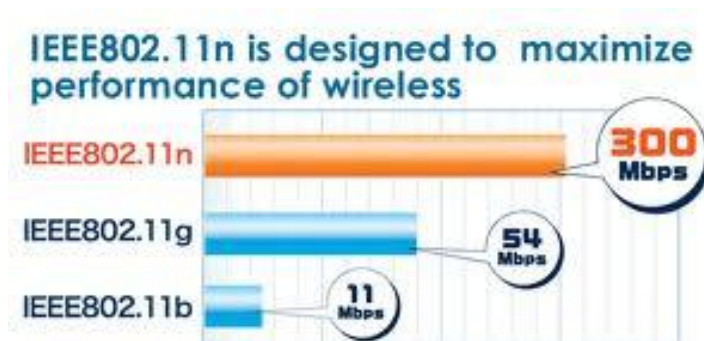


Figura N° 2.28. Comparación entre los diferentes estándares Wi-Fi

Fuente: <http://www.tecnotemas.com/2009/09/13/el-nuevo-estandar-wi-fi-802-11n-ya-es-oficial/>

d) Ventajas y desventajas

La principal ventaja que ofrecen las redes Wi-Fi es el brindar mayor comodidad a la de la red alámbrica, tanto en acceso a usuarios y cobertura desde distintos puntos dentro de un determinado rango de espacio.

En tanto que sus desventajas son: menores velocidades debido a pérdidas de señal e interferencias, y problemas de seguridad, en gran parte causado por el medio, los equipos y el área de cobertura de la red.

2.4.8 La seguridad en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial

Se puede conceptualizar a la seguridad como el conjunto de medidas tomadas para protegerse contra robos, ataques, crímenes y espionajes o sabotajes.

Es decir la seguridad es una necesidad básica de la persona y de los grupos humanos y al mismo tiempo un derecho inalienable del hombre y de las naciones.

En el edificio administrativo de la FISEI la seguridad se ha convertido en un problema constante, ya que afecta a las actividades laborales que allí se realizan, debido a que no se cuenta con personal especializado para asegurar una vigilancia adecuada, integral y eficiente.

Mediante el uso adecuado de las NTICs (Nuevas Tecnologías de Información y Comunicación) se puede contribuir al mejoramiento de la seguridad dentro y fuera de la institución.

Las siguientes gráficas muestran los edificios que componen la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

En la *figura N° 2.29* se presenta la parte delantera del edificio principal de la FISEI, mientras que en la *figura N° 2.30* se muestra el edificio secundario (nuevo edificio), visto desde atrás.



Figura N° 2.29. Edificio principal de la FISEI
Elaborado por: La Investigadora



Figura N° 2.30. Edificio secundario de la FISEI
Elaborado por: La Investigadora

2.4.8.1 Seguridad según el sector

- Seguridad pública

La seguridad pública es un servicio que debe brindar el Estado para garantizar la integridad física de los ciudadanos y sus bienes.

E implica que los ciudadanos pueden convivir en armonía, cada uno respetando los derechos individuales del otro.

- **Seguridad privada**

En casi todos los países hay empresas se encargan de ofrecer custodios, vigilantes y distintos dispositivos de protección para cualquier ciudadano que pueda pagarlos.

Las personas o empresas que se sienten en riesgo pueden acudir a la seguridad privada y contratar uno o más custodios permanentes.

2.4.8.2 Niveles de seguridad

- **Nivel Bajo**: Se puede definir como las consecuencias de que un incidente de seguridad causen un perjuicio limitado.

Una característica que se menciona de *Internet (Niveles de seguridad, <http://www.slideshare.net/eventoscreativos/esquema-nacional-de-seguridad-4812979>, 5, octubre, 2011; 9:30 h)* es que se denota la reducción de forma apreciable en la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.

- **Nivel Medio**: Se puede definir como las consecuencias de que un incidente de seguridad causen un perjuicio grave.

Donde el sufrimiento de un daño significativo por los activos de la organización, pueden causar un perjuicio significativo a algún individuo, de difícil reparación.

- **Nivel Alto**: Se puede definir como las consecuencias de que un incidente de seguridad provoquen un perjuicio muy grave.

De una fuente bibliográfica de *Internet (Niveles de seguridad, <http://www.slideshare.net/eventoscreativos/esquema-nacional-de-seguridad-4812979,5>, octubre, 2011; 9 h)* se hace referencia a este nivel de seguridad como: “La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.

Además del sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización, que pueden originar un perjuicio grave a algún individuo, de difícil o imposible reparación”.

La *figura N° 2.31*, muestra un diagrama sobre los Riesgos y necesidad de Reglamentos de seguridad, los cuales son necesarios en todo ámbito laboral, imponiendo controles para evitar amenazas y disminuir vulnerabilidades, al personal, equipamiento, información e infraestructura.



Figura N° 2.31. Diagrama de relación Riesgos-Reglamentos de seguridad
Fuente: <http://www.iso27000.es/sgsi.html>

2.4.8.3 Reglamentos de seguridad

Conjunto de normativas que conforman una guía de actuación por seguir o como un patrón de referencia relacionado a la seguridad.

Reglamentos de seguridad e higiene son implementados en toda institución de carácter educativo, social y de cualquier otra índole.

Para la coherencia de dichas normativas se deben tener en cuenta las siguientes reglas:

- Se debe delimitar con precisión todos los aspectos de seguridad que se deben cubrir y prever todas las contingencias.
- Los niveles de seguridad deben ser de acuerdo al entorno.
- La seguridad debe ser adecuada a la necesidad de protección de lo asegurado y a los recursos disponibles.

2.5 Hipótesis

El sistema de vigilancia incide en los niveles de seguridad en el edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

2.6 Señalamiento de variables

Variable Independiente: Sistema de vigilancia.

Variable Dependiente: Seguridad en el edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

CAPÍTULO III

METODOLOGÍA

3.1 Enfoque de la investigación

La investigación se fundamentó en el mejoramiento de los niveles de vigilancia del área administrativa de la FISEI, y tuvo un enfoque cuali-cuantitativo, debido a que se realizó un enfoque contextualizado de la situación de seguridad y vigilancia por la que atraviesa dicha área, buscando causas y explicaciones por medio de la toma directa de datos del campo de análisis, para llegar a la comprobación de la hipótesis planteada.

3.2 Modalidad básica de investigación

La investigación se basó en la modalidad de campo y bibliográfica-documental.

De campo porque se utilizaron métodos como la toma de datos en el bloque administrativo para determinar causas, y necesidades, con el fin de aplicar los conocimientos con fines prácticos.

Mientras que bibliográfica-documental para detectar, profundizar diferentes enfoques, teorías, conceptualizaciones, y criterios relacionados a sistemas de video vigilancia.

3.3 Tipos de investigación

La investigación se realizó a nivel *exploratorio* porque permitió efectuar un estudio del problema; a nivel *descriptivo* para reconocer las variables que intervinieron en el problema, y realizar pronósticos siempre y cuando se cuente con conocimiento suficiente de la situación; y a nivel *explicativo* para un análisis, síntesis e interpretación sobre video vigilancia.

La *asociación de variables* estuvo presente para evaluar las variables de comportamiento, y midiendo el grado de relación existente entre ellas.

3.4 Población y Muestra

Población

La población para el análisis del proyecto consta de:

Decano	1
Subdecano	1
Coordinadores de carrera	3
Secretarias	9
Personal de servicio	4
TOTAL	18

Muestra:

Debido al tamaño de la población se trabajó con su totalidad para obtener datos confiables.

3.5 Operacionalización de variables

Variable independiente: SISTEMA DE VIGILANCIA

CONCEPTO	DIMENSIÓN	INDICADORES	ÍTEMS	TÉCNICA/INSTRUMENTO
SISTEMA DE VIGILANCIA. Comprende una serie de procesos mediante el uso de la tecnología para captar información, para así orientar el futuro, y proteger el presente y el futuro de ataques de cualquier índole.	Tecnología	Permite la comunicación de datos.	¿Qué tipo de tecnología se utiliza para la vigilancia del área administrativa?	Observación
	Video vigilancia	Control de seguridad de un área. Utiliza tecnología IP.	¿El sistema de vigilancia actual satisface las necesidades de seguridad?	Encuesta
	Aplicaciones	Permite controlar remotamente. El sistema es flexible y escalable.	¿Cree necesario el desarrollo de un sistema de vigilancia para el control y monitoreo remoto?	Encuesta

*Tabla 3.1. Operacionalización de la variable independiente: Sistema de vigilancia
Elaborado por: La Investigadora*

Variable dependiente: SEGURIDAD EN EL EDIFICIO ADMINISTRATIVO DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CONCEPTO	DIMENSIÓN	INDICADORES	ÍTEMS	TÉCNICA/INSTRUMENTO
SEGURIDAD. Es el conjunto de medidas tomadas para protegerse contra robos, ataques, crímenes y espionajes o sabotajes	Medidas	Acciones de protección.	¿Cuenta la facultad con plan de seguridad para el recurso humano y de trabajo?	Encuesta
	Protegerse	Forma de evitar acciones.	¿Cree que es suficiente la protección física brindada por el personal de seguridad en el área administrativa?	Encuesta
	Ataques	Daño físico Pérdida de información Daños de equipos	¿Un sistema de video vigilancia permitirá brindar mayores seguridades para evitar todo tipo de ataques? ¿La FISEI aplica la normativa vigente en relación a parámetros de seguridad?	Encuesta

*Tabla 3.2. Operacionalización de la variable dependiente: Seguridad en el edificio administrativo de la FISEI
Elaborado por: La Investigadora*

3.6 Técnicas e Instrumentos de Investigación

Las técnicas empleadas para la investigación fueron *observación* para la evaluación de la situación real respecto a la seguridad en el área administrativa, detectando problemas para un análisis posterior y determinación de la solución. Y la *encuesta escrita* que permitió recolectar información mediante una serie de preguntas elaboradas para el personal que allí trabaja.

3.7 Recolección de la información

Preguntas Básicas	
¿Para qué?	Para alcanzar los objetivos de la investigación
¿De qué personas u objetos?	Personal que labora en el área administrativa de la FISEI.
¿Sobre qué aspectos?	Seguridad
¿Quién?	Investigadora: Gabriela Cifuentes
¿Cuándo?	Seis meses a partir de su aprobación
¿Dónde?	Edificio administrativo de la FISEI
¿Qué técnicas de recolección?	Observación y encuesta
¿En qué situación?	Seguridad de infraestructura

*Tabla 3.3. Plan de recolección de información
Elaborado por: La Investigadora*

3.8 Procesamiento de la información

La información se procesó mediante los siguientes pasos:

- Revisión crítica de la información recogida.
- Tabulación o cuadros según las variables de la hipótesis.
- Estudio estadístico de los datos para presentación de resultados.

3.9 Análisis e interpretación de resultados

Análisis integral de los resultados, se realizó en base al marco teórico, y técnicas de recolección de información, interpretación de los resultados por medio de cuadros estadísticos; estructuración de conclusiones y recomendaciones para brindar una solución al problema anteriormente planteado.

Y la estructuración de la propuesta que permitió mejorar los niveles de seguridad en el área administrativa de la FISEI.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

A continuación se presenta la encuesta realizada al personal que trabaja en el área administrativa de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato. También se presenta un análisis por cada pregunta realizada, con una gráfica de porcentajes para mayor entendimiento.

Las preguntas que se realizaron se enfocaron a los sistemas de seguridad existentes en el edificio, su funcionalidad, su eficiencia, y garantía. Además de los beneficios de la implementación de nuevas tecnologías para mejorar la seguridad dentro de la facultad.

También se presenta la Ficha de observación, en donde se analizan temas como tecnología, y el uso de esta por medio del personal administrativo.

4.1 Encuesta

Pregunta 1. ¿Cree usted qué el sistema de vigilancia actual del edificio administrativo es eficiente?

N°	Indicador	Frecuencia	Porcentaje
1	Sí	3	17%
2	No	15	83%
TOTAL		18	100%

Tabla 4.1. Tabulación Pregunta 1
Fuente: Personal del área administrativa
Elaborado por: La Investigadora

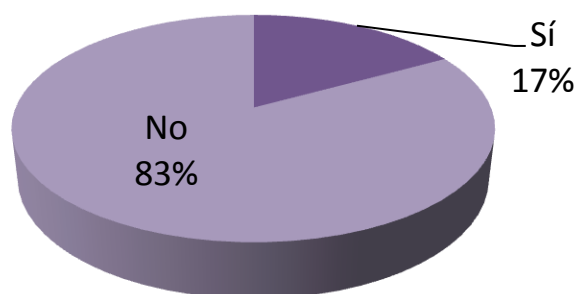


Figura N° 4.1. Pregunta 1
Elaborado por: La Investigadora

Análisis. Una vez realizadas las encuestas, la mayor parte, con un 83% de casos, de la muestra coincidió con que es necesario mejorar la seguridad de edificio en lo que concierne al sistema de vigilancia; mientras que el 17% considera que el sistema actual es suficiente para su realidad. Dichos datos demuestran que es generalizada la visión de que es necesaria una mejora en el sistema de vigilancia del área administrativa.

Pregunta 2. ¿Se han suscitado hechos delictivos o pérdida de información en el área administrativa?

N°	Indicador	Frecuencia	Porcentaje
1	Sí	18	100%
2	No	0	0%
TOTAL		18	100%

Tabla 4.2. Tabulación Pregunta 2
Fuente: Personal del área administrativa
Elaborado por: La Investigadora

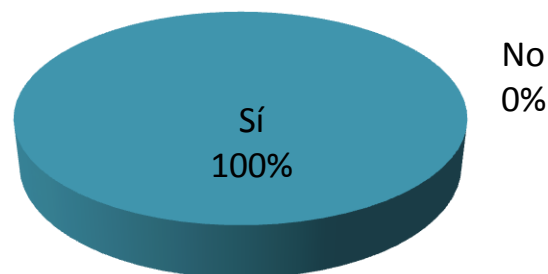


Figura N° 4.2. Pregunta 2
Elaborado por: La Investigadora

Análisis. La totalidad de personas encuestadas afirman que se han suscitado hechos delictivos como robos, daño a equipos e instalaciones del edificio administrativo. Constituyendo así un apoyo indispensable en la factibilidad de la propuesta realizada en el presente documento.

Pregunta 3. ¿Es necesario el diseño de un sistema de vigilancia electrónica para mejorar los niveles de seguridad?

N°	Indicador	Frecuencia	Porcentaje
1	Sí	13	72%
2	No	5	28%
TOTAL		18	100%

Tabla 4.3. Tabulación Pregunta 3
Fuente: Personal del área administrativa
Elaborado por: La Investigadora

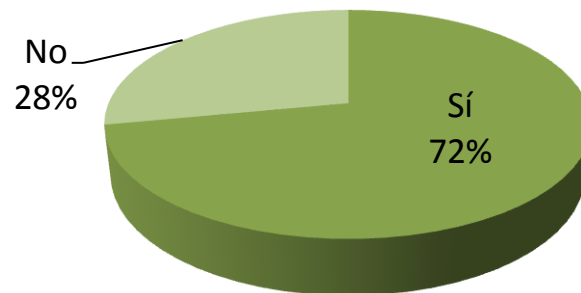


Figura N° 4.3. Pregunta 3
Elaborado por: La Investigadora

Análisis. Según el 72% de los encuestados es necesario el diseño de un sistema de vigilancia electrónico para mejorar los niveles de seguridad dentro del edificio administrativo, para así brindar un mejor servicio a las personas que visitan a dicha área por motivo de trabajo; por otro lado, el 28% piensa que no es necesario dicho sistema por diferentes motivos. Denotando que la perspectiva común es de que sí es necesario dicho sistema de vigilancia.

Pregunta 4. ¿Cree que existen las suficientes seguridades para el acceso al área de oficinas de autoridades y personal administrativo?

N°	Indicador	Frecuencia	Porcentaje
1	Sí	4	22%
2	No	14	78%
TOTAL		18	100%

Tabla 4.4. Tabulación Pregunta 4
Fuente: Personal del área administrativa
Elaborado por: La Investigadora

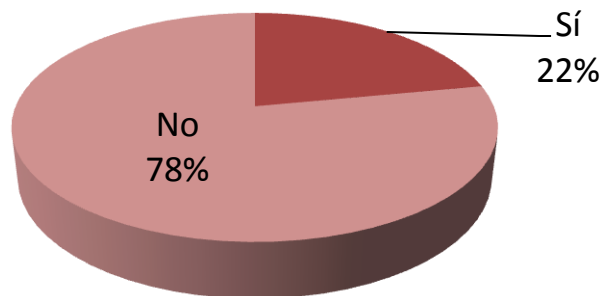


Figura N° 4.4. Pregunta 4
Elaborado por: La Investigadora

Análisis. La mayor parte de participantes (78%) cree que no se cuentan con las seguridades necesarias para el ingreso al edificio; mientras que el 22% de encuestados piensa que se cuentan con las seguridades necesarias para evitar actos delictivos dentro de oficinas, al personal y a la información que allí se resguarda. Estos datos revelan que es necesario un sistema de vigilancia y seguridad que les brinde al recurso humano principalmente una sensación de seguridad, lo cual ayudará al desarrollo de la propuesta planteada.

Pregunta 5. ¿Existen planes para evitar posibles contingencias al recurso humano y de trabajo?

N°	Indicador	Frecuencia	Porcentaje
1	Sí	4	22%
2	No	14	78%
TOTAL		18	100%

Tabla 4.5. Tabulación Pregunta 5
Fuente: Personal del área administrativa
Elaborado por: La Investigadora

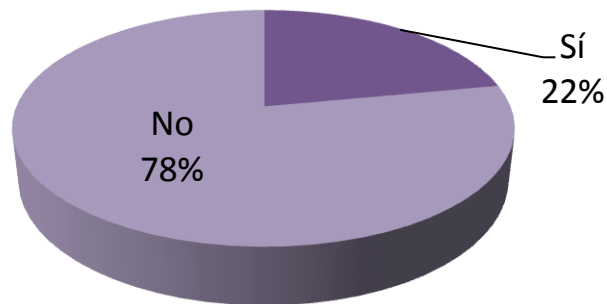


Figura N° 4.5. Pregunta 5
Elaborado por: La Investigadora

Análisis. Considerando el entorno en que los participantes se desenvuelven, el 22% conoce sobre los reglamentos básicos sobre seguridad dentro de las instalaciones del área administrativa, mientras que el porcentaje restante no está al tanto sobre cómo reaccionar ante ciertos riesgos a la seguridad.

Pregunta 6. ¿Qué beneficios se conseguirán con un sistema de video vigilancia inalámbrica?

N°	Indicador	Frecuencia	Porcentaje
1	Control de personas particulares al área	3	17%
2	Monitoreo remoto	1	5%
3	Disminución de la percepción de inseguridad por parte del recurso administrativo	7	39%
4	Escalabilidad del sistema	2	11%
5	Todas las anteriores	5	28%
TOTAL		18	100%

Tabla 4.6. Tabulación Pregunta 6
Fuente: Personal del área administrativa
Elaborado por: La Investigadora

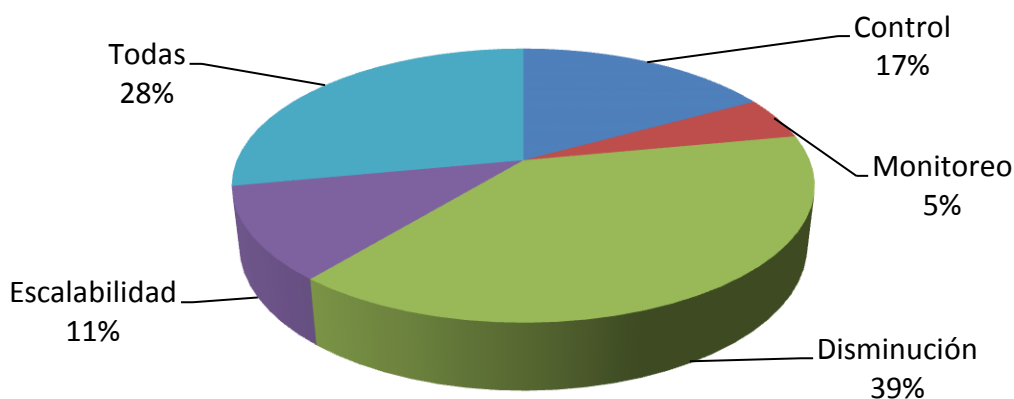


Figura N° 4.6. Pregunta 6
Elaborado por: La Investigadora

Análisis. La mayoría de entrevistados coincide que un sistema de video vigilancia inalámbrica disminuirá la percepción de inseguridad por parte del recurso administrativo, ya que el personal de vigilancia monitorizará las áreas de cobertura desde cualquier punto dentro de una red IP, el 28% de encuestados considera que dicho sistema inalámbrico brindará todas las características mencionadas; mejorando el desenvolvimiento de las actividades de la FISEI en la sociedad.

4.2 Ficha de Observación: Área Administrativa de la FISEI

Luego de la observación respectiva al área de Administración y la tecnología Informática que utilizan para el desarrollo de sus actividades, se ubicará la apreciación sobre el objeto observado, utilizando la siguiente escala de valoración.

1	2	N
Sí	No	No es posible observar

Observación	ESCALA		
	1	2	N
Sobre la tecnología			
¿El edificio administrativo de la FISEI cuenta con tecnología IP?	x		
¿La tecnología actualmente implementada permite la escalabilidad de nuevos sistemas?	x		
¿Se cuenta con personal que administre dicha tecnología adecuadamente?	x		

Tabla 4.7. *Ficha de observación*

Fuente: Área administrativa

Elaborado por: La Investigadora

Análisis (Ficha de observación). Se evidencia que en su totalidad los ítems de la ficha de observación sobre tecnología en el edificio son positivos, lo que permite no solo el diseño de un sistema de video vigilancia inalámbrico sino también escalabilidad de nuevos sistemas que permitan mejorar características de servicio, seguridad y vigilancia dentro de las instalaciones.

4.3 Preguntas discriminantes

Se han tomado en cuenta las preguntas discriminantes, como: *¿Cree usted que el sistema de vigilancia actual del edificio administrativo es eficiente?*, ya que existe un gran porcentaje de personas que trabajan dentro del área que mantienen la percepción de inseguridad latente dentro de su área de trabajo.

La pregunta *¿Se han suscitado hechos delictivos o pérdida de información en el área administrativa?*, dio como resultado un 100% que se han suscitado hechos

delictivos como pérdida de información, robo de equipos y daño a las instalaciones, debido a que el personal que se encarga de la vigilancia no es exclusivo para dicha área durante el horario de trabajo.

Finalmente la pregunta *¿Es necesario el diseño de un sistema de vigilancia electrónica para mejorar los niveles de seguridad?*, dio como resultado que si es necesario el diseño de un sistema de vigilancia que permita el monitoreo remoto, escalabilidad de equipos, grabación de sucesos mediante video cámaras IP, entre otros beneficios.

Estas preguntas al igual que sus resultados demuestran que la propuesta si es factible porque se desarrollará con tecnología actual, escalable y de buena convergencia.

4.4 Situación actual de seguridad y vigilancia en la FISEI

La situación actual con respecto al nivel de seguridad por la que atraviesa la facultad es deficiente en varios aspectos, debido a que cuenta con 2 tipos de seguridad en funcionamiento que brindan un nivel medio-bajo.

El edificio administrativo se encuentra resguardado por dos tipos de vigilancia, uno es la seguridad física brindada por el personal de vigilancia, el cual realiza rondas a determinadas horas durante todo el día; y el sistema de cerraduras metálicas ubicadas en las diferentes puertas de ingreso a las oficinas, y del edificio administrativo.

El segundo sistema de vigilancia con el que cuenta la facultad, es el sistema de vigilancia electrónica en el cual se encuentran:

a) Dos cerraduras eléctricas para accesos secundarios, estando ubicadas en:

- El segundo piso, para el acceso a las oficinas de Subdecanato, Coordinadores de Área y Secretarías.

En la oficina de Secretaría de Subdecanato se encuentra el interruptor para la activación de la cerradura eléctrica.

- En el tercer piso, para el acceso a las oficinas de Decanato, Secretaría y secretaría General.

En la oficina de Secretaría de Decanato se encuentra el interruptor para la activación de la cerradura eléctrica.

b) Sensores de movimiento gobernados a través de tableros de control.

- Existen 2 tableros de control, ubicados en el edificio principal en la oficina de Secretaría de Carrera, y en el edificio secundario de la facultad en la oficina de Dirección de Postgrado respectivamente.

- Mientras que el número de sensores de movimiento es 15, los cuales se encuentran distribuidos de la siguiente manera:

Dos en la oficina de Secretaría de Carrera.

Uno en la oficina de Asesoría Estudiantil.

Doce en los diferentes laboratorios de la facultad.

- Dos sirenas, ubicadas en la fachada exterior del edificio principal, y la fachada exterior del edificio secundario respectivamente.

Entre los sistemas que no se encuentran en funcionamiento debido al deterioro, falta de mantenimiento, o falta de recursos económicos para el funcionamiento de los componentes de los sistemas de vigilancia y seguridad, se encuentran:

- Sistema de una central telefónica marca Panasonic modelo KXT-616, en donde se encuentran funcionando dos líneas externas y 16 extensiones internas, dicha central tiene interconectada una electrocerradura, la cual está ubicada en la puerta de acceso principal al edificio administrativo.

La electrocerradura dejó de prestar sus servicios por falta de mantenimiento al sistema.

- Sistemas de alarmas domesticas ubicadas en oficinas, laboratorios y diferentes pisos que componen el edificio principal y secundario de la FISEI.

Los sistemas dejaron de prestar su servicio por falta de pago a la empresa que se encargaba del monitoreo y vigilancia.

Los dos sistemas descritos anteriormente se encuentran en estado pasivo, pero con un mantenimiento correctivo y pago de servicios de funcionamiento, podrían volver a estar en modo operativo y completamente funcional.

A continuación se presentan fotos de los componentes de cada sistema de vigilancia electrónica.

a) Sistema de alarmas domésticas.

La *figura N° 4.7* muestra el sensor de movimiento ubicado en la oficina de Administración de Redes.



Figura N° 4.7. Sensor de movimiento Administración de Redes
Elaborado por: La Investigadora

La *figura N° 4.8* muestra el sensor de movimiento ubicado en el Laboratorio N°1, ubicado en el segundo piso del edificio principal.



Figura N° 4.8. Sensor de movimiento LAB N° 1
Elaborado por: La Investigadora

La *figura N° 4.9* muestra el sensor de movimiento ubicado en la oficina de Secretaría de Carrera, ubicada en el primer piso del edificio principal.



Figura N° 4.9. Sensor de movimiento Secretaría de Carrera
Elaborado por: La Investigadora

La *figura N° 4.10* muestra una de las dos sirenas de alarma para el sistema de vigilancia electrónica.



Figura N° 4.10. Sirena ubicada en el edificio principal de la facultad
Elaborado por: La Investigadora

La *figura N° 4.11* muestra un tablero de control, el cual se encuentra ubicado en el primer piso del edificio principal.



Figura N° 4.11. Tablero de control
Elaborado por: La Investigadora

b) Sistema de la Central telefónica.

La *figura N° 4.12* y *figura N° 4.13* muestran a la Central telefónica, y su tablero, mientras que la última imagen muestra uno de los varios teléfonos que están conectados a la central.



Figura N° 4.12. Central telefónica
Elaborado por: La Investigadora



Figura N° 4.13. Teléfono interconectado a la Central telefónica
Elaborado por: La Investigadora

La *figura N° 4.14* y *figura N° 4.15*, muestran a la electrocerradura y al botón de activación respectivamente.



Figura N° 4.14. Electrocerradura de la puerta principal del área administrativa
Elaborado por: La Investigadora



Figura N° 4.15. Botón para desactivación de la electrocerradura
Elaborado por: La Investigadora

El sistema de seguridad de Porteros electrónicos se encuentran implementados dentro de las instalaciones que componen la FISEI, mientras que el sistema de vigilancia electrónico compuesto por sensores de movimiento, tableros y sirenas, se encuentran instalados en el edificio principal desde hace ocho años.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Un Sistema de vigilancia es un instrumento necesario en la actualidad para la administración efectiva de la seguridad, a través de: la monitorización, vigilancia y almacenamiento de videos digitalizados.
- El uso de la tecnología inalámbrica en sistemas de vigilancia abre la posibilidad de implementar sistemas con mejores características, y prestaciones, como el uso de mejores y nuevos equipos, mayor área de cobertura, mejor aprovechamiento del espacio físico, entre otros, los cuales pueden ser aplicados para mejorar la seguridad y vigilancia en la FISEI.
- El sistema de vigilancia actual del edificio administrativo de la FISEI se encuentra limitado en cuanto a personal y horarios.
- La falta de control para el acceso al edificio administrativo ha producido un incremento de problemas como la pérdida de información, acceso a oficinas, daños a las instalaciones, y vandalismo.

- El uso de tecnología IP en un sistema de video vigilancia presenta varias ventajas sobre el uso de tecnología analógica como: escalabilidad, y facilidad de conexión en tiempo real dentro de la cobertura de la red IP inalámbrica, este tipo de vigilancia mejorará la seguridad e imagen de esta institución educativa.

5.2 Recomendaciones

- La incorporación de un sistema de video vigilancia inalámbrico a los servicios que presta la infraestructura de red IP que posee la FISEI, permitirá mejorar la vigilancia, y monitorización en tiempo real del área administrativa.

- Se debe contar con un criterio para la selección de los diferentes componentes del sistema de vigilancia IP; entre los más significativos se pueden mencionar los siguientes: características de cada equipo, marcas, proveedores, precios, zonas de cobertura, y entornos de vigilancia.

- El sistema de Vigilancia IP debe contar con cámaras de red con sensores para la detección de movimiento, y detección de audio, debido a que mejoran las prestaciones del sistema de vigilancia. De similar manera se deben seleccionar formatos de compresión como M-JPEG, porque proporcionan calidad de visualización de imágenes, y mejoras en el rendimiento de todo el sistema.

- Para fortalecer el sistema de vigilancia IP inalámbrico es un requisito imprescindible el uso de una red dedicada para la transferencia de información de seguridad, además de equipos hardware con buena capacidad de almacenamiento.

- Con la implementación de un sistema de video vigilancia inalámbrico en la FISEI se mejorarán las características de infraestructura tecnológica, y los procesos de comunicación para la manipulación de información.

- El sistema que requiere la FISEI para administrar su seguridad, deberá ser diseñado para que su gestión, y funcionamiento sean centralizados, tomando en cuenta temas como la confidencialidad de información y manipulación del sistema por un personal preparado.

CAPÍTULO VI

PROPUESTA

6.1 Datos informativos

6.1.1 Título:

Sistema de video vigilancia inalámbrico para el mejoramiento de la seguridad del edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial (FISEI) de la Universidad Técnica de Ambato.

6.1.2 Institución ejecutora:

Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato

6.1.3 Tutor de tesis:

Ing. Giovanni Brito

6.1.4 Beneficiarios:

Personal que labora en el área administrativa de la FISEI

6.1.5 Ubicación:

Edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, ubicado entre la Av. de los Chasquis y Río Guayllabamba, sector Huachi.

6.1.6 Tiempo estipulado:

Seis meses.

6.1.7 Equipo técnico responsable:

Tutor de tesis

Investigadora

6.1.8 Costos:

13.630,67 dólares

6.2 Antecedentes de la propuesta

En la actualidad las instituciones de Educación Superior se han visto inmersas en cambios debido a la globalización, revolución tecnológica y científica, y la educación como factor indispensable para el desarrollo social.

La Facultad de Ingeniería en Sistemas, Electrónica e Industrial para la administración, manejo y control de las actividades propias de la institución, cuenta con información y equipamiento de uso solo para personal que allí trabaja.

Al no contar esta área con un sistema de vigilancia exclusivo, ya sea físico como: guardias de seguridad, electrónico como: control automático de ingreso, video vigilancia IP, entre otros; las tres plantas que componen el edificio no se encuentran debidamente protegidas por dispositivos tecnológicos o mecánicos que permitan brindar una seguridad adecuada; causando problemas como robo de equipos informáticos ubicados en las oficinas de autoridades, daño a las instalaciones, y mal uso de equipamiento por parte del personal y/o personas que visitan el edificio.

Con la implementación de un sistema de vigilancia con tecnología IP se reducirán costos, y se ampliarán los servicios brindados dentro de la infraestructura de la red IP de la FISEI.

6.3 Justificación

El uso de tecnología IP dentro de instituciones de cualquier índole ha mejorado la productividad, ya que permite que servicios como voz y datos converjan más rápido, estas características están relacionadas al ancho de banda, a la reducción de costos y facilidad de uso; lo cual ha permitido mayor flexibilidad y mejor gestión del sistema.

La FISEI actualmente cuenta con equipos tecnológicos que permiten el procesamiento, administración y gestión de la información, para el trabajo, educación e investigación. La infraestructura de la red IP con la que cuenta la facultad, consta de una red híbrida, para la conexión de dispositivos finales, como de dispositivos intermediarios, se utilizan una red cableada y una red inalámbrica; brindando así mayor cobertura a estudiantes, profesores, y empleados.

Para la gestión de la infraestructura tecnológica la facultad cuenta con personal especializado, que se encarga del control, funcionamiento, mejora y actualización de la misma; personal que ha brindado apoyo a la investigadora para mejorar las características de diseño del sistema de vigilancia IP.

La propuesta sobre el diseño de un sistema de video vigilancia inalámbrico mejorará lo concerniente a vigilancia, seguridad, además lo relacionado a comunicaciones, y mejoras en servicio, todo eso en tiempo real desde cualquier punto que se encuentre dentro de la red. El recurso económico es un factor importante que influye en las características del sistema y desenvolvimiento del mismo.

6.4 Objetivos

6.4.1 Objetivo general

Diseñar un sistema de video vigilancia inalámbrico para el mejoramiento de los niveles de seguridad en el edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

6.4.2 Objetivos específicos

- Determinar los requerimientos del sistema y los requerimientos del diseño de Video vigilancia para el edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
- Identificar cada uno de los componentes que intervienen en el sistema de Video vigilancia.
- Realizar un estudio y análisis para la distribución adecuada de los componentes del sistema.
- Demostrar la viabilidad económica y técnica del sistema de vigilancia en la FISEI.

6.5 Análisis de Factibilidad

Los aspectos a analizar son los siguientes:

6.5.1 Factibilidad Técnica

La vigilancia IP es un servicio que en la actualidad está tomando fuerza ya que permite vigilar las actividades en determinadas áreas, para observar lo que está sucediendo en tiempo real, tomar fotografías o videos; los cuales serán gestionados por un software.

El sistema de video vigilancia inalámbrica, es un sistema que opera con tecnología IP, y presenta el beneficio de varias fuentes bibliográficas que permitirán a la investigadora desarrollar una propuesta que garantice calidad, al tener las especificaciones técnicas, y económicas necesarias para su diseño.

6.5.2 Factibilidad Operativa

Al contar la facultad con una infraestructura tecnológica adecuada, la convergencia del servicio de vigilancia sobre IP es factible, ya que se cuenta con equipamiento que permite la escalabilidad del sistema de vigilancia inalámbrico; y con personal especializado que se encargará de la manipulación del sistema de vigilancia IP, por medio de la obtención de imágenes a través de las cámaras IP, las cuales transmitirán la información por la red de datos a una central de monitoreo. Además se realizará un ahorro de tiempo del personal a través de una gestión centralizada y del acceso remoto al sistema propuesto.

6.5.3 Factibilidad Económica

Para el análisis de factibilidad económica se tomará en cuenta que el presupuesto implica el costo económico de equipos necesarios para la implementación de sistema de Video vigilancia inalámbrico, el cual es rentable y justifica la inversión debido a que el sistema es un sistema de vigilancia y seguridad que cuenta con características de escalabilidad, convergencia, y que incorpora tecnología inalámbrica, además se tomó en cuenta varios imprevistos que podrían surgir durante su funcionamiento, demostrando así que es un sistema eficiente, flexible, y convergente.

6.6 Fundamentación

SISTEMA DE VIDEO VIGILANCIA INALÁMBRICO

6.6.1 Video Vigilancia IP Inalámbrico

Un sistema de vigilancia IP ofrece herramientas y mejoras en el ámbito de seguridad, permitiendo gestionar video y grabarlo desde cualquier lugar de la red IP cableada o inalámbrica, ya sea una red pública o privada.

- Componentes

Los componentes básicos de un sistema de video en red son:

- La cámara de red,
- El codificador/decodificador de video,
- El sistema de gestión y almacenamiento de video (software y hardware) y
- La red IP.

Detalle de los componentes:

6.6.1.1 Cámaras de red

Son cámaras, que poseen características de un ordenador para gestionar su funcionamiento dentro de una red IP.

Las características de una cámara IP son:

- Calidad de imagen
- Resolución
- Compresión
- Audio
- Funcionalidades de red.

Entre las clases de cámaras de red se encuentran las siguientes:

a) **Cámaras fijas:** Una cámara fija es aquella cuyo ángulo de visión se fija una vez que se monta. La *figura N° 6.1* muestra una cámara fija de marca AXIS, muy utilizada en áreas que requieren un punto fijo de seguridad.



Figura N° 6.1. Cámara Fija

Fuente: AXIS COMMUNICATIONS, IP-Surveillance design guide (2008, pág. 11)

b) **Cámaras de red domo fijas:** o mini-domos, consisten en una cámara fija que está pre-instalada en una pequeña carcasa domo; permitiendo la visión en cualquier dirección.



Figura N° 6.2. Cámara Domo Fija

Fuente: http://www.axis.com/es/products/video/camera/fixed_domes/index.htm

c) **Cámaras PTZ (Pan-Tilt-Zoom)**

Una cámara de red PTZ ofrece funciones de video en red combinadas con funciones de movimiento horizontal, vertical y zoom. Donde el movimiento es controlado por un ordenador conectado a la red.

En la *figura N° 6.3*, se visualiza una cámara PTZ marca AXIS, las cuales permiten gran ángulo de cobertura, además características de zoom digital.



Figura N° 6.3. Cámara PTZ

Fuente: AXIS COMMUNICATIONS, *IP-Surveillance design guide* (2008, pág. 11)

6.6.1.2 Codificadores de video

Integra un sistema de vigilancia analógico CCTV a un sistema de video en red, evitando descartar los equipos analógicos como cámaras analógicas y el cableado coaxial.

Son una opción que permite reutilizar instalaciones con tecnología analógica.

A continuación se muestra un codificador de video (*figura N° 6.4*) marca AXIS, señalando sus partes, conectores para audio, interfaces, alimentación e indicadores para mostrar su estado de funcionamiento.



Figura N° 6.4. Codificador de video

Fuente: AXIS COMMUNICATIONS, *Guía de productos* (2011, pág. 19)

6.6.1.3 Sistemas de gestión de video

Los sistemas de gestión de video tienen como tarea: la visualización, grabación, reproducción y almacenamiento del video.

Para eso los sistemas de video vigilancia usan software de grabación y monitorización profesional, lo que convierte al servidor de PC's de una red en un grabador de vídeo en red (NVR, Network Video Recorder).

a) Plataformas de hardware

Existen dos tipos para un sistema de gestión de video en red:

- Plataforma de servidor de PC
- Plataforma NVR

Una plataforma de servidor de PC está formada por uno o más PC, que ejecutan un programa de software de gestión de video; mientras que una plataforma basada en una grabadora de video en red (NVR) que es un hardware patentado con software de gestión de video preinstalado.



Figura N° 6.5. Servidor HP ProLiant ML350 G6

Fuente: Guía de Configuración Servidores ProLiant y StorageWorks para América Latina (2009, pág. 10)

b) Plataformas de software

El software permite al operador visualizar lo que está sucediendo, además opciones para almacenar y gestionar el video con un NVR.

Esta plataforma se debe instalar en los PC's para la monitorización, almacenamiento, visualización y gestión de video; para brindar mayor funcionalidad al sistema de video IP. El software puede ser una aplicación para un único PC o una aplicación más avanzada basada en cliente/servidor que proporcione soporte a usuarios múltiples.

La *figura N° 6.6*, muestra el software de gestión usado en las cámaras de red inalámbricas marca D-Link.

D-ViewCam
Software para la gestión y monitorización de hasta
32 cámaras D-Link



Figura N° 6.6. Software de Gestión de cámaras IP D-Link

Fuente: www.videovigilanciadlink.es/?p=d-viewcam-software-gestion-camaras-videovigilancia

Se pueden utilizar plataformas de software diferentes para gestionar video:

- Funcionalidad incorporada
- Software basado en cliente de Windows
- Software basado en Web

6.6.1.4 Resolución

La resolución de video define la calidad y claridad que se puede obtener en una imagen.

Para video analógico, se utilizan los estándares:

- **NTS** (Comité Nacional de Sistema de televisión)
- **PAL** (Línea de Alternancia de Fase)

Para el análisis de un sistema de vigilancia IP, es importante que los codificadores de video proporcionen este tipo de resoluciones al digitalizar las señales que provienen de las cámaras analógicas.

Para video digital, se aplican las siguientes resoluciones:

- **VGA** (Tabla de Gráficos de Video), es la resolución más adecuada para cámaras de red, ya que el video basado en VGA produce pixeles cuadrados que coinciden con los de las pantallas de ordenador.

- **HDTV** (Resolución de televisión de alta definición), es un estándar internacional que proporciona una resolución hasta cinco veces más alta que la televisión analógica estándar, esto significa imágenes más nítidas, y mejor fidelidad de color.

El tamaño del frame está definido por número de de píxeles horizontales por el número de píxeles verticales, por ejemplo: 1920x1080.

6.6.1.5 Técnicas de compresión

Los formatos de compresión mejoran la calidad de la imagen al momento de la grabación, reduciendo los requerimientos de ancho de banda y almacenamiento.

Como se mencionan en *AXIS-PROXIM-Vigilancia IP inalámbrica para aplicaciones de seguridad (2009, pág. 19)* las compresión dependerá de varios factores, “La técnica de compresión más adecuada depende de los límites que quiera poner el usuario en lo relacionado con calidad de imagen y consumo de ancho de banda”. Para así ahorrar espacio en el disco duro y para hacer más rápidas las transmisiones de información.

Para realizar el proceso de compresión de video se aplica un algoritmo al video original para crear un archivo comprimido, el cual será transmitido o almacenado; mientras que para la reproducción del archivo comprimido se aplica el algoritmo inverso, el cual incluirá el mismo contenido que el video original.

El *manual técnico de AXIS-Guía técnica de vídeo IP (2009, pág. 56)* menciona que “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.”

Los algoritmos que funcionan conjuntamente para la compresión/descompresión se denominan códec de video (codificador/decodificador), cabe mencionar que los códec de diferentes estándares no son compatibles entre sí.

Los formatos más utilizados por sus características son:

a) Formato MJPEG (Motion-JPEG es una versión extendida del algoritmo JPEG)

Motion JPEG es una técnica de compresión/descompresión para el video en la red, es una secuencia de video digital compuesta por una serie de imágenes JPEG individuales. (JPEG, Grupo de Expertos Fotográficos Unidos).

Entre sus principales características están:

- Cada imagen de una secuencia de video puede conservar la misma calidad garantizada que se determina mediante el nivel de compresión elegido para la cámara IP ó codificador de video.
- Cuanto más alto es el nivel de compresión, menor es el tamaño del archivo y la calidad de imagen.
- Al no haber dependencia alguna entre los fotogramas de M-JPEG, un video M-JPEG es resistente, lo que significa que si falla un fotograma durante la transmisión, el resto del video no se verá afectado.
- Uso de ancho de banda elevado a velocidades por encima de 10 fps.

b) Formato MPEG-4 Parte 2 (Grupo de Expertos en Imágenes en movimiento)

Es un estándar internacional, para la codificación de audio y video, orientado a medios de almacenamiento digital.

Sus características son las siguientes:

- Ofrece vídeo de alto rendimiento con buena resolución y demandas moderadas de ancho de banda de transmisión.
- Requiere una licencia
- Del Glosario técnico denominado *Vídeo en red*, presentado por *AXIS COMMUNICATIONS* (www.axis.com/es/corporate/corp/glossary_video.htm; 12, diciembre, 2011; 17:00 h) se menciona que: “Los usos principales del estándar MPEG-4 son la Web (transmisión multimedia) y la distribución de CD, para usos de conversación (videoteléfono) y las retransmisiones televisivas”.
- 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.
- Mayores tasas de compresión (superior a 10 fps).

c) Formato H.264

El H.264, puede reducir el tamaño de un archivo de video digital en más de un 80% si se compara con el formato M-JPEG, y hasta un 50% más en comparación con el estándar MPEG-4; requiriendo menor ancho de banda y espacio de almacenamiento para los archivos de video.

En el White paper de *AXIS-H.264 video compression standard (2008, pág. 6)*. “Este formato utiliza el método *codificación de diferencia*, el cual reduce los datos del video mediante la eliminación de información innecesaria.”

Es un buen protocolo de Streaming (diseñado para visualización en tiempo real), ya que puede sincronizar audio y video. Además posee tasas de compresión superiores a 10 fps.

H.264 y MPEG-42 proporcionan soporte para audio sincronizado, mientras que M-JPEG no lo hace.

6.6.1.6 Soporte de Audio

En un sistema de vigilancia IP, una cámara de red con soporte de audio procesa el audio, y envía tanto el audio como el video a través del mismo cable de red para supervisarlos o grabarlos; eliminando la necesidad de un cable adicional y facilita la sincronización de audio y video.

En la *figura N° 6.7* se indica cómo se envía la información a través de un medio a un dispositivo final dentro de la red IP.

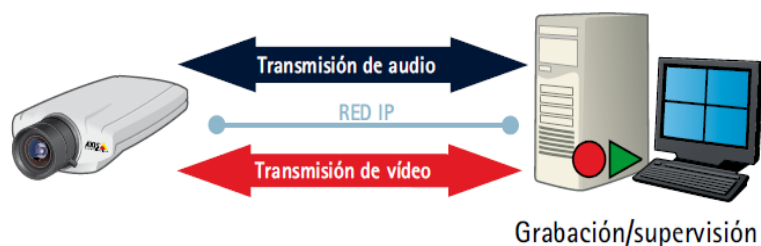


Figura N° 6.7. Soporte de audio y video

Fuente: AXIS COMMUNICATIONS, Guía técnica de video IP (2009, pág. 64)

- Modos de audio

- a) **Simplex:** el audio se envía de la cámara al operador y viceversa. Las aplicaciones incluyen supervisión a distancia y video vigilancia.
- b) **Semidúplex:** el audio se envía en ambas direcciones, pero sólo puede enviar una de las partes cada vez.
- c) **Dúplex completo:** el audio se envía a y desde el operador simultáneamente.

6.6.2 Sistemas Inalámbricos

6.6.2.1 Topologías de un sistema inalámbrico

Las topologías que presentan estos sistemas son: sistemas punto a punto y los sistemas punto a multipunto.

a) Sistemas Inalámbricos Punto a multipunto

Sistemas compuestos por múltiples bridges inalámbricos, denominados Unidades de Suscriptor (SU, Subscriber Units), que se comunican con una unidad de Estación Base (BSU, Base Subscriber Unit) inalámbrica.

Las capacidades de transmisión varían desde los 11 a los 60 Mbps y una cobertura de 5 a 20 Kilómetros.

La *figura N° 6.8* presenta la estructura de una red con topología Punto-Multipunto, muy utilizada para la transmisión de señales inalámbricas, como por ejemplo Sistemas de video vigilancia IP inalámbrica.

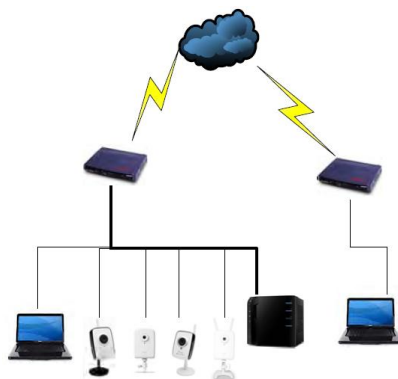


Figura N° 6.8. Topología Punto - Multipunto
Fuente: D-Link, D-ViewCam (2010, pág. 5)

b) Bridges Ethernet Inalámbricos Punto a Punto

Los bridges punto a punto conectan solo dos localizaciones. Su principal ventaja es que ofrecen mayor cobertura física que los sistemas punto a multipunto, mientras que su capacidad de transmisión va de los 11 a los 430 Mbps.

6.6.2.2 Seguridades de para un sistema inalámbrico:

Para brindar seguridad dentro del sistema existen varias medidas, entre ellas se pueden mencionar:

- **Protección por contraseña:** Protección para el monitor y el otro para proporcionar y monitorizar/modificar los privilegios.
- **Protección de la transmisión/criptación:** Transmisión de señales únicas que precisan el mismo equipamiento en ambos lados para la decodificación.

6.6.2.3 Estándar IEEE 802.11 (Wi-Fi)

El estándar Wi-Fi puede conceptualizarse como un “Estándar que define el protocolo y compatibilidad de interconexión de los equipos de comunicación de datos a través del aire, de radio o infrarrojo, en un área local (LAN)”. Una de sus ventajas es que no requiere licencia para la configuración, y funcionamiento de la red.

a) **Componentes de la arquitectura**

La norma 802.11 LAN está basada en una arquitectura celular, donde el sistema es subdividido en células, cada célula (BSS – Subsistema de Estaciones Base) es controlada por una *estación base* (AP- Punto de Acceso).

Las estaciones **BSS** se reconocen mediante un único SSID (Service Set Identifier), es decir necesitan un punto de acceso (**AP**) para unirse a la red.

Un punto de acceso (**AP**) es un dispositivo que interconecta varios dispositivos de comunicación inalámbrica para formar una red inalámbrica; también puede ser interconectado a una red cableada; se encarga de transmitir información entre los dispositivos conectados a la red.

La *figura N° 6.9* muestra la arquitectura general de los sistemas que utilizan medios no guiados para la transmisión de información.

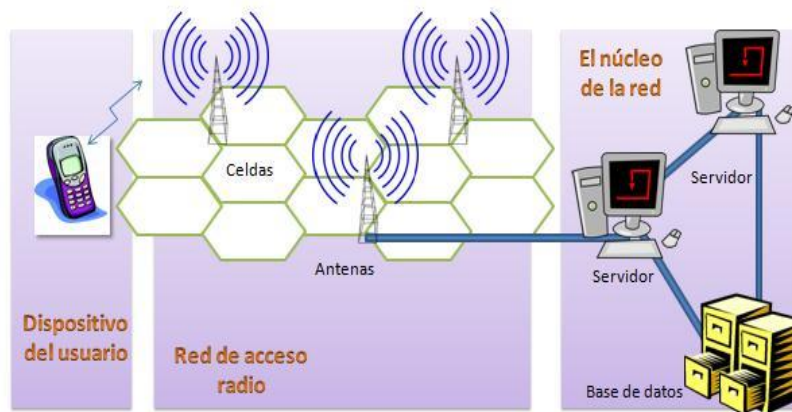


Figura N° 6.9. Arquitectura de un Sistema inalámbrico

Fuente: <http://posttecnoblogspot.com/2010/11/arquitectura-del-sistema.html>

b) Extensiones más relevantes de la norma IEEE 802.11

Estos estándares son los más importantes en cuanto a uso, compatibilidad, y cobertura física.

Las características más importantes de los diferentes estándares de la familia IEEE 802.11, se detallan a continuación:

- 802.11a

Opera en la frecuencia de 5 GHz y ofrece velocidades de hasta 54 Mbps, con una cobertura indoor de 7.62m a 22.86m.

Una desventaja es que la cobertura de la señal es inferior a la de 802.11g, ya que funciona en una frecuencia superior; requiriendo más puntos de acceso para la transmisión en la banda de 5 GHz que en la de 2.4 GHz.

- 802.11b

Funciona a 2.4 GHz y proporciona velocidades de hasta 11 Mbps, con una cobertura indoor de 30.48m a 60.96m.

- **802.11g**

Funciona a 2.4 GHz y proporciona velocidades de hasta 54 Mbps, y ofreciendo una cobertura indoor de 30.48m a 60.96m.

En general, los productos WLAN son compatibles con 802.11b/g.

- **802.11n**

Ofrece velocidades de hasta 600 Mbps, y puede trabajar en dos bandas de frecuencias: 2.4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a), permitiendo la compatibilidad con dispositivos basados en todas las ediciones anteriores de Wi-Fi.

c) **Seguridad**

- **WEP (Wired Equivalent Privacy)**

Evita que intrusos accedan a la red sin la clave correcta.

No obstante, tiene puntos débiles, como claves relativamente cortas y otros defectos que permiten que las claves se reconstruyan a partir de una cantidad relativamente pequeña de tráfico interceptado.

- **WPA/WPA2 (Wi-Fi Protected Access)**

Es un cifrado que aumenta significativamente la seguridad, ya que trata las deficiencias del estándar WEP.

En *Internet* (<http://wifiw.com/1306/seguridad-en-redes-wireless-y-diferencias-entre-cifrado-wep-y-wpawpa2.html>; 8, diciembre, 2011; 21:00 h) se hace referencia a que “WPA emplea el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP.”

6.7 Metodología

La metodología a utilizar para el desarrollo de la propuesta es la siguiente:

- Determinar la ubicación de las cámaras IP para que brinden una cobertura eficiente.
- Analizar y dimensionar los equipos necesarios para el sistema.
- Realizar el diseño físico y lógico para la red IP de vigilancia.
- Seleccionar los equipos en base a los requerimientos de seguridad y vigilancia.
- Realizar el presupuesto de la propuesta.
- Señalar las conclusiones y recomendaciones del diseño del Sistema de Video vigilancia Inalámbrico.

6.8 Diseño técnico del sistema

El sistema de video vigilancia IP para el edificio administrativo de la FISEI será diseñado en base a los requerimientos y parámetros de seguridad los cuales serán detallados a continuación.

6.8.1 Introducción

Para el diseño del sistema de vigilancia, parámetros técnicos como: ancho de banda, formatos de compresión, capacidad de almacenamiento de sistema de gestión, accesibilidad remota, entre otras serán tomadas en cuenta para el desenvolvimiento adecuado del sistema.

Se planteo la disposición de las cámaras IP que se utilizaron para cubrir áreas que requieren vigilancia y control del personal, personas que visitan las instalaciones y sucesos indeseados.

Adicionalmente factores como rendimiento, escalabilidad y funcionalidad serán proyectados a futuro para aprovechar las características de sistemas que manejan tecnología IP.

Para el adecuado diseño del sistema de Video vigilancia inalámbrico se tomará en cuenta el diseño físico, y el lógico; determinando el número de equipos y sus direcciones lógicas.

Los pasos que se seguirán para el diseño del sistema de Video vigilancia Inalámbrica son los siguientes:

- Paso 1: Definición del escenario y el tipo de productos de vídeo en red que se necesita.
- Paso 2: Determinación de las necesidades de aplicación: características, grabación y almacenamiento.
- Paso 3: Necesidades de en cuanto a la red (WLAN).

6.8.2 Diseño físico

a) Determinación y descripción de las áreas de vulnerabilidad con el control por medio de cámaras de video.

- *Puertas de ingreso al edificio.* Es una de las zonas más vulnerables ya que constituyen el ingreso y salida del personal y de todos quienes visitan el área administrativa.
- *Oficinas de las autoridades y demás personal.* Son sectores en donde el acceso es restringido, ya que manejan equipamiento de alto valor, y documentación reservada.

- *Escaleras.* Son sectores donde todo el personal transita y puede acontecer algún tipo de percance.

6.8.2.1 Topología física

La topología física utilizada para el sistema es de estrella extendida, en la cual cada cámara de red según su ubicación se conecta a un determinado radio de comunicación inalámbrica, y estos radios a su vez se conectan a un Switch Ethernet.

Con el uso de esta topología los equipos se encuentran directamente conectados, facilitando la administración y gestión de los mismos, además existe facilidad de instalación e implementación, y la posibilidad de desconexión de cualquier dispositivo final (cámara IP) sin que esto afecte el desempeño de la red.

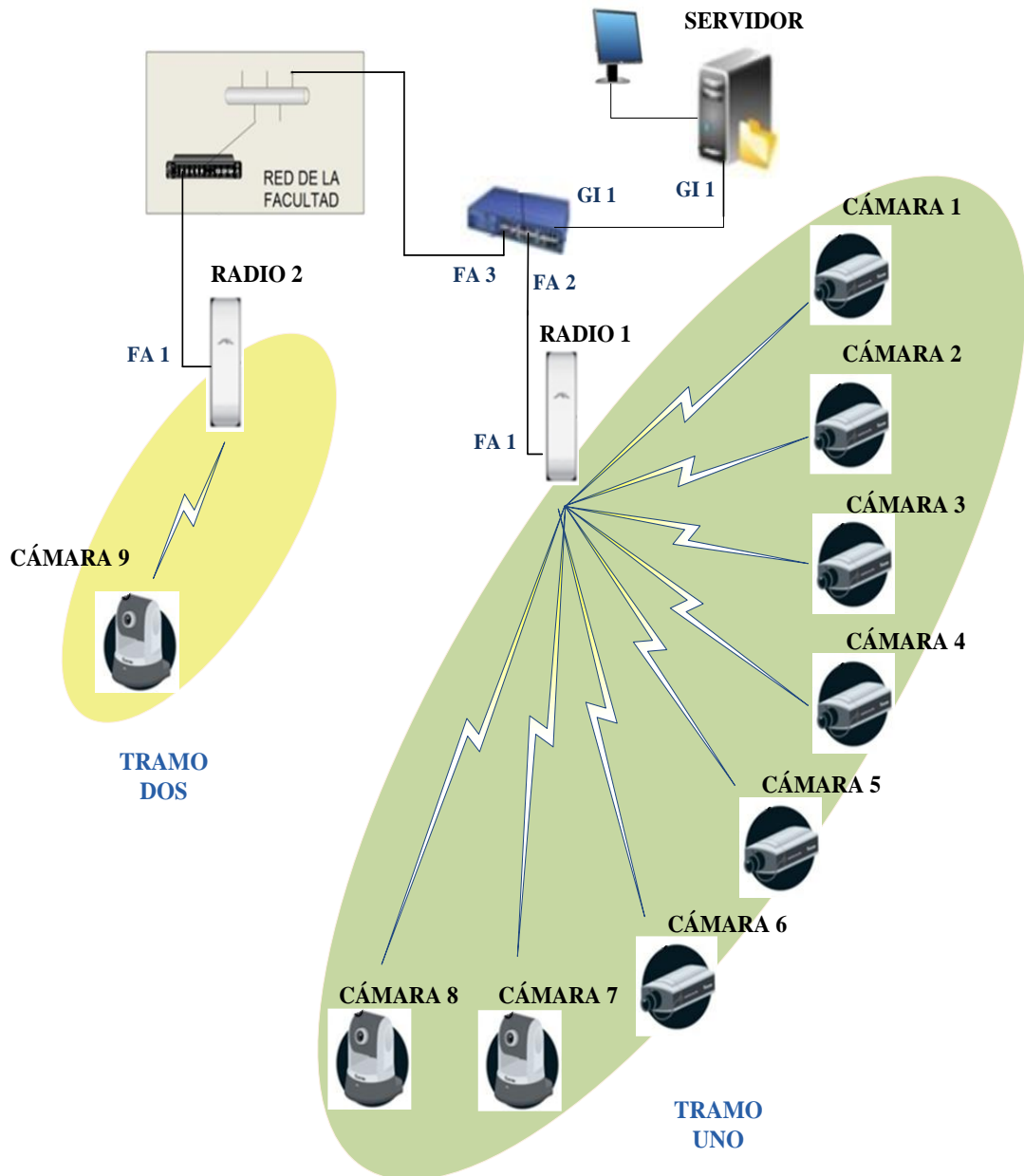
Para la conexión de las cámaras IP con sus respectivos radios de comunicación, se utilizó una red inalámbrica; consecuentemente se usó el aire como medio de transmisión, obteniendo ventajas como:

- a) Movilidad, para poder conectarse desde cualquier punto dentro del área de cobertura de la red.
- b) Capacidad de ampliación, se puede ampliar fácilmente la red con el equipo existente.
- c) Seguridad, gracias a los diferentes métodos de seguridad y encriptación.
- d) Menor costo económico, debido a que no se debe realizar la adquisición de medios de transmisión.
- e) Y mejor acceso a la información, ya que se puede conectar el dispositivo final en áreas de difícil acceso.

Mientras que para la conexión de los radios de comunicación inalámbrica, y del servidor de almacenamiento al switch Ethernet, se utilizó una red alámbrica, con un medio de transmisión guiado tipo Ethernet 100BASE-TX (UTP CAT 5E).

Formando así una red híbrida, la cual conforma el sistema de video vigilancia.

El esquema físico del sistema de Vigilancia IP inalámbrico se detalla a continuación:



*Figura N° 6.10. Diagrama físico de la red
Elaborado por: La Investigadora*

En donde se utiliza la siguiente simbología:

SIMBOLOGÍA		DESCRIPCIÓN
CÁMARA DE RED FIJA		Cámara IP fija inalámbrica día/noche
CÁMARA DE RED PTZ		Cámara IP PTZ inalámbrica de gran resolución
RADIO INALÁMBRICO		Radio para la comunicación inalámbrica
SERVIDOR DE ALMACENAMIENTO		Servidor para la gestión centralizada de la información
PERIFÉRICO DE VIZUALIZACIÓN (PANTALLA)		Monitor de video
SWITCH ETHERNET		Switch para la conmutación de información
CABLEADO ESTRUCTURADO DE LA FISEI		Cableado estructurado de la facultad, el cual comunicará el radio de comunicación inalámbrica con la red LAN de vigilancia
ENLACE INALÁMBRICO		Medio no guiado de conexión
CONEXIÓN ALÁMBRICA (UTP CAT 5E)		Medio guiado de conexión UTP CAT 5E

Figura N° 6.11. Simbología del diagrama físico de red
Elaborado por: La Investigadora

b) Parámetros para la ubicación de los componentes del sistema

Para la ubicación de cada cámara IP se tomó en cuenta los siguientes parámetros:

- Objetivo de vigilancia: visión general del área para poder realizar un seguimiento del movimiento de personas u objetos
- Luz: para la ubicación de cada cámara se tomo en cuenta la cantidad de iluminación, siendo situadas en sectores con buena iluminación o cercanas a iluminarias para captar buenas imágenes.
- Alcance dinámico de la escena: para que no afecte el alcance dinámico cada cámara será colocada a cierta altura que no afecte el ángulo de visión requerido.

Cálculos para seleccionar la ubicación óptima de las cámaras de red

- Para seleccionar la ubicación de cada cámara se realizará una simulación en el programa *IP Video System Design Tool*.

IP Video System Design Tool, es un software que ayuda al diseño de **sistemas de vídeo modernos de vigilancia** de forma rápida y fácil. El programa cuenta con las siguientes herramientas de diseño:

- Aumentar la eficiencia del sistema de seguridad encontrando las mejores ubicaciones para la cámara.
- Calcular **longitud focal precisa del lente** de la cámara y ángulos de visión.
- Comprobar el campo de visión de cada cámara y encontrar zonas muertas para aumentar el nivel de seguridad de las instalaciones utilizando 2D y modelado en 3D.

Para el cálculo del campo de visión requerido (altura y ancho), se deben ingresar los siguientes valores: distancia a la cual se encuentra el objeto a ser visualizado por la cámara, y la altura de la cámara; como resultado también se obtienen los ángulos de visión (horizontal y vertical) necesarios para dicho campo de visión.

La siguiente figura (*figura N° 6.12.*) detalla los aspectos del campo visual:

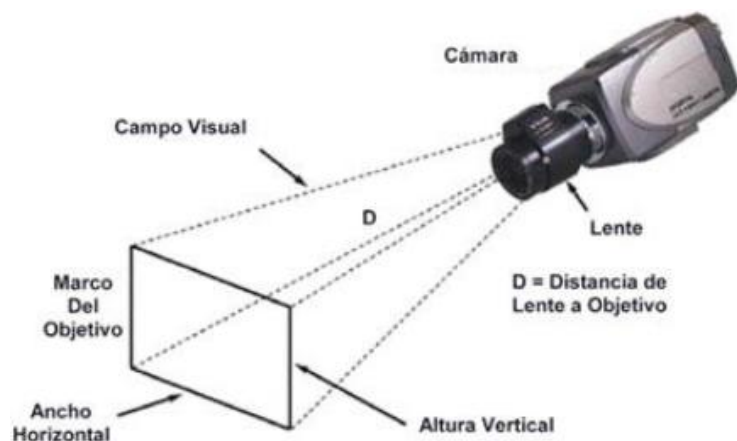


Figura N° 6.12. Campo visual de una cámara de red
Fuente: <http://www.redatel.net/html/DocumentosCCTV.html>

Los resultados gráficos para cada cámara son los siguientes:

- Cámara 1: cámara ubicada en la oficina de Secretaria de carrera.

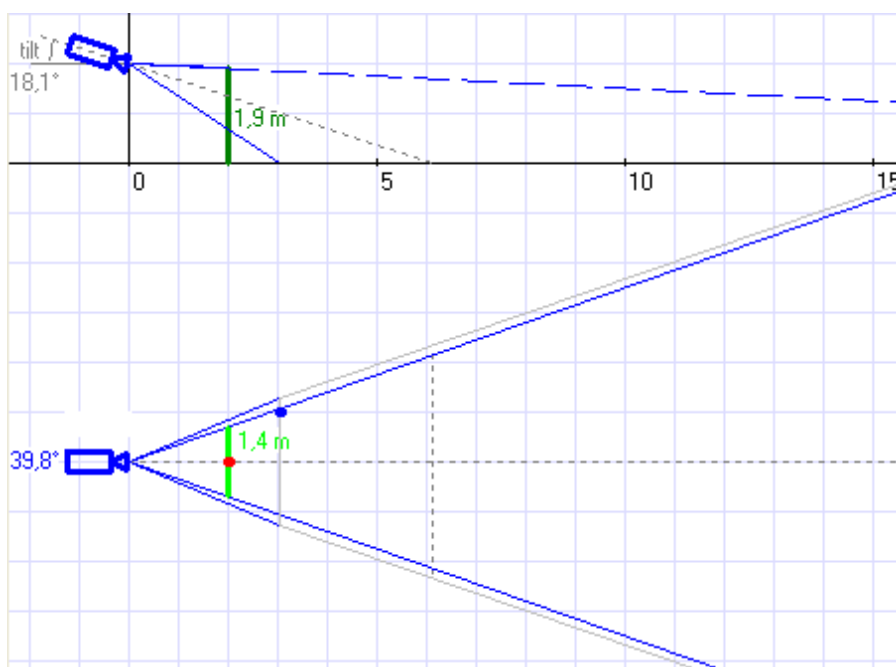


Figura N° 6.13. Campo visual de la cámara 1
Elaborado por: La Investigadora

- Cámara 2: ubicada en la entrada al ágora del edificio principal.

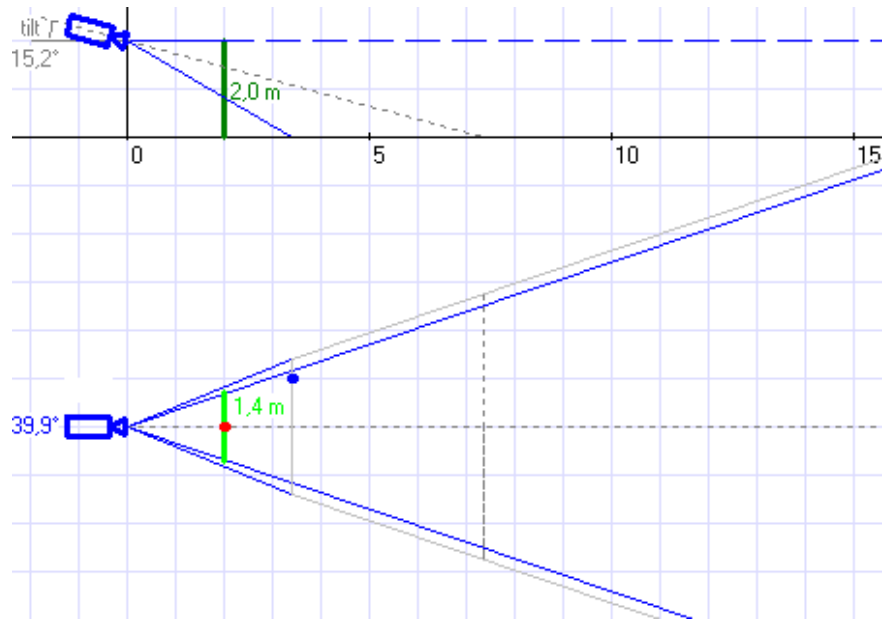


Figura N° 6.14. Campo visual de la cámara 2
Elaborado por: La Investigadora

- Cámara 3: ubicada en las escaleras del primer piso del edificio administrativo.

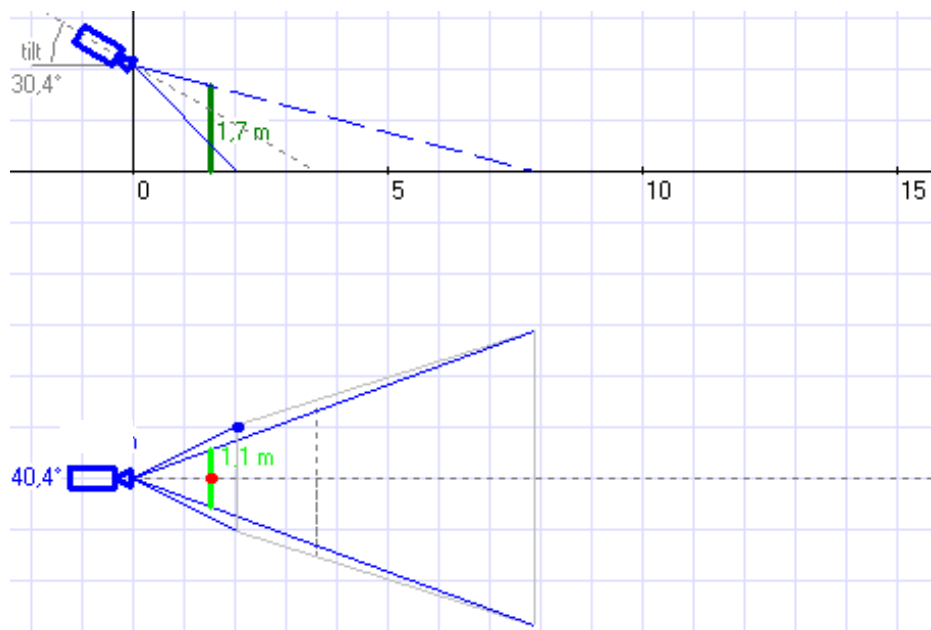


Figura N° 6.15. Campo visual la cámara 3
Elaborado por: La Investigadora

- Cámara 4: ubicada en Secretaría de Subdecanato.

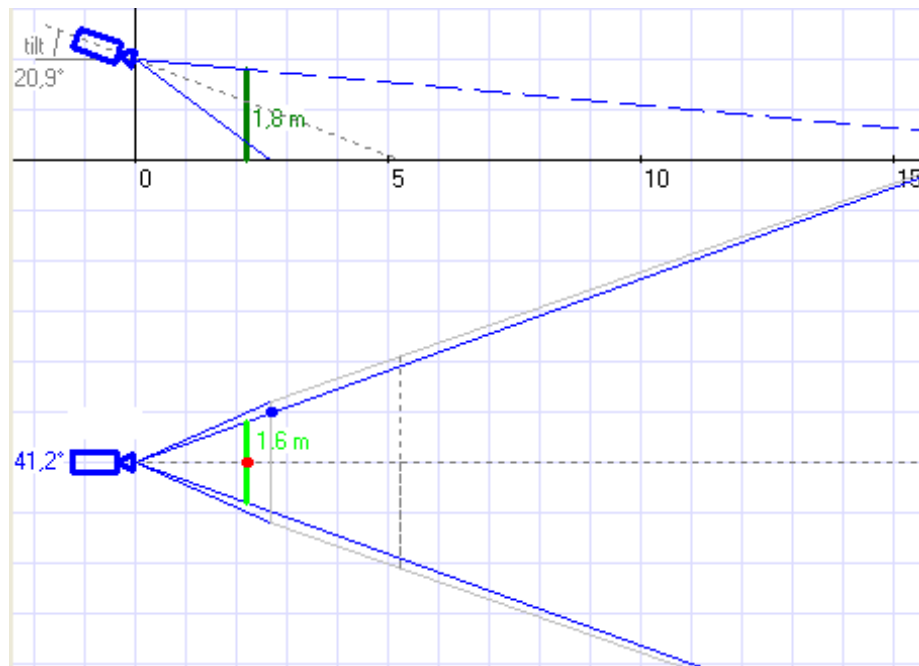


Figura N° 6.16. Campo visual de la cámara 4
Elaborado por: La Investigadora

- Cámara 5: ubicada en oficina de Asistente de Secretaría General.

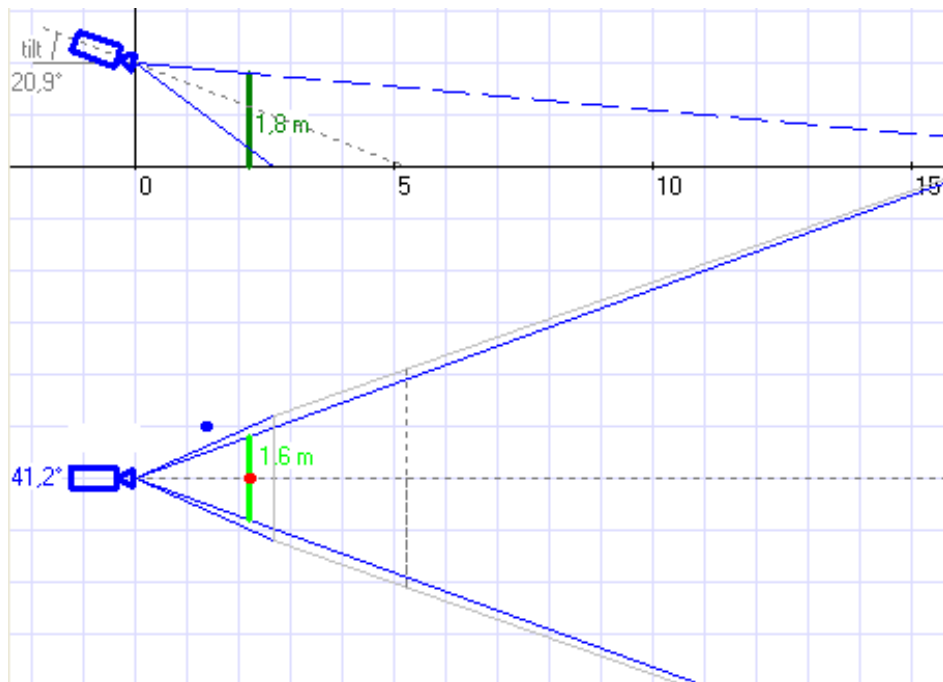


Figura N° 6.17. Campo visual de la cámara 5
Elaborado por: La Investigadora

- Cámara 6: ubicada en entrada secundaria al edificio principal.

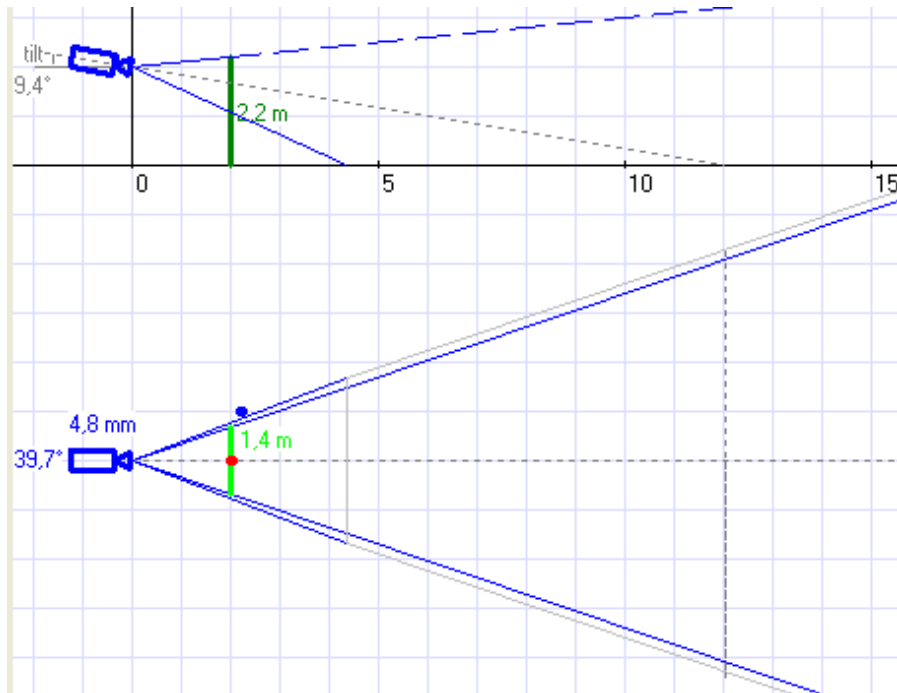


Figura N° 6.18. Campo visual de la cámara 6
Elaborado por: La Investigadora

- Cámara 7: ubicada en el segundo piso frente a la Biblioteca.

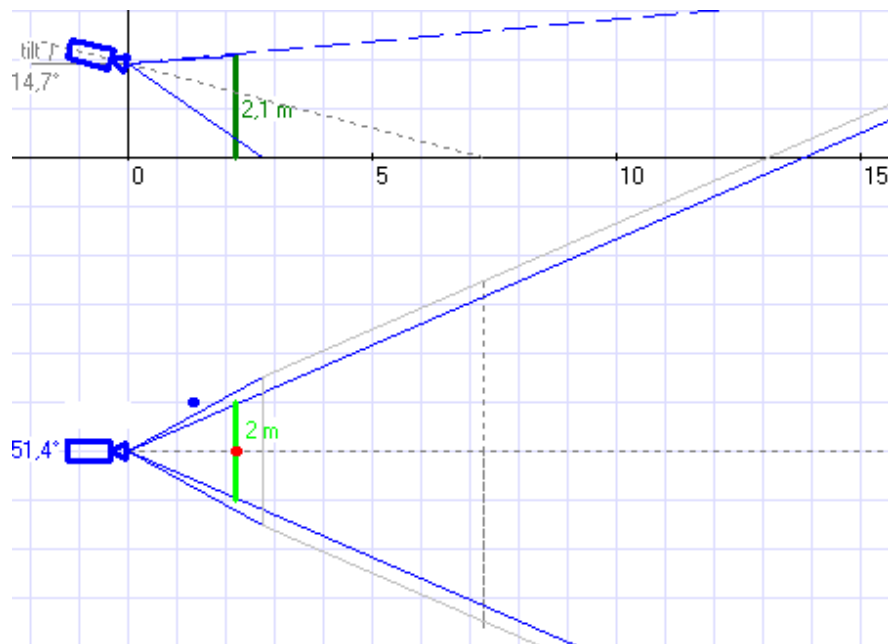


Figura N° 6.19. Campo visual de la cámara 7
Elaborado por: La Investigadora

- Cámara 8: ubicada en el segundo piso frente al ágora.

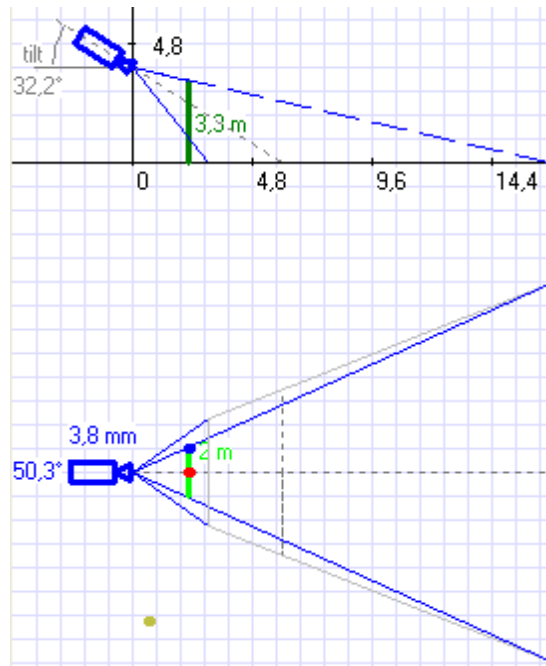


Figura N° 6.20. Campo visual de la cámara 8
Elaborado por: La Investigadora

- Cámara 9: ubicada en el primer piso del nuevo edificio frente a las escaleras.

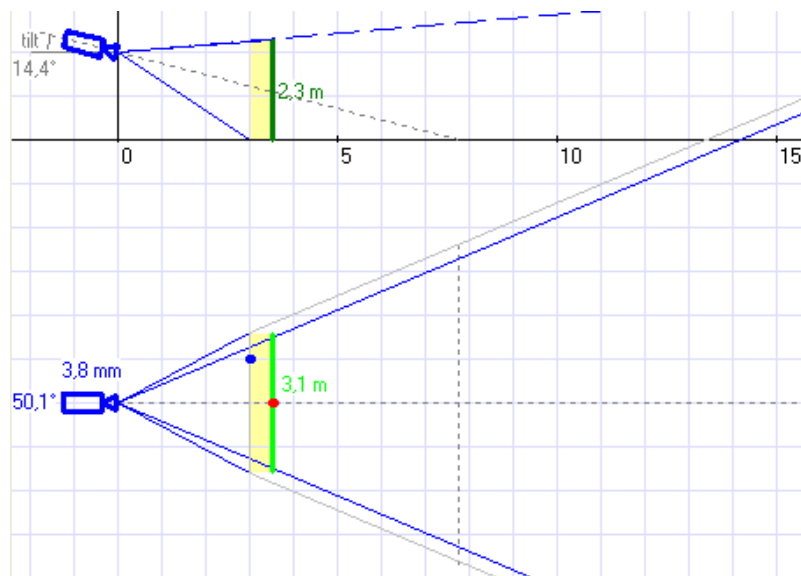


Figura N° 6.21. Campo visual de la cámara 9
Elaborado por: La Investigadora

En la siguiente tabla se muestran los respectivos resultados, para cada cámara IP:

Equipo	Altura instalación (m)	Distancia al objeto (m)	Ángulos de visión		Longitud focal	
			Horizontal (grados)	Vertical (grados)	Altura objeto (m)	Ancho CDV (m)
CÁM 1	2	2	41	31,3	1,9	1,4
CÁM2	2	2	39,3	30,5	2	1,4
CÁM 3	2,1	1,5	40,9	31,2	1,7	1,1
CÁM 4	2	2,2	41,1	31,4	1,8	1,6
CÁM 5	2	2,2	41	31,3	1,8	1,6
CÁM 6	2	2	41	31,3	2,2	1,4
CÁM 7	1,9	2,2	51	39,4	2,1	2
CÁM 8	3,8	2,2	51	39,4	3,3	2
CÁM 9	2	3,5	49,9	38,5	2,3	3,1

Tabla 6.1. Parámetros de ubicación de cámaras IP
Elaborado por: La Investigadora

Después de la apreciación y análisis respectivo de cada figura y los resultados obtenidos, se puede concluir que la ubicación de cada cámara IP, ofrece un campo de visualización eficiente para cada área que se requiere salvaguardar con el sistema de vigilancia IP.

- Para comprobar el radio enlace PTM que requiere la red Radio inalámbrico-Cámaras IP, se realizarán los siguientes cálculos:

1. Longitud del enlace y Radio de la primera Zona de Fresnel

Para calcular la primera zona de Fresnel se aplica la siguiente fórmula:

$$rf = 31,6 \times \sqrt{\frac{\lambda \times d1 \times d2}{d_{total}}}$$

Donde:

d1 = distancia desde el radio de comunicación

d2 = distancia desde la cámara

dt = distancia total del enlace

rf = radio de la primera Zona de Fresnel

λ = longitud de onda, que es igual a:

$$\lambda = \frac{c}{f} = \frac{3 * 10^8}{5,8 * 10^9} = 0,0517 \text{ m}$$

Aplicando la fórmula se obtienen los siguientes resultados:

	d1 (Km)	d2 (Km)	dt = d1+d2	rf
CAM1 -R1	0.005	0.006	0.011	0.375
CAM 2-R1	0.005	0.004	0.009	0.339
CAM 3-R1	0.005	0.001	0.006	0.207
CAM 4-R1	0.005	0.004	0.009	0.339
CAM 5-R1	0.003	0.005	0.008	0.311
CAM 6-R1	0.013	0.005	0.018	0.432
CAM 7-R1	0.007	0.007	0.014	0.425
CAM 8-R1	0.005	0.003	0.008	0.311
CAM 9-R2	0.005	0.008	0.013	0.399

Tabla 6.2. Radios de la Primera Zona de Fresnel
Elaborado por: La Investigadora

2. Línea de vista

$$\text{LOS} = [x * (d - d_1) * 1000] + h_2$$

$$x = \frac{h_1 - h_2}{d * 1000}$$

Donde:

h1 = altura del Radio (m)

h2 = altura de la cámara (m)

	h1 (m)	h2 (m)	d1 (Km)	dt (Km)	x	LOS
CAM 1	4.000	2	0.005	0.011	0.182	3.091
CAM 2	4.000	2	0.005	0.009	0.222	2.889
CAM 3	4.000	2.1	0.005	0.006	0.317	2.417
CAM 4	4.000	2	0.005	0.009	0.222	2.889
CAM 5	4.000	2	0.003	0.008	0.250	3.250
CAM 6	4.000	2	0.013	0.018	0.111	2.556
CAM 7	4.000	1.9	0.007	0.014	0.150	2.950
CAM 8	4.000	3.8	0.005	0.008	0.025	3.875
CAM 9	2.000	2	0.005	0.013	0.000	2.000

Tabla 6.3. Cálculos para Línea de Vista
Elaborado por: La Investigadora

3. Cálculo de la Atenuación Libre en el Espacio

Las ondas de radio al momento de propagarse en el espacio experimentan pérdidas, mientras mayor sea la trayectoria entre dos antenas, provocando una dispersión de la señal según se aleja el transmisor.

La ecuación que establece el valor de la atenuación es:

$$\alpha_{el} (dB) = 92,45 + 20\log_{10}(F_{GHz}) + 20\log_{10}(D_{Km})$$

Donde:

D = Distancia total del tramo (Km)

F = Frecuencia a la que se está trabajando (GHz)

Obteniéndose lo siguientes resultados:

CÁMARA	Frecuencia (GHz)	Distancia respecto al Radio inalámbrico (Km)	FSL (dB)
CAM 1	5.800	0.011	68.546
CAM 2	5.800	0.009	66.803
CAM 3	5.800	0.006	63.282
CAM 4	5.800	0.009	66.803
CAM 5	5.800	0.008	65.780
CAM 6	5.800	0.018	72.824
CAM 7	5.800	0.014	70.641
CAM 8	5.800	0.008	65.780
CAM 9	5.800	0.013	69.997

Tabla 6.4. Atenuación en el Espacio Libre
Elaborado por: La Investigadora

4. Intensidad de Campo eléctrico en recepción

La intensidad de campo en el espacio libre se determina con la fórmula:

$$E_0(dB\mu) = 74,77 + P_{TX}[dB] + G_{TX}[dB] - 20 \log(dt) [Km]$$

Donde:

P_{TX} = potencia de transmisión

G_{TX} = ganancia de transmisión

dt = distancia del enlace

En donde se obtienen los siguientes resultados:

	Distancia enlace (Km)	Eo (dBu)	Eo (dB)	Eo (V/m)
CAM 1 - R1	0.011	108.642	48.642	270.450
CAM 2 - R1	0.009	110.385	50.385	330.500
CAM 3 - R1	0.006	113.907	53.907	495.840
CAM 4 - R1	0.009	110.385	50.385	330.550
CAM 5 - R1	0.008	111.408	51.408	371.870
CAM 6 - R1	0.018	104.365	44.365	165.200
CAM 7 - R1	0.014	106.547	46.547	212.490
CAM 8 - R1	0.008	111.408	51.408	371.870
CAM 9 - R2	0.013	107.191	47.191	228.840

Tabla 6.5. *Intensidad de Campo eléctrico en recepción*
Elaborado por: La Investigadora

5. Potencia de recepción

La potencia de recepción nominal se obtiene restando la P_{TX} en dB de las atenuaciones, al espacio libre y sumando la ganancia de antenas. En términos matemáticos:

$$P_{RX}(dB) = P_{TX}(dB) + G_{TX}(dB) + G_{RX}(dB) - \alpha_{el} (dB)$$

Donde:

P_{TX} = potencia de transmisión = -18 dB

G_{TX} = ganancia de transmisión = 12,7 dB

G_{RX} = ganancia de recepción = 12,7 dB

α_{el} = atenuación en el espacio libre = FSL

6. Margen de desvanecimiento

El margen de desvanecimiento es la diferencia entre el nivel de recepción calculado y el umbral requerido por el fabricante para garantizar una cierta confiabilidad.

$$M_D = P_{RX}(dB) - U_{RX} (dB)$$

Donde:

P_{RX} = potencia de recepción

U_{RX} = umbral de recepción

La potencia umbral del receptor es el nivel mínimo de potencia que asegura una determinada tasa de error BER.

$$U_{RX} = -203,98 + 10 \log B(\text{Hz}) + 3\text{dB} + 10\text{dB} + F$$

Donde:

B = ancho de Banda del equipo receptor (20 MHz)

F= Factor de ruido del equipo receptor en dB (-40 dB)

$$U_{RX} = -203,98 + 10 \log(20 \times 10^6) + 3\text{dB} + 10\text{dB} - 40\text{dB}$$

$$U_{RX} = -157,970 \text{ dB}$$

De donde se obtienen los siguientes resultados de Potencia de recepción y Margen de desvanecimiento:

	FSL (dB)	PRX (dB)	MD (dB)
CAM 1 - R1	68.546	-61.146	96.824
CAM 2 - R1	66.803	-59.403	98.567
CAM 3 - R1	63.282	-55.882	102.088
CAM 4 - R1	66.803	-59.403	98.567
CAM 5 - R1	65.780	-58.380	99.590
CAM 6 - R1	72.824	-65.424	92.546
CAM 7 - R1	70.641	-63.241	94.729
CAM 8 - R1	65.780	-58.380	99.590
CAM 9 - R2	69.997	-62.597	95.373

Tabla 6.6. Potencia de recepción y Márgenes de desvanecimiento
Elaborado por: La Investigadora

El margen de desvanecimiento está directamente relacionado con la confiabilidad del sistema que representa la disponibilidad anual del mismo.

En la *tabla 6.7* se hace una relación respecto al porcentaje de confiabilidad respecto al Margen de desvanecimiento.

Tabla de Confiabilidad	
Confiabilidad %	M.D (dB)
90	10
99	20
99.9	30
99.99	40
99.999	50
99.9999	60
99.99999	70
99.999999	80
99.9999999	90

Tabla 6.7. *Tabla de Confiabilidad en base al Margen de Desvanecimiento
Elaborado por: La Investigadora*

De los resultados obtenidos de los diferentes cálculos, se determina que el enlace tiene una confiabilidad de aproximadamente 100%, durante su funcionamiento; debido a que los valores de cada Margen de desvanecimiento sobrepasan los 90dB.

Los resultados obtenidos se deben a que el sistema cuenta con equipos de comunicación inalámbrica, robustos y de buenas características de potencia de transmisión y sensibilidad de recepción.

c) Distribución de los equipos

Los equipos activos del sistema se encuentran distribuidos en los diferentes niveles de los edificios que componen la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

En la primera planta del edificio principal:



Figura N° 6.22. Cámara 1 ubicada en la oficina de Secretaria de Carrera
Elaborado por: La Investigadora

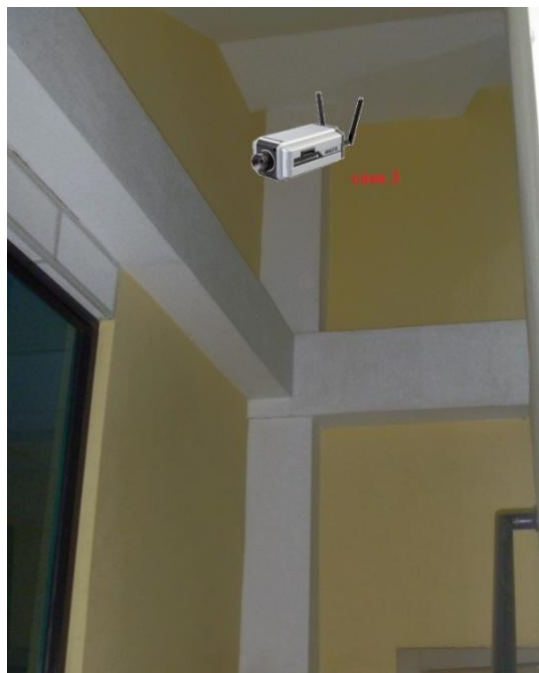


Figura N° 6.23. Cámara 3 ubicada en las escaleras del primer piso
Elaborado por: La Investigadora

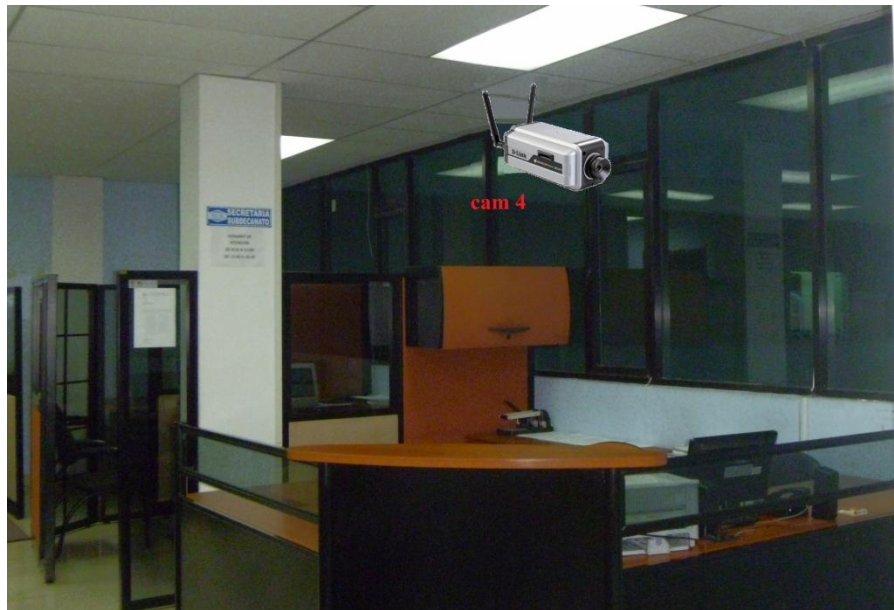


Figura N° 6.24. Cámara 2 ubicada en la entrada al ágora del edificio principal
Elaborado por: La Investigadora



Figura N° 6.25. Cámara 6 ubicada en la entrada secundaria al edificio principal
Elaborado por: La Investigadora

En la segunda planta del edificio principal:



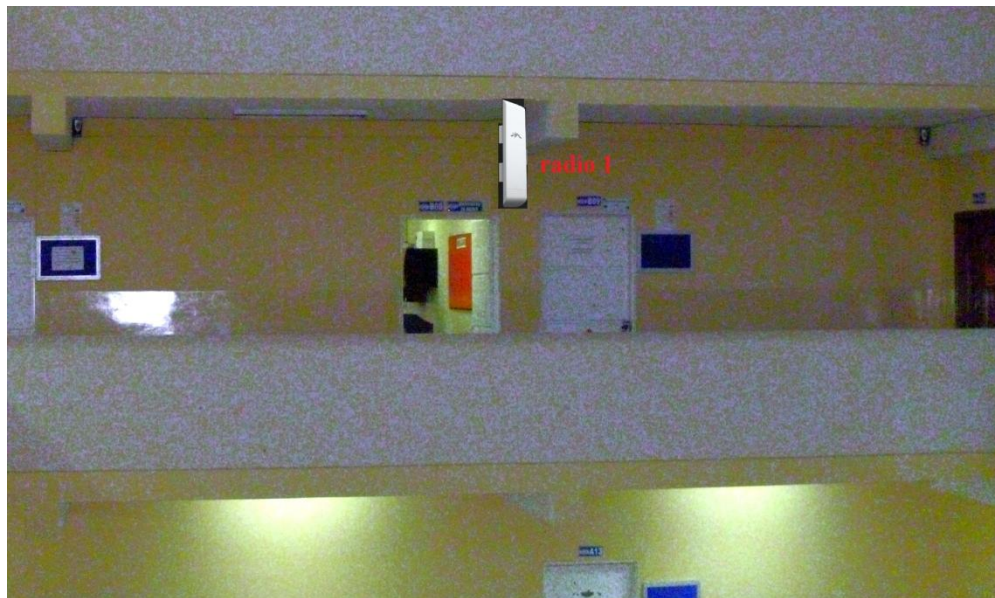
*Figura N° 6.26. Cámara 4 ubicada en la oficina de Secretaria Subdecanato
Elaborado por: La Investigadora*



*Figura N° 6.27. Cámara 7 ubicada en el segundo piso frente a la Biblioteca
Elaborado por: La Investigadora*



*Figura N° 6.28. Cámara 8 ubicada en el segundo piso frente al ágora
Elaborado por: La Investigadora*



*Figura N° 6.29. Radio 1 localizado en el segundo piso frente a Administración de redes
Elaborado por: La Investigadora*

En la tercera planta del edificio principal:



Figura N° 6.30. Cámara 5 localizada en la oficina de Asistente de Secretaria General

Elaborado por: La Investigadora

En la primera planta del nuevo edificio:

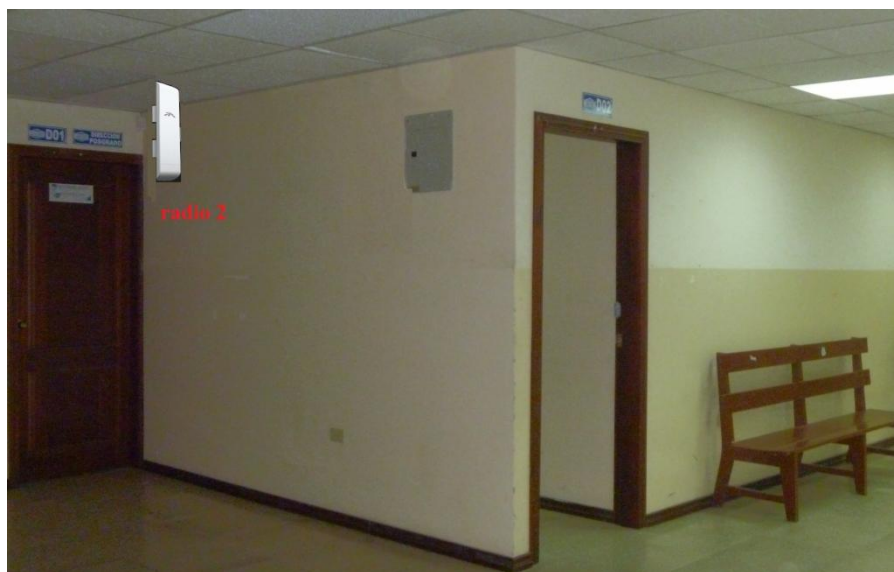


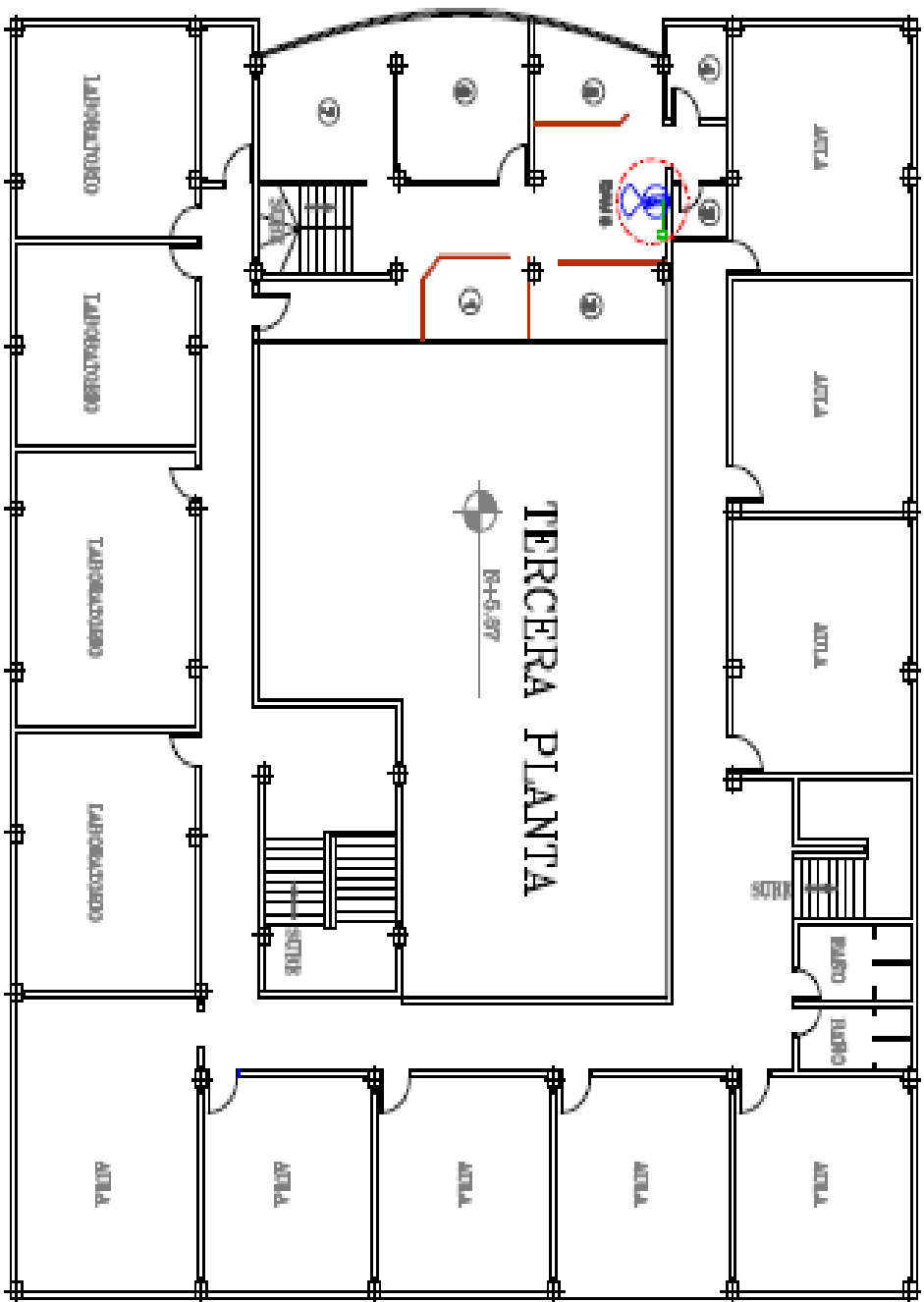
Figura N° 6.31. Radio 2 ubicado en la primera planta

Elaborado por: La Investigadora



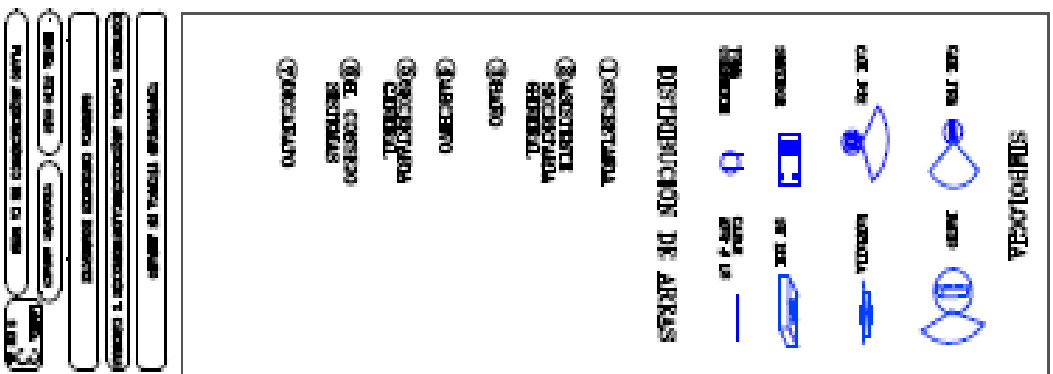
Figura N° 6.32. Cámara 9 ubicada en la primera planta del nuevo edificio
Elaborado por: La Investigadora

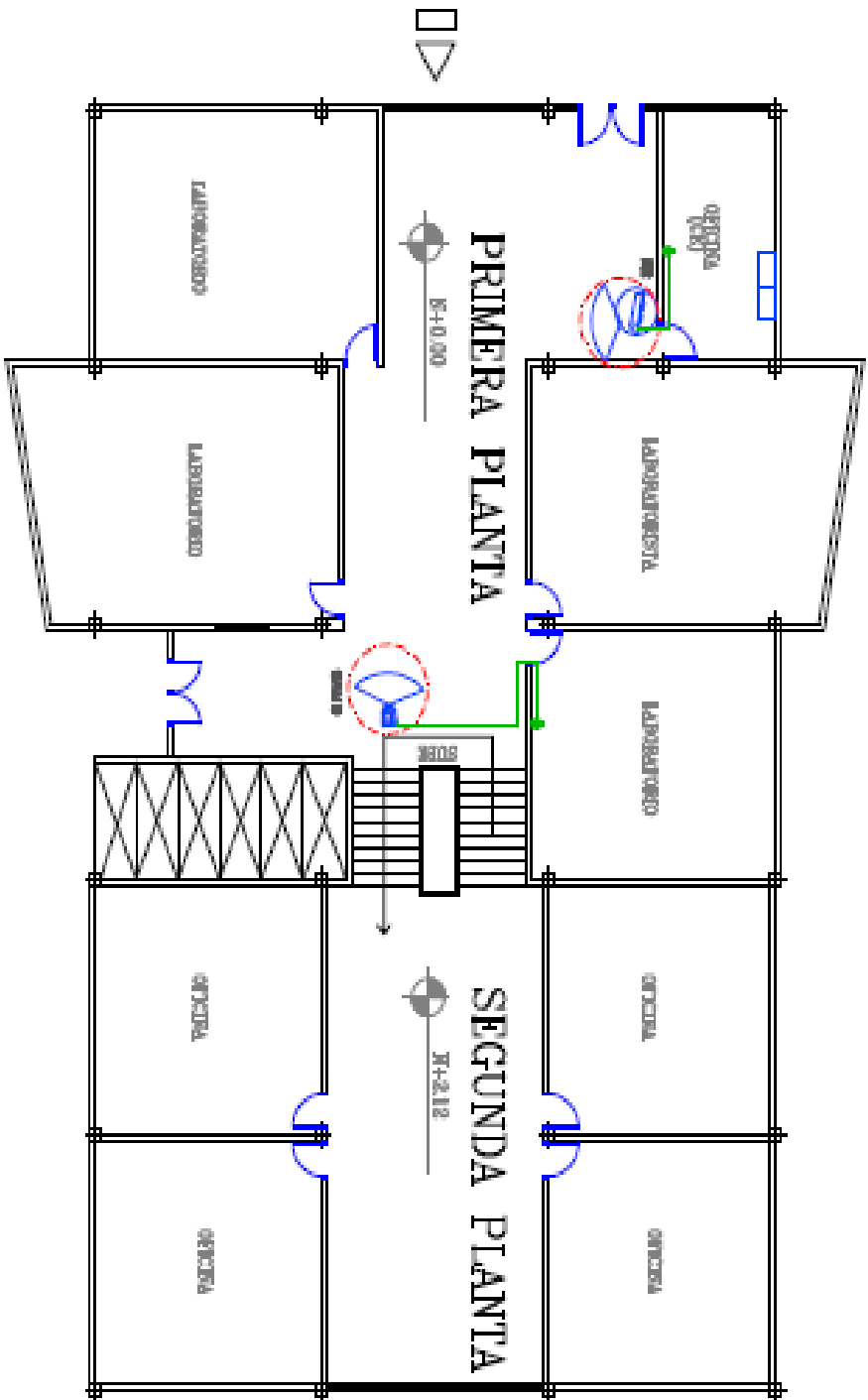
Las cámaras que se utilizarán serán para vigilancia interior.



TERCERA PLANTA EDIFICIO PRINCIPAL, FISEI

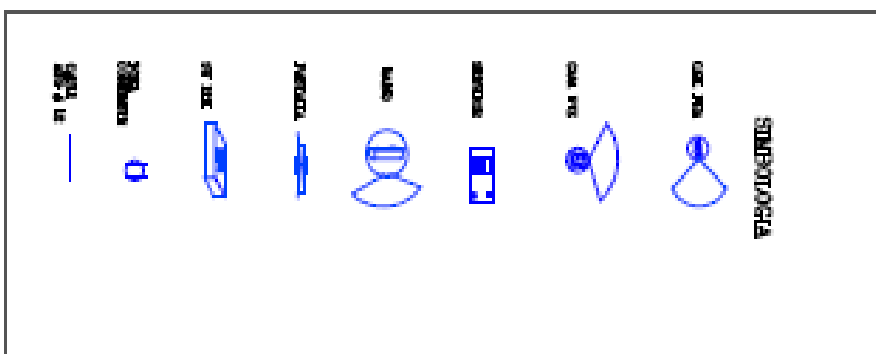
Figura 17.14. Tercera planta del edificio principal con abastecimiento de agua.





PRIMERA PLANTA NUEVO EDIFICIO FISEI

Proyecto de Edif. FISEI, Proyecto de Edif. FISEI, Proyecto de Edif. FISEI



Para la alimentación eléctrica de los equipos y dispositivos que componen el sistema de Video vigilancia, la toma de energía se realizará de los puntos más cercanos que se tengan a cada equipo y componente del sistema.

6.8.3 Diseño lógico

6.8.3.1 Topología lógica

La topología lógica de una red IP, describe la manera en que los datos son convertidos en una trama específica, y la forma en la que estos pulsos eléctricos son transmitidos a través del medio de comunicación.

La topología que se usó en la red es la *topología broadcast*, donde cada equipo (radios inalámbricos, y servidor de almacenamiento) envía sus datos hacia los demás equipos que se encuentran conectados al medio de la red.

Para la asignación de direcciones IP se tomará en cuenta que el único tráfico de información es audio y video procedente de las diferentes cámaras de red ubicadas en las diferentes instancias de los edificios que componen la FISEI.

Por esta razón se tendrá una sola subred, la cual también incorpora a los radios de comunicación inalámbrica y al servidor de almacenamiento.

Se usará la dirección *192.168.1.0* con máscara por defecto *255.255.255.0*, la que permite hasta 254 hosts. Para optimizar direcciones se dividirá mediante VLSM en una subred con las siguientes características:

Dirección de Subred: 192.168.1.0

Máscara de subred: 255.255.255.240

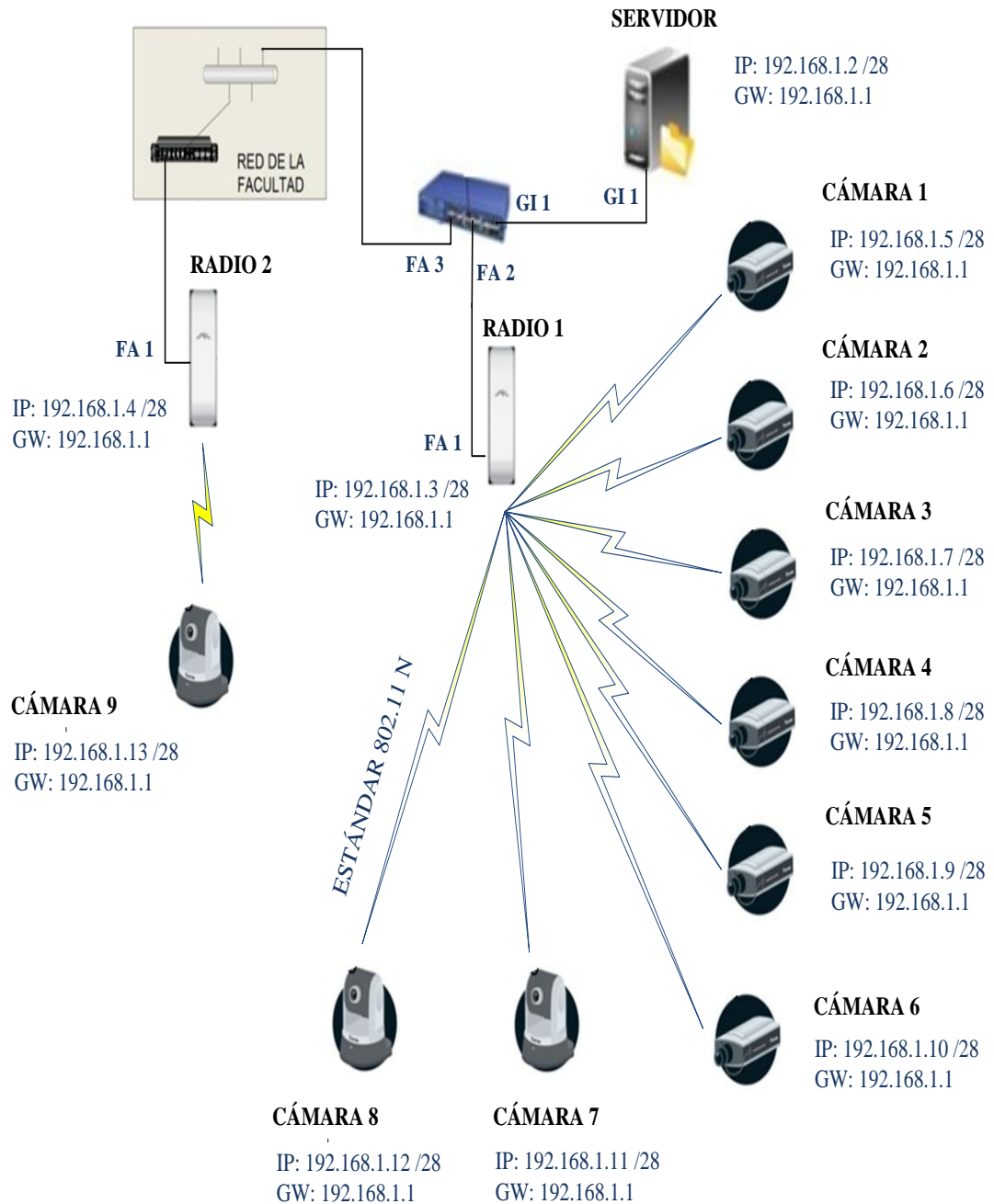
Gateway: 192.168.1.1

Que permiten tener 14 direcciones de host válidas, las cuales se enuncian en la siguiente tabla:

EQUIPO	UBICACIÓN	DIRECCIONES IP
Servidor de video	Oficina de Administración de redes	192.168.1.2
RADIO 1	Segundo piso frente a Administración de redes	192.168.1.3
RADIO 2	Primer piso del nuevo edificio	192.168.1.4
CAM 1 (fija)	Secretaria de Carrera	192.168.1.5
CAM 2 (fija)	Entrada al ágora del edificio principal	192.168.1.6
CAM 3 (fija)	Escaleras del primer piso	192.168.1.7
CAM 4 (fija)	Secretaria Subdecanato	192.168.1.8
CAM 5 (fija)	Asistente de Secretaria General	192.168.1.9
CAM 6 (fija)	Entrada secundaria al edificio principal	192.168.1.10
CAM 7 (PTZ)	Segundo piso frente a la Biblioteca	192.168.1.11
CAM 8 (PTZ)	Segundo piso frente al ágora	192.168.1.12
CAM 9 (PTZ)	Primer piso del nuevo edificio frente a las escaleras	192.168.1.13
SWITCH ET	Oficina de Administración de redes	No administrable

Tabla 6.8. *Topología lógica de la red de Video Vigilancia*
Elaborado por: La Investigadora

El esquema lógico para el sistema de Vigilancia IP es el que presenta a continuación:



*Figura N° 6.37. Diagrama lógico de la red IP
 Elaborado por: La Investigadora*

6.8.4 Requerimientos del sistema

En base a las necesidades de seguridad y vigilancia expresadas en las entrevistas con las principales autoridades de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, Ing. Oswaldo Paredes (Decano) y con el Ing. Vicente Morales (Subdecano), sobre las áreas que requieren mayor seguridad en el sector administrativo, y requerimientos para el diseño del sistema de vigilancia IP, se determinó una solución de vigilancia y seguridad que cumple con los siguientes parámetros y requerimientos:

- La cobertura planteada para el sistema, cubre zonas que manejan información exclusiva como secretarías de Carrera y secretaría General, las cuales requieren cámaras de buena resolución de imagen durante el día y la noche, grabación continua en ciertas áreas.

La ubicación de las cámaras se encuentra definida en el punto *distribución de equipos*.

- Se debe contar con un servidor de almacenamiento de video, el que se encargará de administrar las cámaras de red, para lo cual se deberá tomar en cuenta la capacidad del servidor de acuerdo con el número de cámaras a usar, y los días que se almacenará el video.

Mientras que los requerimientos para el diseño son:

- Cobertura, se alcanzará incorporando un servidor de video en la en un área acondicionada para los equipos, el cual puede ser accedido desde cualquier punto de la red, de esta forma monitorear o revisar grabaciones de algún evento en especial.
- Las cámaras IP serán ubicadas de manera que no invadan la privacidad del personal administrativo.

- Escalabilidad, el diseño del sistema se realizará en base a la información suministrada por las autoridades y el personal encargado del funcionamiento y seguridad de la FISEI, sin embargo el sistema deberá permitir su expansión a más puntos de vigilancia en el futuro.
- Administración de Video Vigilancia, la propuesta deberá permitir el acceso a la revisión de video grabado y en vivo, de y desde todas áreas de conforman el edificio administrativo por medio de la red informática privada. La solución de Video Vigilancia, deberá permitir la administración, configuración y personalización de forma local o remota.
- Seguridad, el sistema contará con políticas de seguridad a los sistemas de grabación para impedir el acceso de usuarios tanto internos como externos.

El sistema permitirá un monitoreo en tiempo real, solo para personal autorizado.

- Hardware propuesto, se describe los componentes de hardware necesarios para armar la solución a los niveles deficientes de seguridad, con los requerimientos mínimos a cumplir o superar del Hardware, con características como convergencia y robustez.
- Se acondicionará un espacio para el cuarto de equipos, donde el acceso será para personal autorizado.

Dimensionamiento de equipos

Las especificaciones respecto a componentes del sistema son:

a) Red inalámbrica

- Switch Ethernet

Este tipo de equipo es un dispositivo de red que interconecta y dirige información entre los radios de comunicación inalámbrica y el hardware de gestión (servidor de almacenamiento).

Las características con las que debe contar para su integración al sistema son:

Soporte de:	Voz, datos, tecnología inalámbrica
Número de puertos LAN:	Mínimo 4
Modo de comunicación:	Full dúplex

Tabla 6.9. Características de selección para el Switch Ethernet
Elaborado por: La Investigadora

- Radio, equipos para la transmisión/recepción inalámbrica

Las características para este equipo son:

Potencia de transmisión:	>18 dBm
Sensibilidad de recepción:	Mínimo -80 dBm
Seguridad inalámbrica:	Al menos WPA
Modo Bridge:	Sí

Tabla 6.10. Características de selección para el Radio de comunicación inalámbrica
Elaborado por: La Investigadora

b) Cámaras IP

Las características que deben cumplir las cámaras de red, se listan en las siguientes tablas según el tipo de cámara.

Para la selección de cámaras fijas

Mínima iluminación:	>0.2 lux
Resolución:	640x480 píxeles
Campo de visión:	> 30° (horizontal y vertical)
Formato de compresión a los que debe funcionar:	2
Soporte de audio y video simultáneo:	Sí
Vigilancia día/noche:	Sí

Tabla 6.11. Características de selección para Cámaras IP fijas
Elaborado por: La Investigadora

Para la selección de cámaras PTZ

Mínima iluminación:	> 0.5 lux
Resolución:	640x480 píxeles
Campo de visión:	Pan >50°, Tilt >100°
Formato de compresión a los que debe funcionar:	2
Soporte de audio y video simultáneo:	Sí
Vigilancia día/noche:	Sí

Tabla 6.12. Características de selección para Cámaras IP PTZ
Elaborado por: La Investigadora

c) Central de monitoreo

- Servidor de video

Procesador Intel Core 2 Duo al menos de 2.8 GHz	Sí
Memoria de 2GB	Sí
Disco duro en el orden de los TB:	Sí
Puertos Gigabit Ethernet RJ-45:	Sí
Puertos de expansión:	Sí
Monitor Flat Panel	Sí

Tabla 6.13. Características de selección para el servidor de video
Elaborado por: La Investigadora

- Software para Gestión de video

Permitir grabación de video y audio en directo	Sí
Grabación de video tipo:	MJPEG, MPEG-4
Monitorización y reproducción	Sí
Funciones de grabación:	Continua/Programada/Manual
Seguridad en ficheros de video	Sí
Niveles de seguridad:	Control de usuarios y accesos
Compatible con el equipo servidor	Sí

Tabla 6.14. Características de selección para el software de gestión de video
Elaborado por: La Investigadora

Selección de equipos

Para la selección de los equipos que componen el sistema de vigilancia se tomó en cuenta las características establecidas en el dimensionamiento de equipos, a esto se adicionó facilidad de instalación, costo, y características de garantía.

- Switch Ethernet

Equipo	WS-c2960-8TC-L	SD2005
Número de puertos	8	5
Protocolos de gestión remota	SNMP 1 , HTTPS , TFTP , SSH , Telnet, HTTP	No es administrable
Subtipo	Fast Ethernet	Gigabit Ethernet
<i>Fabricante</i>	CISCO	CISCO
<i>Costo</i>	774,8	70

Tabla 6.15. Comparación Switch Ethernet
Elaborado por: La Investigadora

- Equipos de transmisión inalámbrica

Equipo	NanoStation M	Access Point 3Com 8760
Interface de red	2 x 10/100 BASE-TX ETH	1 x 10 BASE-T, o 10/100 BASE-TX ETH
Configuración de red	PMP, PTP	PMP, PTP
Método de alimentación	PoE	Inyector de corriente
Ganancia de antena	13,7 dB	4 dB (2 dB por antena)
Frecuencia de operación	5470-5825 MHz	5 GHz
Alcance	15 Km	475 m
Estándares	802.11 n	802.11 a, b, g
Método de Espectro Extendido	TDMA	OFDM
Tipo de antena	Incluida	Externa desmontable (dos)
<i>Fabricante</i>	UBIQUITI	HP-3COM
<i>Costo</i>	259,1	404,97

Tabla 6.16. Comparación equipos inalámbricos
Elaborado por: La Investigadora

- Cámaras IP

Cámaras Fijas Día/noche

Cámara	IP7154	DCS-3430
	Día/noche	Día/noche
<i>Video</i>		
Resolución	640x480	640x480
Frames por segundo	30	más de 30
Mínima iluminación	0.2 Lux	0.5 Lux
Simultaneous dual streaming	x	

Cámara	IP7154	DCS-3430
Ángulo de visión	horizontal: 26.7° - 69° vertical: 20° - 51°	horizontal: 41° vertical: 31° diagonal: 51°
Zoom digital		16x
Zoom óptico		16x
<i>Compresión</i>		
Motion JPEG	x	x
MPEG-4	x	x
H.624		x
<i>Seguridad</i>		
Protección multinivel	x	x
Filtro IP	x	
Encriptación HTTPS	x	
IEEE 802.1X	x	x
<i>Estándares 802.11</i>		
Versión	802.11 b/g	802.11 b/g/n
<i>Fabricante</i>	VIVOTEK	D-LINK
<i>Costo</i>	726,432	404,04

*Tabla 6.17. Comparación cámaras IP fijas
Elaborado por: La Investigadora*

Cámaras PTZ

Cámara	PZ7132	DCS-5220B1	DCS-5635
<i>Video</i>			
Resolución	640x480	640x480	704x480
Frames por segundo	30	más de 30	30
Mínima iluminación	1.25 Lux	1 Lux	0.7 Lux
Simultaneous dual streaming	x	x	x
Pan	350° (-175° - +75°)	50° - -50°	165° - -165°
Tilt	125° (-35° - +90°)	90° - -45°	-87° - +34°
Zoom digital		4x	16x
Zoom óptico	2.6x		10x
<i>Compresión</i>			
Motion JPEG	x	x	x
MPEG-4	x	x	x
H.624			x
<i>Seguridad</i>			
Protección multinivel	x	x	x
Filtro IP	x		
Encriptación HTTPS	x	x	x
IEEE 802.1X	x	x	x
<i>Estándares 802.11</i>			
Versión	802.11 b/g	802.11 b/g	802.11 n
<i>Fabricante</i>	VIVOTEK	D-LINK	D-LINK
<i>Costo</i>	448	341,6	881,44

*Tabla 6.18. Comparación cámaras IP PTZ
Elaborado por: La Investigadora*

- Central de monitoreo

Equipo	HP ProLiant ML350 G6 serie SAS/SATA-SFF	Computador
Formato	Torre, convertible a 5U para RACK	Torre
Procesador	Intel Xeon 6-Core E5645: 2.4 GHz, con cache 12MB L3 cache	Intel I5-2400 3.1GHZ 2da G S1155
Memoria RAM	6GB, Máximo 288GB	Memoria DDR3 PC1333 4GB MARKVISION
Capacidad de discos	2 discos de 500 GB SAS	2 discos duros SATA SAMSUNG de 500GB
Slot de ampliación	6 (1 PCI-Express Gen2 x16 y 5 PCI-Express Gen2 x8)	6 (1 x procesador, 2 x memoria, 1 x PCI Express 2.0X16, 1 x PCI)
Controlador de red	PCI Express Gigabit NIC 10/100/1000	Intel 82579V Gigabit Ethernet
Fuente de poder	Fuente de poder redundante 750 Watts	Fuente de 900 Watt
Monitor	HP de 17"	LG W1943S LCD 18.5"
Mainboard		BOARD INTEL DH61WW BULK(I3,I5,I7 SEGUNDA G)
Unidad de disco		DVD-WRITER SATA LG
Lector de memorias		Lector de memorias interno 3.5" MARKVISION
Tipo de torre		CASE DLUX MF451
<i>Costo</i>	3580	780

Tabla 6.19. Comparación servidores de video
Elaborado por: La Investigadora

En base a las características físicas, funcionamiento, y costo económico se seleccionaron los siguientes equipos que conformarán la red del sistema de Vigilancia IP:

- Cámaras IP, Marca **D-Link**

Se seleccionó la cámara Fija *DCS-3430*, ya que permite mayor cantidad de fps en comparación a las otra opciones, trabaja con tres formatos de compresión mejorando las características de administración de video, es compatible con el estándar 802.11 n permitiendo mayor alcance y mejores prestaciones a la red inalámbrica. Además la cámara IP es la solución perfecta para aplicaciones en interior y exterior.

Para la grabación de video en zonas que requieren mayor rango de cobertura se seleccionó la cámara PTZ *DCS-5635*, porque ofrece mayor resolución de video a

comparación de las demás opciones presentadas, graba en ambientes con poca cantidad de luz, lo que la hace ideal para áreas que requieren vigilancia constante, presenta mejores características de zoom óptico, además permite trabajar con tres formatos de compresión, evitando el excesivo consumo de ancho de banda.

En el ANEXO 2, se muestran las características técnicas de la cámara Fija *DCS-3430*. Mientras que en el ANEXO 3, se presentan las características técnicas de la cámara PTZ *DCS-5635*, datos importantes como fps (imágenes por segundo), tipo de sensor para la imagen, ángulos de visión, entre otras características que la convierten en la mejor opción para la satisfacer las necesidades de vigilancia del edificio administrativo.

- *Hardware de gestión, Marca **HP***

Para la gestión del video se selecciono el servidor *HP ProLiant ML350 G6 serie SAS/SATA-SFF*, que permite procesar y almacenar grandes cantidades de información durante largos períodos de tiempo. Además cumple con parámetros para el ahorro de energía.

Al trabajar con un computador como hardware de gestión no se cuenta con muchas características de ampliación como se podría hacer con un servidor, además la velocidad de procesamiento y la administración de servicios son características que se tomaron en cuenta para la selección.

En el ANEXO 4, se muestran las características técnicas del hardware de gestión de video *HP ProLiant ML350 G6 serie SAS/SATA-SFF*, el cual es un servidor que presenta buenas características de procesamiento y almacenamiento.

- *Software de gestión, Marca **D-Link***

El software *D-ViewCam*, es un sistema de vigilancia integral diseñado para gestionar de forma centralizada múltiples cámaras IP, para monitorizar video

digital en directo, grabar vídeo, sonido y eventos para diferentes aplicaciones de seguridad y vigilancia.

Como se menciona en la página web de la empresa D-Link (http://www.dlink.es/cs/Satellite?c=Guide_P&childpagename=DLinkEurope-ES%2FDLGeneric&cid=1197382658083&p=1197318960431&packedargs=locale%3D1195806681347&pagename=DLinkEurope-ES%) D-ViewCam “Este software incorpora una amplia gama de funcionalidades para su mayor comodidad, incluyendo grabación y reproducción de vídeo, Modo Vídeo, Modo Mapa, Modo Asistente, Modo Experto, Acción de Eventos, entre otras funcionalidades, ofreciendo un software completo y fácil de utilizar.”

Soporta hasta 32 cámaras IP, es compatible con todas las cámaras IP actuales de D-Link, servidores de vídeo y ofrece control digital y grabación de video y audio. Este software proporciona a los usuarios una amplia gama de características, entre las que se mencionan:

- Monitorización y gestión en tiempo real.
- Grabación y reproducción de vídeo.
- Sistemas de respaldo de video y bases de datos
- De fácil uso, y viene integrado de manera gratuita en las cámaras D-Link.
- Visualiza y gestiona hasta 32 cámaras en una única pantalla sin problemas ni complicaciones.
- Controla y configura cámaras desde cualquier sitio, ya sea través de internet o en una red local.
- Gestión de Video vigilancia efectiva y sin costes.
- Funciona con todas las versiones de Windows a partir de Windows 98.

En la *figura N° 6.38* muestra la pantalla principal del programa D-ViewCam, y sus diferentes secciones, a través de las cuales se gestiona y administra las funcionalidades de la cámara de red IP el video.



Figura N° 6.38. Pantalla principal del software de gestión D-ViewCam de D-Link
Elaborado por: La Investigadora

La pantalla está dividida en diferentes áreas, las cuales son descritas a continuación:

- a) Área 1, *Main Display Area*; se encarga de la monitorización del video.
- b) Área 2, *System Board Area*; indica la hora y fecha del sistema.
- c) Área 3, *Select Device and Map Area*; estructura en árbol para visualizar los mapas y dispositivos.
- d) Área 4, *Preview Window Area*; muestra un mapa o imagen del video actual, si una cámara activa se selecciona de la estructura de árbol.
- e) Área 5, *Manual Control Area*; instantánea, grabación manual, controles de audio de dos vías y la pantalla de vídeo congelación.
- f) Área 6, *PTZ Control Area*; seleccionable cuando una cámara seleccionada tiene pan, tilt, zoom y la función de enfoque.
- g) Área 7, *Event Action Log*; lista de registros de eventos.

h) Área 8, *Setting and Search Area*; muestra pantalla completa, la configuración del sistema, búsqueda y reproducción, búsqueda y reproducción de eventos, página de ayuda.

Las características más importantes para la configuración son las listadas a continuación:

- a) Agregar la cámara el software
- b) Asignar un direccionamiento IP.
- c) Seleccionar la configuración de grabación:
 - 24/7 grabación continua, todos los días de la semana.
 - 24/7 grabación económica, todos los días de la semana, con menor calidad de imagen, activación por detección de movimiento.
 - Horario de oficina económico, graba en horario de oficina (8:00 AM hasta 18:00 PM), con menor calidad de imagen, y habilitación por detección de movimiento.
 - No horario de oficina económico, la grabación se establece fuera del horario de oficina (antes de las 8:00 AM y después de las 18:00 PM), ofrece menor calidad de imagen, y habilitación por detección de movimiento.

En el modo de *Configuración Experto*, se presentan más características que se pueden configurar y modificar. Entre ellas están:

- a) Reciclar, permite borrar el video o fotos grabados para liberar espacio en el disco de almacenamiento.
- b) Espacio disponible, el sistema contará y mostrará el espacio disponible del disco en este cuadro de texto.
- c) Acción por eventos, Establecer acciones para los eventos del sistema, entre ellos se listan:

- Cambiar el Estado de la salida digital, activa los dispositivos que se conectan al sistema, como las luces de alarma y sirenas; cuando se produjo un evento.
- Enviar por correo electrónico, permite enviar un correo electrónico a las cuentas especificadas que indican el tipo de evento, adjuntando una imagen tomada al mismo tiempo que se produjo el evento.
- Reproducir sonido.

d) Configuraciones para administrador, y para usuario.

En la *figura N° 6.39* se visualiza la pantalla del Modo de configuración experto del software D-ViewCam.

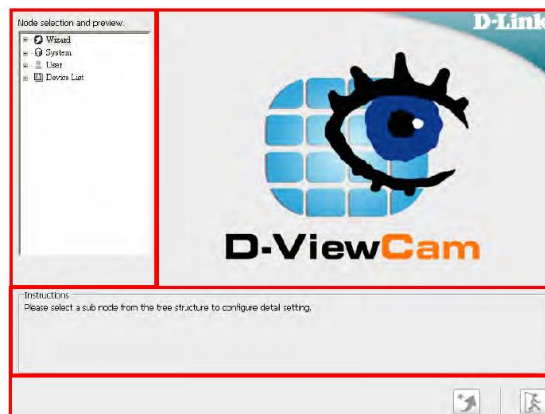


Figura N° 6.39. Pantalla principal del modo de Configuración Experto
Elaborado por: La Investigadora

D-ViewCam también presenta las opciones de:

- a) Búsqueda de video y gestión de reproducción.

La "búsqueda y reproducción de vídeo" permite la reproducción de video grabado a través de la grabación programada, grabación de eventos, y grabación manual.

b) Búsqueda de eventos y gestión de Reproducción.

El cual permite reproducir el evento que se registra en el sistema. En esta opción se puede elegir el tipo de eventos que desea ver marcando la casilla, elegir un canal que desea ver, consultar un evento, reproducir el vídeo, además se puede exportar la información de registro de eventos a un archivo .txt (en el registro se menciona: Fecha / hora, el origen, tipo, acción, relación fuente y la información de contexto).

En fuentes como la Internet se pueden encontrar varios manuales sobre configuración, en los cuales se detalla los pasos a seguir para configurar un determinado modo de funcionamiento.

En el ANEXO 5, se muestran las características técnicas del software de gestión de video D-ViewCam, el cual será utilizado para la administración del video y sonido grabado a determinadas horas del día.

- *Equipo de comunicación inalámbrica, Marca Ubiquiti*

Para la selección de equipo inalámbrico se escogió el *NanoStation M5*, que a diferencia del otro equipo ofrece un alcance superior, y mayor ganancia, los cuales son factores muy importantes en la configuración de una red inalámbrica, finalmente su costo económico y la confiabilidad que existe en la marca hacen que la selección sea la adecuada.

En el ANEXO 6, se muestran las características técnicas del equipo NanoStation M5, necesario para la comunicación inalámbrica de las cámaras de red, se detalla patrones de radiación, tipo de polarización, valores de potencia, sensibilidad de recepción, entre otros, que son muy importantes para el correcto desempeño de la red inalámbrica.

- *Equipo de conmutación de red, Marca Cisco*

Para la conmutación de la red se utilizará el switch *SD2005*, el equipo consta de cinco puertos Gigabit Ethernet, el equipo cumple con estándares de ahorro de energía, además su tamaño compacto facilita su ubicación, y tiene características de Plug & Play, se escogió esta opción por su costo inferior y las prestaciones anteriormente mencionadas las cuales satisfacen las necesidades de conmutación de la red.

En el ANEXO 7, se muestran las características técnicas del equipo switch *SD2005*, necesario para la conmutación de la red IP, el cual está situado entre los equipos de transmisión inalámbrica y el servidor de gestión.

6.8.5 Grabación y almacenamiento

Para el cálculo de ancho de banda y almacenamiento (fórmulas sacadas del proyecto “Diseño de una red de Video vigilancia local y remota sobre IP en tiempo real para una hostería aplicando el concepto de GREEN IT” de CACHIGUANGO Yuri, 2010, pág. 71) de un sistema de debe tener en cuenta lo siguiente:

- Número de cámaras
- Número de horas al día que la cámara estará grabando
- Resolución de imagen
- Tipo de compresión de video: Motion JPEG, MPEG-4, H.264
- Y tiempo de almacenamiento de los datos

a) Ancho de banda

- *Calculo de ancho de banda*

Un sistema de video vigilancia transmite información de audio y video, requiriéndose un cálculo de ancho de banda real. Los factores que afectan el ancho de banda son:

- Tamaño real de bits a transmitir (referencia de la trama Ethernet) y la sobrecarga generada
- Velocidad de imagen, resolución de la imagen, y formato de compresión
- Número de cámaras

Para el diseño se usó como referencia la siguiente tabla de valores, en donde se relacionan tipos de resolución, niveles de compresión y sus respectivos valores numéricos en base a los estándares de resolución.

RESOLUCIÓN	NIVEL DE COMPRESIÓN		
	BAJO (KB)	MEDIO (KB)	ALTO (KB)
PAL 352x288	12	8	4
PAL 704x576	52	34	20
NTSC 352x240	10	7	3
NTSC 704x480	43	28	13

Tabla 6.20. Relación entre la compresión y la resolución
Elaborado por: La Investigadora

Los factores a tomar en cuenta para el cálculo son:

Resolución NTSC 704x480, con nivel medio de compresión y 28 KB en formato M-JPEG.

La trama Ethernet contiene el **campo de datos**, en donde el tamaño real de bytes a transmitir es de 1460 Bytes, y la **sobrecarga de total** por trama es de 66 Bytes.

- Número de tramas

$$\text{número de tramas} = \frac{\text{tamaño de la aplicación}}{\text{datos útiles de la trama Ethernet}}$$

$$\text{número de tramas} = \frac{28 \text{ KB}}{1460 \text{ B}}$$

$$\text{número de tramas en Bytes} = 19,18 \text{ B} \approx 19 \text{ B}$$

- Sobrecarga que produce el paquete transmitido

$$\text{Sobrecarga total} = \text{núm tramas} * \text{sobrecarga trama Ethernet}$$

$$\text{Sobrecarga total} = 19 * 66 \text{ B}$$

$$\text{Sobrecarga total en Bytes} = 1254 \text{ B}$$

Cálculo de los datos totales transmitidos (1 imagen)

- Datos totales transmitidos

$$\text{Datos totales transmitidos} = \text{tam aplicación} + \text{sobrecarga total}$$

$$\text{Datos totales transmitidos} = 28 \text{ KB} + 1254 \text{ B} = 23.40 \text{ Kbits}$$

$$\text{Datos totales transmitidos en Bytes} = 29254 \text{ B}$$

$$\text{Datos totales transmitidos en bits} = 234032 \text{ bits} \approx 23,40 \text{ Kbits}$$

$$\text{Datos totales transmitidos en Kbits} = 23,40 \text{ Kbits}$$

Como último punto se establece el ancho de banda requerido por una sola cámara IP para una frecuencia de 10 imágenes por segundo, que es un parámetro promedio admisible en aplicaciones de video vigilancia.

- Ancho de banda

$$AB_{1C} = \frac{23,40 \text{ Kbits}}{1 \text{ imagen}} * \frac{10 \text{ imágenes}}{1 \text{ segundo}}$$

$$AB_{1C} = 2,34 \text{ Mbps}$$

- Ancho de banda total del sistema

$$AB \text{ total} = \text{núm de cámaras} * AB_{1C}$$

$$AB \text{ total} = 9 * 2,34 \text{ Mbps} = 30 \text{ Mbps}$$

$$AB \text{ total} = 21,06 \text{ Mbps}$$

$$AB \text{ total} \approx 30 \text{ Mbps}$$

El Ancho de Banda que se manejará en la red será de 30 Mbps.

b) Para el Almacenamiento

- *Cálculo de los requisitos de almacenamiento*

Las características para el cálculo son:

- Horas del día en las que la cámara grabará
- Tiempo de almacenamiento
- Formato de compresión
- Número de cámaras
- Tipo de grabación (continua o programada)

Los parámetros para las necesidades de almacenamiento son los siguientes:

- a) Número de cámaras: **9**
- b) Número de horas por día en que la cámara estará grabando: 24 horas o las programadas por el administrador.
- c) Tiempo de almacenamiento: 2 semanas
- d) Tipo de grabación:
 - Áreas con cámaras de grabación continua (24 horas)
 - Áreas con cámaras con grabación programada
- e) Velocidad de imagen, formato de compresión, calidad de imagen y complejidad.

Para el cálculo se utilizará el formato M-JPEG, que maneja un método de compresión de excelente calidad de video pero demanda un gran ancho de banda para su transmisión.

La resolución es NTSC 352x240, con un nivel de compresión de 10KB, con 10 fps (imágenes por segundo).

Las fórmulas para calcular la necesidad de almacenamiento del sistema con el formato de compresión Motion JPEG es:

$$\text{Tamaño de imagen} \times \text{imágenes por segundo} \times 3.600s = \text{kilobyte por hora}/1.000$$

Tamaño de imagen x imágenes por segundo x 3.600s = megabyte (MB)

MB por hora x horas de funcionamiento diarias/1.000 = gigabyte (GB) por día

GB por día x período de almacenamiento solicitado = Necesidades de almacenamiento

- Almacenamiento por hora

*Capacidad/hora = tam imagen * núm imágenes*

$$\text{Capacidad/hora} = \frac{10 \text{ KB}}{\text{imagen}} * \frac{10 \text{ imágenes}}{\text{segundo}} * \frac{3600 \text{ segundos}}{1 \text{ hora}}$$

$$\text{Capacidad/hora} = 360 \text{ MB / hora}$$

- Almacenamiento por día
- Grabación continua

*Capacidad/día = Capacidad/hora * 24 horas*

$$\text{Capacidad/día} = 360 \text{ MB/hora} * 24 \text{ horas}$$

$$\text{Capacidad/día} = 8,437 \text{ GB/día}$$

- Grabación programada

*Capacidad/día = Capacidad/hora * 12 horas*

$$\text{Capacidad/día} = 360 \text{ MB/hora} * 12 \text{ horas}$$

$$\text{Capacidad/día} = 4,218 \text{ GB/día}$$

- Capacidad de almacenamiento total
- Grabación continua

*Capacidad total = Capacidad/día * núm días*

$$\text{Capacidad total} = 8,437 \text{ GB/día} * 14 \text{ días}$$

$$\text{Capacidad total} = 118,118 \text{ GB}$$

- Grabación programada

$$\text{Capacidad total} = \text{Capacidad/día} * \text{núm días}$$

$$\text{Capacidad total} = 4,218 \text{ GB/día} * 14 \text{ días}$$

$$\text{Capacidad total} = 59,052 \text{ GB}$$

Para los cálculos finales sobre la capacidad de almacenamiento se tomará e cuenta la siguiente tabla:

Cámara	# cámaras	Horas de grabación	MB / hora	GB / día	Días de grabación	TOTAL por cámara (GB)
Grabación continua	4	24	360	8,437	14	118,118
Grabación programada	5	12	360	4,218	14	59,052

Tabla 6.21. Cálculo para la capacidad de almacenamiento
Elaborado por: La Investigadora

- Capacidad de almacenamiento para todo el sistema

$$\text{Capacidad sistema} = \text{cap total grabación continua} * \text{núm cámarasc} + \text{cap total grabación programada} * \text{núm cámarasp}$$

$$\text{Capacidad sistema} = 118,118 \text{ GB} * 4 + 59,052 \text{ GB} * 5$$

$$\text{Capacidad sistema en TeraBytes} = 0,75 \text{ TB}$$

Donde:

cap total grabación continua es la Capacidad total de grabación continua

núm cámarasc es el Número de cámaras para grabación continua

cap total grabación programada es la Capacidad total de grabación programada

núm cámarasp es el Número de cámaras para grabación programada

Por el Sistema operativo y el software de gestión que se utilizarán, además del espacio libre la capacidad del sistema se le incrementará un 20% más al valor de *capacidad del sistema*.

$$\text{Capacidad del sistema} = 0,85 \text{ TB} \approx 1 \text{ TB}$$

6.8.6 Red WLAN

Descripción y funcionamiento del sistema.

El sistema estará compuesto de 9 cámaras IP inalámbricas (6 cámaras fijas y 3 PTZ), 2 *Radios Nano M5*, un switch Ethernet CISCO de la serie 2960 y un *equipo de monitoreo (computador personal)*.

El computador personal tendrá acceso directo a las cámaras mediante la red *wLAN* formada por los radios Nano y las cámaras IP, permitiendo el monitoreo de las áreas anteriormente mencionadas, el hardware de gestión se localizará en la *Administración de Redes y Sistemas informáticos*.

Las cámaras serán distribuidas de tal forma que tengan un buen campo de visualización, y que puedan conectarse a los *Radios Nano M5*, los cuales estarán ubicados estratégicamente para recibir la señal de las cámaras IP y conectarse mediante cable UTP (CAT 5E) a la red formada por el switch y el servidor de video.

El primer Radio Nano estará ubicado sobre la puerta del área de Administración de Redes, y se conectará a un puerto del dispositivo intermediario (switch Ethernet), al que también se conectará el servidor de video; el servidor se encargará de la gestión y control de las siguientes cámaras:

1. Cámara de acceso a las Oficinas, esta cámara está prevista para vigilar el ingreso a las oficinas de que se encuentran en el primer piso.
2. Cámara de acceso principal al edificio administrativo, permitiendo controlar el ingreso y salida del edificio, al igual que la cámara 6 con la

diferencia que será localizada para brindar mayor seguridad en la puerta de ingreso posterior del edificio principal.

3. Cámara de ingreso a las plantas superiores, esta cámara tiene el objetivo de monitorear el ingreso a las oficinas que se encuentran en los pisos dos y tres.

4. Cámara ubicada en la Secretaría de Subdecanato, teniendo como objetivo de monitorear el ingreso a las oficinas de que se encuentran en el segundo piso.

5. Cámara localizada en el área de Secretaría de Decanato, ubicada con el objetivo de monitorear el ingreso a las oficinas de que se encuentran en el tercer piso.

Las cámaras 7 y 8 serán ubicadas en el segundo piso del edificio principal de la FISEI, para el monitoreo de actividades de los pasillos cercanos al área de la Biblioteca y ágora de la facultad.

El segundo radio *NanoStation* se ubicará sobre la puerta del cuarto de equipos localizado en el primer piso, frente a la entrada del edificio secundario de la facultad, conectándose al cableado estructurado de la FISEI; controlando la cámara 9, la cual está situada en la entrada principal, para precautelar la seguridad de los y las estudiantes, profesores, laboratorios y equipos que reposan en las diferentes áreas que componen el nuevo edificio. Dicho radio se conectará a la red de Vigilancia IP por medio de la red de la FISEI, mediante el backbone de fibra óptica de la red de la FISEI.

6.9 Presupuesto

Se indicarán los costos de equipos necesarios para el sistema de vigilancia IP.

Descripción	Cantidad	P. Unitario	P. Total
Cámara DCS-3430	6	404,04	2.424,24
Cámara DCS-5635	3	881,44	2.644,32
Servidor HP ProLiant ML350 G6 serie SAS/SATA-SFF	1	3580	3.580,00
Radio NanoStation M5	2	259,1	518,20
Switch SD2005	1	70	70,00
Licencia Windows 2008 SERVER	1	950	950,00
UPS APC BE550G-LM (300W)	5	65	325,00
UPS APC SURTA2200XL (1600W)	1	1369,76	1.369,76
Costos de instalación y programación de cámaras	9	40	360,00
Costo de instalación y programación del servidor	1	150	150,00
SUBTOTAL			12.391,52
IMPREVISTOS (10%)			1.239,15
TOTAL			13.630,67

*Tabla 6.22. Presupuesto total
Elaborado por: La Investigadora*

6.10 Viabilidad de la propuesta

Para demostrar la viabilidad de la propuesta se realizará un Análisis de Costo-Beneficio, el cual implica comparar los costos económicos con la potencialidad de alcanzar eficientemente los objetivos del proyecto.

La falta de una vigilancia eficiente dentro de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, ha provocado que se susciten varios hechos que han afectado la imagen de la institución; como robo de equipos, daño a las instalaciones, y cierta sensación de inseguridad por parte de las y los estudiantes, docentes, personal administrativo, y personas que visitan la facultad.

Como solución al problema de seguridad y vigilancia se plantean dos propuestas:

- Seguridad brindada por un personal de vigilancia.
- Seguridad a través de un sistema de Video vigilancia inalámbrico.

Para demostrar la viabilidad de la propuesta se tomaron en cuenta los parámetros de coste de adquisición e instalación entre un sistema de video vigilancia basado en IP completamente digital (cámaras de red, infraestructura IP, servidor, software de gestión de vídeo y almacenamiento), con un sistema de vigilancia físico.

Actualmente la facultad cuenta con un sistema de vigilancia físico, compuesto por una persona que realiza rondas dentro y alrededor de la facultad, a determinadas horas del día y noche. Se debe tomar en cuenta que el personal de guardianía no es para vigilancia exclusiva de la seguridad de la facultad, y que no satisface las necesidades de seguridad y vigilancia que requieren las instalaciones y las personas que diariamente ingresan a la facultad. Razón por la cual se requiere un grupo de seguridad compuesto por tres personas, las cuales si pueden cubrir el área física que compone la facultad, previniendo varios incidentes como robos a estudiantes, robo de equipos informáticos, y seguridad en general.

El costo económico considerado por la contratación de cada persona es de \$300 (sueldo aproximado) mensuales, para el cálculo de gasto anual se tomará en cuenta una cantidad de \$600, como beneficios que un empleado debe recibir obligatoriamente, lo que nos dará un gasto de:

Sueldo mensual	Beneficios	Sueldo anual	
300,0	600,0	4.200,0	
<i>Sueldo anual para el personal de vigilancia</i>			12.600,0

Tabla 6.23. *Tabla de gastos para Vigilancia física*
Elaborado por: La Investigadora

También se debe considerar que se debe asignar un espacio físico para que el guardia pueda descansar o resguardarse, lo que implica un gasto extra. Lo que implica un gasto superior al de \$12.600,0.

Mientras que para la adquisición e implementación del sistema de Vigilancia IP se requiere un presupuesto de \$13.630,67. Dentro de lo concerniente al funcionamiento del sistema se deberán realizar los siguientes gastos económicos:

- En base al consumo eléctrico:

Equipos	Consumo de Watts	Cantidad de equipos	Consumo de Watts
Cámara fija	6,9	6	41,4
Cámara PTZ	11,0	3	33,1
Radios	8,0	2	16,0
Switch	6,0	1	6,0
Servidor	750,0	1	750,0
Pantalla	14,0	1	14,0
Total en kW:			0,9

Tabla 6.24. Tabla de gastos para Vigilancia IP
Elaborado por: La Investigadora

Con un costo de 0.20 ctvs. por kW/hora:

Total kW/hora	Total kW/día	Total kW/mes	Total kW/año + Mantenimiento
0,2	4,1	128,0	1.636,5

Tabla 6.25. Costo de funcionamiento del sistema de Vigilancia IP
Elaborado por: La Investigadora

Con un gasto anual de \$1.636,5 incluido gastos de funcionamiento y mantenimiento.

Cabe recalcar que el sistema de vigilancia IP ofrece ciertas ventajas, que ningún otro sistema podría superar, las cuales mencionan a continuación:

- El uso de tecnología IP ofrece prestaciones como: ahorro de energía, flexibilidad, uso de nuevos equipos, disminución de costos económicos, tecnologías amigables con el ambiente, plataformas de servidor, medios de transmisión con mayores tasas de transferencia, entre otros.

- Se puede aprovechar la infraestructura IP existente, eliminando así costos de cableado e instalación del sistema.

En base al análisis presentado desde el punto de vista de la investigadora, se puede determinar que el sistema de Video vigilancia IP inalámbrico es viable, porque es económico, cuenta con protecciones para su continuo funcionamiento, y presenta las siguientes características:

- Mejor calidad de imagen,
- Mejor mantenimiento y servicio,
- Aumento de la flexibilidad en todo el sistema.
- Usa el aire como medio de transmisión.

6.11 Conclusiones y Recomendaciones

Conclusiones

- Un sistema de Video vigilancia inalámbrico está compuesto de cámaras IP, un sistema de gestión de video y una red IP; los cuales forman una poderosa herramienta para la administración efectiva de la seguridad y vigilancia, con la finalidad de proteger al personal, equipamiento, información e instalaciones que conforman el edificio administrativo de la FISEI, y demás áreas que requieren una vigilancia y seguridad eficiente, dentro de la facultad.
- El uso de tecnología IP ofrece ventajas como: la gestión centralizada de las cámaras de red, e interacción remota con el sistema, todo esto en tiempo real.
- Los sistemas digitales hacen posible el uso de formatos de compresión que disminuyen los requerimientos de ancho de banda, en cuanto a transmisión y almacenamiento, sin dejar de lado la calidad de la señal.

- La aplicación de sistemas inalámbricos proporciona un mejor despliegue en exteriores e interiores, y costes inferiores en comparación con sistemas que utilizan medios guiados para la transferencia de información.
- El empleo de equipos con estándares abiertos, facilita la compatibilidad entre diferentes proveedores en base a la funcionalidad, características y costos.
- El criterio de selección de dispositivos activos necesarios para el sistema se basó en la interoperabilidad entre dispositivos, permitiendo una fácil administración, gestión y funcionamiento de todos los equipos que componen el sistema de video vigilancia.

Recomendaciones

- Se recomienda realizar un sobredimensionamiento de la red, para ampliaciones futuras y aumento de equipos, para que no afecte el ancho de la red ya existente.
- Es recomendable implementar políticas de seguridad para contraseñas, niveles de acceso y administración, que permitan el acceso al sistema, y a la información almacenada.
- Se deberá realizar un mantenimiento preventivo de los componentes del sistema, para que funcionen óptimamente, y evitar el deterioro de los mismos.
- La administración del Sistema de Video vigilancia inalámbrico deberá ser realizado por una persona, o personal con conocimiento sobre el funcionamiento de los equipos y el tipo de tecnología que se está utilizando.

BIBLIOGRAFÍA

- CACHIGUANGO, Yuri. *Diseño de una red de Video Vigilancia local y remota sobre IP en tiempo real para una Hostería aplicando el concepto de GEEN IT*. 2010.
- Datos oficiales del INEC. Censo del 28 de Noviembre de 2010
- FERNÁNDEZ, Eduardo. *Wi-Fi: nuevos estándares en evolución*. Centro de Difusión de Tecnologías ETSIT-UPM. Publicado en enero del 2007.
- KEAGY, Scott. *Integración de redes de voz y datos*. Primera edición, Madrid, España. Cisco System Inc. 2001.
- PALLO, Juan P. *Comunicaciones Ópticas*. 2010.
- ROLDAN, David. *Comunicaciones Inalámbricas*. Primera edición. Alfaomega grupo editor. Madrid. 2005.
- TOMASI, Wayne. *Sistemas de Comunicaciones Electrónicas*. Primera edición. España. Editorial Prentice Hall. 1996.

LINKOGRAFÍA

- APC. <http://www.apc.com>
- AXIS Communications. *Vigilancia IP Inalámbrica para aplicaciones de seguridad*. Publicado en 2003. <http://www.axis.com>
- CONSTITUCIÓN DEL ECUADOR. http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf
- D-Link. http://www.dlinkla.com/home/productos/familia.jsp?id_fam=9
- FULUSHIMA, Sergio. *Video en red*. http://www.rnds.com.ar/articulos/059/Cap_01.pdf
- Hewlett-Packard Development Company, L.P. *Guía de Configuración Servidores ProLiant y StorageWorks para América Latina*. 2009.

- *Medios de transmisión.* www.wiener.edu.pe/manuales2/4to-ciclo/...1/Manual-Redes.pdf
- Ministerio de Coordinación de Seguridad, www.micsie.gov.ec
- *Niveles de seguridad,*
<http://www.slideshare.net/eventoscreativos/esquema-nacional-de-seguridad-4812979>
- PALACIOS, Kleber. *Estudio Y Diseño De Un Sistema De Vigilancia Y Monitoreo De Video En Tiempo Real, Sobre Una Red IP, Para Un Terminal De Despacho Y Bombeo De Combustible De La Gerencia Regional Sur De Petrocomercial.* Publicado en 2006.
<http://www.dspace.espol.edu.ec/handle/123456789/3075>
- *¿Qué es Seguridad electrónica?*
<http://www.slideshare.net/martinn2/que-es-seguridad-electrnica>
- SANDOVAL, Francisco. *Regulaciones para la utilización de Videocámaras para Video Vigilancia en lugares públicos en Ecuador.* Publicado en 2007. <http://fralbe.com/2010/09/regulaciones-para-la-utilizacion-de-videocamaras-para-video-vigilancia-en-lugares-publicos-en-ecuador>
- *Sistemas de Video Vigilancia.*
http://www.superinventos.com/Sistemas_Videovigilancia.htm
- Telecomunicaciones. <http://www.universidades-rusia.com/latinoamerica/paginasbody/orivocacional/telecomu.htm>
- UBIQUITI NETWORKS. <http://www.ubnt.com/nanostationm>
- VELLACOTT, Oliver. *¿Por qué usar video IP?*
www.rnds.com.ar
- *802.11: Wireless LANs.*
<http://standards.ieee.org/about/get/802/802.11.html>

GLOSARIO DE TÉRMINOS:

- Ancho de banda: Rango de frecuencias que emplea un medio de transmisión sin distorsión.
- Ángulo de visión: Ángulo de la escena que el lente de una cámara de video puede mostrar en un monitor, como el ángulo diagonal, ángulo horizontal y ángulo vertical, están descritos en grados.
- Bps: Bits por segundo, es un indicador de la velocidad de transmisión a través de un sistema.
- Broadcast: Paquete de datos enviado a todos los nodos que conforman una red.
- Cámara: Dispositivo electrónico que captura video en tiempo real.
- Códec: Algoritmo o programa informático para reducir el tamaño de archivos y programas grandes.
- Compresión: Reducir y eliminar datos redundantes del video para que el archivo de video digital se pueda enviar por la red y ser almacenado.
- Contraluz: Vista o aspecto de las cosas cuando se miran desde el lado opuesto a aquel por el que están iluminadas.
- Convergencia: Combinar diferentes servicios sobre una plataforma IP.
- Encriptación: Proceso que convertir la información a un formato ilegible.
- Escalabilidad: Característica de ampliación de un sistema, para incrementar nuevos equipos.
- Estándar: es un documento técnico, con especificaciones técnicas las cuales permiten la compatibilidad entre dispositivos y sistemas de diferentes fabricantes.
- Fast Ethernet: Estándar de Ethernet que provee una velocidad de transmisión de 100 Mbps.
- Fotograma: o frame, imagen de video completa.
- FPS: Frame por segundo, unidad de velocidad de fotogramas utilizada para describir la frecuencia de actualización de una secuencia de video en una unidad de tiempo.

- Gestión de video: Visualización, grabación, reproducción y almacenamiento del video.
- Hangar: Lugar utilizado para guardar aeronaves.
- IEEE: es una organización internacional dedicada a la estandarización, publica revistas técnicas, es patrocinador de conferencias, desarrolla estándares de la tecnología y apoya los intereses profesionales de más de 400.000 miembros.
- Interconexión: Vinculación de recursos físicos y soportes lógicos, para permitir el funcionamiento de una red de datos.
- Latencia: Retardo entre el momento en que un dispositivo solicita acceso a una red, y el momento en que se le concede permiso para transmitir; en otras palabras es el intervalo de tiempo que toma el procesamiento de una tarea.
- Longitud focal: Determina el campo de visualización horizontal a una distancia específica.
- Lúx: Unidad de iluminación.
- Modelo OSI: modelo de referencia de Internetwork, usado para el diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas.
- Modelo TCP/IP: es un modelo de protocolo, que describe las funciones que ocurren en capa de protocolos.
- Monitorización: Visualización del video para control.
- Nitidez: Control de la precisión de los detalles de una imagen.
- NTSC: Comité Nacional de Sistemas de Televisión, sistema de codificación de colores analógico.
- Objetivo de una cámara: Determina el campo de visión.
- PAL: Línea de Alternancia de Fase.
- Píxel: Puntos de color que forma parte de una imagen digital.

- Red Híbrida: Combinación entre una red alámbrica y una red inalámbrica.
- Resolución: Calidad, nitidez, y detalle de la imagen.
- Sensor: Sensor de imagen de video.
- Servidor: es un ordenador que presenta más características que un ordenador normal, además ejecuta ciertos programas, los cuales proveen servicios a los denominados clientes.
- Software de gestión: Software que administra los recursos de un sistema de Video vigilancia IP, así como a visualizar le video captado por las cámaras.
- STP: Cable de par trenzado apantallado, medio guiado para la transmisión de información dentro de una red de datos.
- Streaming: Tecnología que permite transmitir audio y video eficientemente, a través de la red sin necesidad de descargar los archivos por el usuario.
- Topología: Nivel al que están conectados los dispositivos a la red.
- Transferencia: Envío de video desde la cámara hacia el software de gestión.
- UTP: Cable par trenzado no apantallado, medio guiado para la transmisión de información.
- Video inteligente: Convierte los datos de las secuencia de video en información procesable.
- Vigilancia IP: o Video vigilancia es un sistema que brinda vigilancia por medio de transmisiones telemáticas de video y audio, hacia un centro de gestión y administración.

ACRÓNIMOS:

- AP: Punto de Acceso.
- BSS: Conjunto de Servicios Básicos.
- CCD: Dispositivo de Carga Acoplada.
- CDV: Campo de Visión
- CMOS: Semiconductor de Óxido Metálico Complementario.
- FPS: Frame por segundo
- HDTV: Resolución de televisión de alta definición.
- IEEE: Instituto de Ingenieros Eléctricos y Electrónicos.
- M-JPEG: Grupo Conjunto de Expertos en Fotografía en movimiento
- M-PEG: Grupo de Expertos en Imágenes en movimiento.
- MPEG-1: Grupo de Expertos en Imágenes en movimiento versión 1.
- MPEG-2: Grupo de Expertos en Imágenes en movimiento versión 2.
- NTICS: Nuevas Tecnologías de Información y Comunicación.
- NTSC: Comité Nacional de Sistemas de Televisión.
- NVR: Grabadora de Video en Red.
- OSI: Organización Internacional para la Estandarización.
- PAL: Línea de Alternancia de Fase.
- PoE: Alimentación a través de Ethernet.
- PTM: Punto Multi Punto
- PTZ: Pan/Tilt/Zoom.
- TCP/IP: Protocolo de Control de Transmisión/Protocolo de Internet.

- VGA: Tabla de Gráficos de Video.
- VLSM: Máscara de Subred de Longitud Variable.
- WAP: Protocolos de aplicaciones inalámbricas.
- WEP: Privacidad Equivalente al Cableado.

ANEXOS

ANEXOS 1

ENCUESTA Y FICHA DE OBSERVACIÓN

ANEXO 2

DESCRIPCION TÉCNICA DE LA CÁMARA FIJA DCS-3430

ANEXO 3

DESCRIPCION TÉCNICA DE LA CÁMARA PTZ DCS-5635

ANEXO 4

DESCRIPCION TÉCNICA DEL SERVIDOR

HP PROLIANT ML350 G6 SERIE SAS/SATA-SFF

ANEXO 5

DESCRIPCION TÉCNICA DEL SOFTWARE DE GESTIÓN DE VIDEO

D-VIEWCAM

ANEXO 6

DESCRIPCION TÉCNICA DEL EQUIPO NANOSTATION M5

ANEXO 7

DESCRIPCION TÉCNICA DEL SWITCH SD2005

ANEXO 8

DESCRIPCION TÉCNICA DE UPS

ANEXO 9

PROTOTIPO DEL SISTEMA DE VIGILANCIA IP

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL (FISEI)

Encuesta dirigida para los empleados del área administrativa de la FACULTAD DE INGENIERIA EN SISTEMAS, ELECTRONICA E INDUSTRIAL de la UNIVERSIDAD TÉCNICA DE AMBATO.

OBJETIVO: Recolectar información sobre la actual condición de los niveles de seguridad del edificio administrativo de la FISEI.

INSTRUCTIVO:

- Procure ser lo más objetivo y veras
- Marque con una X en el paréntesis la alternativa que usted eligió.

1. **¿Cree usted que el sistema de vigilancia actual del edificio administrativo es eficiente?**
Si () No ()
2. **¿Se han suscitado hechos delictivos o pérdida de información en el área administrativa?**
Si () No ()
3. **¿Es necesario el diseño de un sistema de vigilancia electrónica para mejorar los niveles de seguridad?**
Si () No ()
4. **¿Cree que existen las suficientes seguridades para el acceso al área de oficinas de autoridades y personal administrativo?**
Si () No ()
5. **¿Existen planes para evitar posibles contingencias al recurso humano y de trabajo?**
Si () No ()
6. **¿Qué beneficios se conseguirán con un sistema de video vigilancia inalámbrica?**
Control de personas particulares al área ()
Monitoreo remoto ()
Disminución de la percepción de inseguridad por parte del recurso administrativo ()
Todas las anteriores ()

¡Agradecemos su colaboración!

Ficha de Observación: Área Administrativa de la FISEI

Luego de la observación respectiva se ubicará la apreciación que sobre el objeto observado, utilizando la siguiente escala de valoración.

1	2	N
Sí	No	No es posible observar

Observación	ESCALA		
	1	2	N
Sobre la tecnología			
¿El edificio administrativo de la FISEI cuenta con tecnología IP?			
¿La tecnología actualmente implementada permite la escalabilidad de nuevos sistemas?			
¿Se cuenta con personal que administre dicha tecnología adecuadamente?			

**WIRELESS N DAY & NIGHT NETWORK CAMERA WITH 3G
MOBILE VIDEO SUPPORT****DCS-3430****24-HOUR
SURVEILLANCE**

A CMOS sensor with low lux sensitivity produces high-quality images under varied lighting conditions.

**TRIPLE CODEC &
MULTIPLE PROFILES**

Optimized image quality and bandwidth efficiency with separate profiles for web viewing, 3G mobile viewing, and recording.

**WIRELESS
CONNECTIVITY**

Can be accessed anytime, anywhere over a wireless 802.11b/g/n network.

The DCS-3430 is a wireless day & night camera, equipped with a CMOS sensor to deliver exceptional picture quality under varied lighting conditions. The camera can be placed anywhere on the network either through a wired Ethernet or wireless 802.11 b/g/n connection. The DCS-3430 features digital input/output connectors making it possible to connect sensors and alarms with this camera and comes with a RS-485 interface, for controlling an optional pan/tilt device, over an IP network. The camera is housed in an aluminum casing for maximum heat dissipation and protection against tampering.

KEY FEATURES

- View live video streams from a 3G mobile phone or PDA.
- Simultaneous Motion JPEG and MPEG-4, H.264 streaming for optimized image quality and bandwidth-efficiency.
- Simultaneous profile support: web viewing, 3G mobile viewing, and video recording.
- RS-485 support for an external PT device.
- Low light recording and 16X digital zoom.
- BNC connector to integrate the network camera into a CCTV network.
- Digital I/O support for sensors and alarms.
- 12V 200 mA DC power output for LED lens.
- Optional Auto-iris lens or IR LED lens for low light or night vision.
- Save snapshots/video clips to local hard drive via web browser or to NAS or SD card.

SURVEILLANCE SOFTWARE

D-ViewCam software is included to manage up to 32 cameras simultaneously, send automated e-mail alerts, and record video to your hard drive when motion is detected or according to a set schedule.

CAMERA SPECIFICATIONS

- Built-in 1/4" CMOS sensor
- Built-in IR-cut Removable Filter
- Minimum Illumination: 0.5 lux @ F1.8;
- 0 lux (10 meter range with optical IR lens)
- CS mount lens: 6 mm, F1.8
- Resolution: 640 x 480
- Electronic Shutter:
 - NTSC: 1/60~1/100,000 sec.
 - PAL: 1/50~1/110,000 sec.
- Lens mount support: Auto-iris or IR lens (10 meter range)
- Field of view: 51° diagonal, 31° vertical, 41° horizontal

LED INDICATORS

- Link & Activity
- Power

RESET BUTTON

- Reset to factory default settings

EXTERNAL DEVICE INTERFACE

- 2 Inputs:
 - Photo Relay
 - Active High 12V, +/-3 V, Dropout: 0V DC
- 1 Output:
 - Photo Relay
 - Open circuit voltage: 240VAC or 350VDC
 - Power output: 12 V DC 200 mA
- RS-485 connector for external PT devices

MEMORY

- SDRAM: 64 MBytes
- Flash Memory: 8 MBytes

VIDEO FEATURES

- Adjustable image size, quality and bit rate
- Time stamp and text overlays
- Motion adaptive de-interlacing

VIDEO RESOLUTION

- NTSC/PAL support:
 - Up to 30 frames at 640 x 480
 - Up to 30 frames at 320 x 240
 - Up to 30 frames at 160 x 120
- For BNC TV out:
 - NTSC: 720 x 480
 - PAL: 720 x 576

VIDEO ALGORITHM SUPPORT

- JPEG for still images
- MJPEG/MPEG4/H.264 multi-profile compression
- Supports up to 4 video profiles simultaneously
- Supports 3GPP mobile surveillance

DIGITAL ZOOM

- 16X

MICROPHONE

- Omni-directional
- S/N ratio: over 58 dB

AUDIO

- Sampling Rate:
 - GSM-AMR: 12.2 Kbps
 - PCM: 8 Kbps
- Full-duplex audio communication

NETWORK CONNECTIVITY

- 10/100 Mbps Fast Ethernet Auto-negotiation
- Frequency Range and Channels
 - 2.412-2.4835 GHz
 - 3 Channels (depends on Area)
- Transmission: 2TX, 2RX
- Data Rate:
 - IEEE 802.11n: From MCS0 to MCS15
 - IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps
 - IEEE 802.11b: 11, 5.5, 2, 1 Mbps
 - Auto-select or manual
- Output Power:
 - 12 dBm@11n
 - 12 dBm@11g
 - 16 dBm@11b
- Sensitivity:
 - 802.11n: -66 dBm
 - 802.11g: -66 dBm
 - 802.11b: -82 dBm
- Antenna:
 - Connector: MHF
 - Operating Frequency: 2.4 Ghz
- Security:
 - WEP/WPA-PSK/WPA 2

NETWORK INTERFACE

- IEEE 802.3/802.3u 10/100BASE-TX Ethernet port
- Supports full-duplex operations
- Supports 802.3x Flow Control in full-duplex mode
- NETWORK PROTOCOL SUPPORT
 - IPv4, ARP, TCP/IP, UDP, RTSP, RTP, RTCP, HTTP, SMTP, FTP, NTP, DNS, DHCP, UPnP, DDNS, PPPoE, Samba Client, 3GPP

REMOTE MANAGEMENT

- Configuration accessible via web browser
- Take snapshots/video clips and save to local hard drive via web browser or to NAS or SD card

SECURITY

- Administrator and user group protected
- Password authentication

D-ViewCam SOFTWARE FUNCTIONS

- Remote management/control of up to 32 cameras
- Viewing of up to 32 cameras on one screen
- Management functions are provided in the web interface
- Scheduled, motion triggered, or manual recording options

SYSTEM REQUIREMENTS

- Operating System: Microsoft XP, Vista, Windows 7
- Browser: Internet Explorer, Firefox, Mozilla or Opera
- 3GPP Mobile Phone

POWER INPUT

100-240 V AC, 50/60 Hz, 0.4 A

POWER OUTPUT

12 V DC, 1.25 A

POWER CONSUMPTION

6.9 watts maximum

POWER SUPPLY

External AC to DC switching power adapter

DIMENSIONS (LxWxH)

177 x 78 x 60 mm

WEIGHT

577.8 grams

OPERATION TEMPERATURE

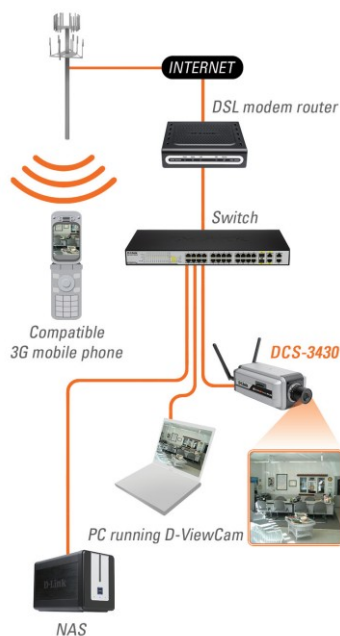
0° to 40° C (32° to 104° F)

STORAGE TEMPERATURE

-20° to 70° C (-4° to 158° F)

HUMIDITY

20% to 80% non-condensing



Wireless N H.264 PTZ Network Camera**DCS-5635****VERSATILE IMAGING**

Capture as much action as possible thanks to pan/tilt and 10x optical zoom

CONVENIENT REMOTE MONITORING

Multiple codecs allow you to configure a video stream compatible with your computer or 3G mobile device.

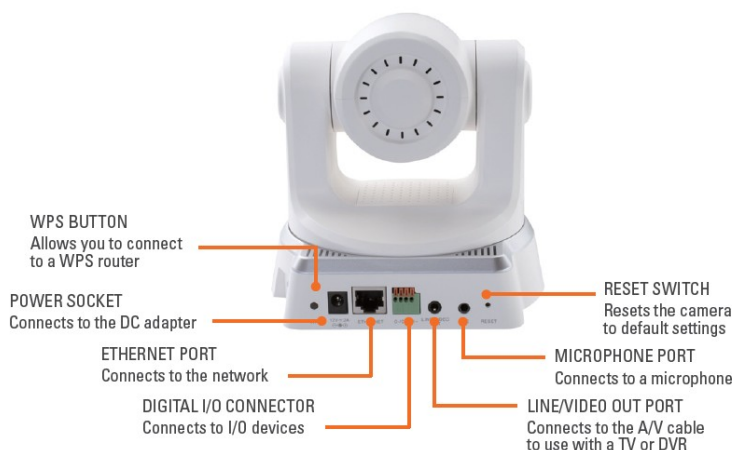
MAXIMIZED EFFICIENCY

The H.264 codec uses significantly less bandwidth relative to earlier video compression technologies

The DCS-5605/DCS-5635 is a professional IP surveillance solution which connects to your network to provide high-quality live video over the Internet. The camera apparatus supports precise high-speed pan/tilt/zoom functionality for extensive monitoring and object tracking.

KEY FEATURES

- Multiple H.264 streams
- Pan and tilt camera with 10x optical zoom and auto focus
- Micro SD card slot for local storage
- 3GPP mobile surveillance
- 802.11n wireless connectivity
- WPS support

TECHNICAL SPECIFICATIONS

WIRELESS N H.264 PTZ NETWORK CAMERA
DCS-5605/DCS-5635

CAMERA SPECIFICATIONS

- Image Sensor: 1/4-inch Color CCD Sensor, De-Interlace Scan Mode
- Lens Type: 10x Optical Zoom Fixed Lens
- Digital Zoom: 16x
- Electronic Shutter:
 - NTSC: 1/60~1/120,000 sec.
 - PAL: 1/50~1/120,000 sec.
- Minimum Illumination:
 - Color: 0.7 Lux / F1.8
 - B/W: 0.02 Lux / F1.8
- Pan angle: +/- 165 degrees
- Tilt angle: -87 to +34 degrees
- Lens mount support: Auto-iris or IR lens (10 meter range)
- Field of view: 63° diagonal, 40° vertical, 51° horizontal

LED INDICATORS

- Link/Power/WPS

WIRELESS

- Security: WEP, WPA-PSK, WPA2
- Supports WPS
- Transmit ion: 2TX, 2RX
- Data Rate:
 - IEEE802.11n: From MCS0 to MCS15
 - IEEE802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps
 - IEEE802.11b: 11, 5.5, 2, 1 Mbps
 - Auto-select or manual
- Output Power
 - 12 dBm@11n/11g
 - 16 dBm@11b
- Sensitivity
 - 802.11n: -66 dBm
 - 802.11g: -66 dBm
 - 802.11b: -82 dBm
- Antenna
 - Connector: MHF
 - Operating Frequency: 2.4Ghz

AUDIO

- Two-way audio
- External audio in
- External audio out
- GSM-AMR: 12.2kbps, PCM: 8Kbps

MICROPHONE

- Omni-directional
- S/N ratio: over 58 dB

PROTOCOLS

- IPv4, ARP, TCP, UDP, ICMP, DHCP Client, NTP Client (D-Link), DNSClient, DDNSClient (D-Link), SMTP Client, FTP

Client, HTTP Server, Samba Client, PPPoE, UpnP Port Forwarding, RTP, RTSP, RTCP, 3GPP

VIDEO RESOLUTION

- NTSC: 704x480 / 352x240 / 176x120 : 30 fps
- PAL: 704x576 / 352x288 / 176x144 : 25 fps

CODEC SUPPORT

- MPEG4/MJPEG/H.264 (simultaneous)
- JPEG for still image

INTERFACES

- LAN, Microphone, I/O, Line/ Video Out, MicroSD, WPS, Reset

DATA RATES

- IEEE 802.11n: From MCS0 to MCS15
- IEEE 802.11g: 54 - 6 Mbps
- IEEE 802.11b: 11, 5.5, 2, 1 Mbps
- Auto-select or manual

POWER

12 V DC, 2 A

POWER CONSUMPTION

100-240 VAC, 50/60 Hz, 0.4 A

SYSTEM REQUIREMENTS

- Operating System: Microsoft XP, Vista, Windows 7
- Browser: Internet Explorer, Firefox, Mozilla or Opera
- 3GPP Mobile Phone

DIMENSIONS (LxWxH)

140.3 x 136.1 x 140.1 mm

WEIGHT

855 grams

OPERATION TEMPERATURE

0° to 40° C (32° to 104° F)

STORAGE TEMPERATURE

-20° to 70° C (-4° to 158° F)

D-ViewCam SOFTWARE FUNCTIONS

- Remote management/control of up to 32 cameras
- Viewing of up to 32 cameras on one screen
- Management functions are provided in the web interface
- Scheduled, motion triggered, or manual recording options.

WIRELESS N H.264 PTZ NETWORK CAMERA
DCS-5605/DCS-5635

SERVIDOR ML350G6 SIX CORE



Product Specifications	
Manufactured	HP
Manufactured part#	638181-001
Product description	ML350T06 E5645 SFF BASE US SVR
Type	SERVER
Form factor	TOWER 5U
Approximate dimensions (WxDxH)	8.6 IN X 23.5 IN X 18.5 IN
Approximate weight	54 LBS
Localization	UNITED STATES
Server scalability	2-WAY
Processor	1 X INTEL XEON E5645/2.4 GHZ (6-CORE)
Processor main features	HYPER THREADING TECHNOLOGY, INTEL TURBO BOOST TECHNOLOGY
Cache memory	12 MB L3 CACHE
Cache per processor	12 MB
RAM	6 GB (INSTALLED)/288 GB (MAX)-DDR3 SDRAM ADVANCED ECC-1333 MHZ-PC3 10600
Storage controller	RAID (SERIAL ATA-300/SAS 2.0) PCI EXPRESS 2.0 X4
Server storage bays	HOT-SWAP 2.5"
Hard drive	2 DISCOS HP 500 GB 6G SAS 7.2K 2.5 IN DP MDL
Optical storage	DVD-ROM
Graphics controller	ATI ES1000
Video memory	64 MB
Networking	NETWORK ADAPTER-PCI EXPRESS X4-ETHERNET FAST ETHERNET, GIGABIT ETHERNET-ETHERNET PORTS: 2XGIGABIT ETH
Power	AC 120/230V (50/60 HZ)
Power redundancy	FUENTE REDUNDANTE HP 750 WCS GOLD Ht Plg Pwr Supply Kit
Monitor	HP de 17"

D-ViewCam 3.0 IP Camera Surveillance Software



D-ViewCam 3.0 IP camera surveillance software is a comprehensive surveillance system designed to centrally manage multiple IP cameras for Home, Small Office and Home Office (SOHO), or Small and Medium Business (SMB) users. Supporting up to 32 IP cameras, D-ViewCam 3.0 is compatible with all current D-Link IP cameras, Video Servers and offers digital monitoring and recording capabilities of video, audio, and events for various security applications. This software provides users with a wide array of features for added convenience, including video recording, playback, video live view, offering users a powerful surveillance software that's easy to use.

Features

- Support to manage up to 32 IP cameras
- Megapixel IP cameras support
- Multilingual support
- H.264, MPEG-4, MJPEG video formats support
- Monitor cameras via e-Map or video mode
- Open playback window/remote playback server to view historical videos
- Record and live display at different frame rates and resolution
- Pan, tilt, zoom, and focus functions to control movement of P/T/Z capable cameras
- Event e-mail notification
- Screen division layout
- Adjustable pan and tilt speed
- Automatically patrols selected vicinity preset by user
- Capture images directly from live video with snapshot
- Locate important events in recorded video using a motion histogram
- Move P/T/Z camera orientation by clicking the video viewing window
- Start a conversation with 2-way audio
- The data streaming bandwidth of each remote client connection can be monitored and blocked
- Reconstruct, repair or relocate the recordings in local drive, external drive or network drive
- Search for recorded files by date, time, and event
- Control video speed in both Video and Event playback
- Event action relay to camera and I/O device
- Automatic camera model detection

TECHNICAL SPECIFICATIONS

GENERAL

- Supports up to 32 cameras
- Megapixel IP camera support
- MJPEG/MPEG-4/H.264 compression format support
- Multilingual support
- OSD (on screen display) setting support
- Live Monitoring
- 30 FPS maximum recording per camera (subject to camera and video server capacity)
- Automatic camera model detection
- E-mail notification to address book
- Lock system to avoid abnormal change

SYSTEM USER MANAGEMENT

- User validation
- User password restriction
- User profiling
- Access privilege control

RECORDING

- Multiple storage locations support
- Record by schedule
- Record by event
- Pre-record/Post-record support
- Manual recording with up to 32 channel support
- Support single way audio record of multiple channels
- Record and live display at different frame rates and resolution

DATA SEARCH AND PLAYBACK

- Video playback control
- Histogram quick search for video
- Video Stamp
- Video extract by snapshot or by VI/ASF
- Support remote playback/web playback to play historical videos

VIDEO MODE

- Screen division layout support
- Monitor display by video drag and drop
- Support full screen to display videos
- Information windows support
- Enable move function to control P/T/Z camera

- Digital zoom in/out support
- Support remote livewer/web live viewer to display videos

MAP MODE

- Multiple map support
- Alarm notification
- Customized map background support
- Camera preview
- Camera and I/O indicator

P/T/Z CONTROL

- Manual control
- Preset positions (device dependent)
- Preset patrolling
- Multiple patrol group support

I/O FEATURE

- Output port control
- Input port trigger on event
- Output port relay when event detected



Video Mode Display (16 camera view)

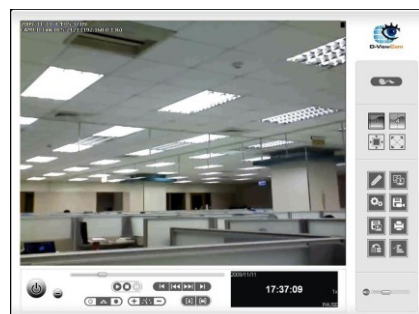


ILLUSTRATION OF NETWORK SETUP USING D-VIEWCAM 3.0

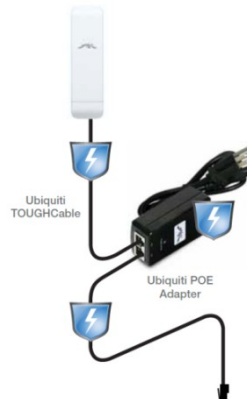


RADIO NANOSTATIONM5

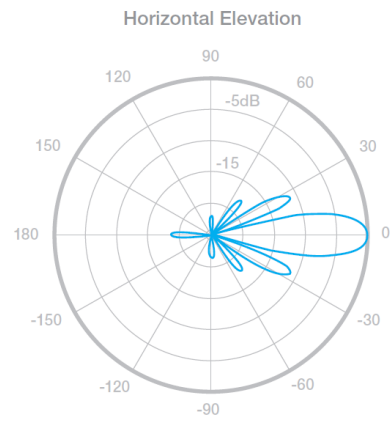
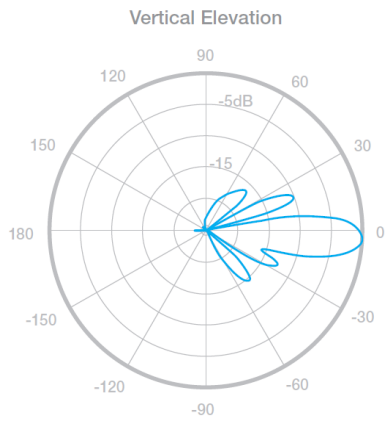
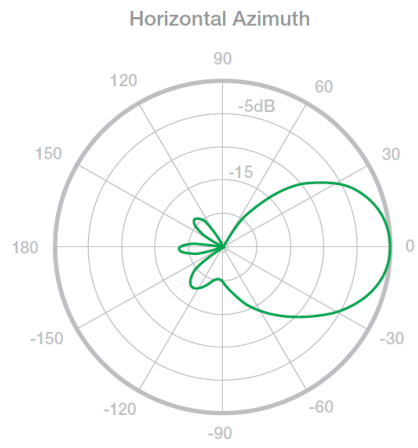
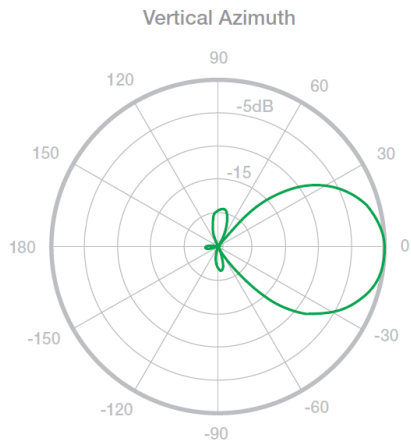


System Information	
Memory Information	32MB SDRAM, 8MB Flash
Networking Interface	2 X 10/100 BASE-TX (Cat. 5, RJ-45) ETH
Regulatory / Compliance Information	
Wireless Approvals	FCC Part 90Z
RoHS Compliance	YES
Physical / Electrical / Environmental / Antenna	
Enclosure Characteristics	Outdoor UV Stabilized Plastic
Mounting Kit	Pole Mounting Kit included
Power Method	Passive Power over Ethernet
Operating Temperature	-30C to 75C
Dimensions	294 x 31 x 80 mm
Weight	0.4 kg
Power Supply (included)	24V, 0.5A POE
Max Power Consumption	8 Watts
Antenna Gain	16 dBi
Polarization	Dual Linear
Operating Frequency Summary (MHz)	5470-5825 MHz
Antenna Information	
Gain	14.6 - 16.1 dBi
Max VSWR	1.6:1
Beamwidth	43° (H-pol) / 41° (V-pol) / 15° (Elevation)

Forma de conexión:



Los patrones de radiación son los siguientes:



CISCO SD2005 5-PORT GIGABIT SWITCH



Specifications	
Standards	IEEE 802.3, 802.3u, 802.3x, 802.3ab
Ports	5 RJ-45 10/100/1000 Mbps ports
Cabling type	Category 5 Ethernet
LEDs	System, 1 through 5
Security feature	Security slot
Dimensions (WxHxD)	140 x 33 x 140 mm
Unit weight	0.94 lb
Power	DC 12V/0.5A
Operating temperature	32° to 104°F (0° to 40°C)
Package Contents	Cisco SD2005 5-Port 10/100/1000 Gigabit Switch
	Power adapter
	Quick Start Guide

APC Back-UPS 550VA, 8 outlet, 120V LAM BE550G-LM



Incluye: DC con software, Cable USB, Manual del usuario

Salida

Capacidad de Potencia de Salida: 330 Vatios / 550 VA

Máxima potencia configurable: 330 Vatios / 550 VA

Tensión de salida nominal: 120V

Frecuencia de salida (sincronizada a red eléctrica principal): 47 - 63 Hz

Tipo de forma de onda: Aproximación acompasada de una onda sinusoidal

Conexiones de salida

4) NEMA 5-15R (Respaldo de batería)

4) NEMA 5-15R (Protección contra sobretensiones)

Entrada

Entrada de voltaje: 120V

Frecuencia de entrada: 50/60 Hz +/- 3 Hz (autosensible)

Tipo de enchufe : NEMA 5-15P

Longitud del cable: 1.52 metros

Baterías y autonomía

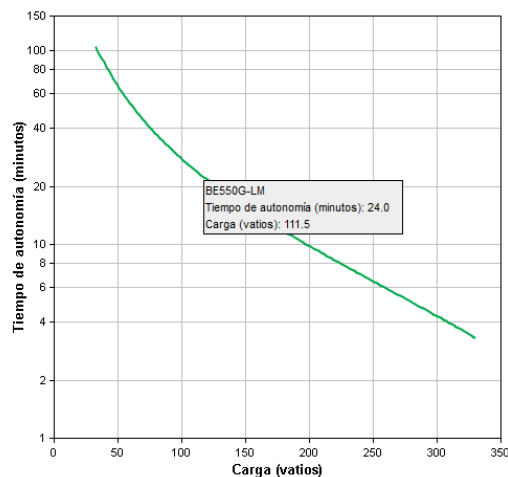
Tipo de batería: Batería sellada de plomo sin necesidad de mantención con electrolito suspendido: a prueba de filtración

Tiempo típico de recarga: 24 hora(s)

Cartucho de repuesto de batería: APCRBC110

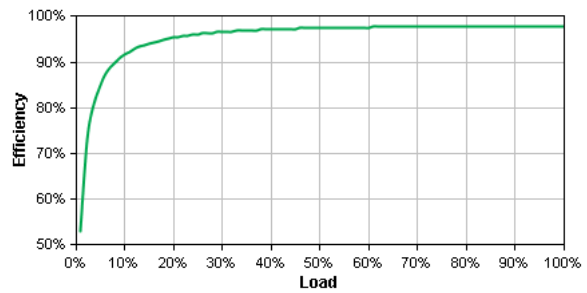
Cantidad de cartuchos de batería de recambio: 1

Gráfico de autonomía:



Uso de energía / eficiencia

Load	Efficiency
25%	96.1%
50%	97.5%
75%	97.8%
100%	97.7%



Comunicaciones y manejo

Puerto de interfaz: USB

Panel de control: Visualizador de estatus LED en línea, Batería en actividad

Alarma audible

Físico

Dimensiones de altura máxima: 88.00 mm

Dimensiones de anchura máxima: 180.00 mm

Dimensiones de profundidad máxima: 302.00 mm

Peso neto: 5.50 KG

Color: Negro

Ambiental

Ambiente operativo: 0 - 40 °C

Elevación de operación: 0-3000 metros

Ruido audible a 1 metro de la superficie de la unidad: 45.00 dBA

APC SMART-UPS RT 2200VA 120V SURTA2200XL



Incluye: DC con software, CD de documentación, Guía de instalación, Cable RS-232 de señalización Smart del UPS, Cable USB, Manual del usuario

Salida

Capacidad de Potencia de Salida: 1600 Vatios / 2200 VA

Máxima potencia configurable: 1600 Vatios / 2200 VA

Tensión de salida nominal: 120V

Frecuencia de salida: 50/60 Hz +/- 3 Hz ajustable por el usuario +/- 0,1

Factor de cresta: 3:1

Tipo de forma de onda: Onda senoidal

Conexiones de salida: (6) NEMA 5-15R

Entrada

Entrada de voltaje: 120V

Frecuencia de entrada: 50/60 Hz +/- 5 Hz (autosensible)

Tipo de enchufe : NEMA 5-20P

Longitud del cable: 1.83 metros

Baterías y autonomía

Tipo de batería: Batería sellada de plomo

Baterías pre-instaladas: 1

Tiempo típico de recarga: 3 hora(s)

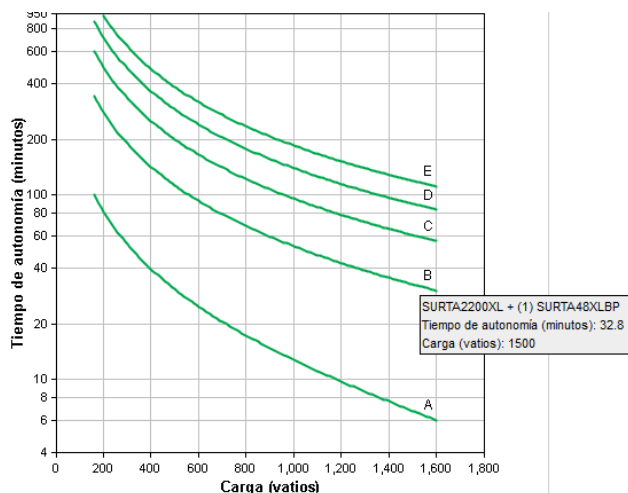
Cartucho de repuesto de batería: RBC57

Cantidad de cartuchos de batería de recambio: 1

Opciones de funcionamiento extendido para APC SMART-UPS RT 2200VA 120V

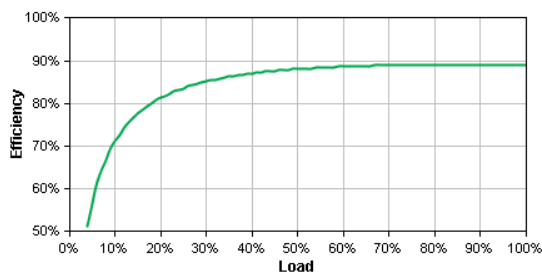
Gráfico de autonomía:

Curve	Part Number(s)
A	SURTA2200XL
B	SURTA2200XL + (1)SURTA48XLBP
C	SURTA2200XL + (2)SURTA48XLBP
D	SURTA2200XL + (3)SURTA48XLBP
E	SURTA2200XL + (4)SURTA48XLBP



Uso de energía / eficiencia

Load	Efficiency
25%	83.6%
50%	88.1%
75%	89.1%
100%	89.1%



Comunicaciones y manejo

Puerto de interfaz: DB-9 RS-232, SmartSlot, USB

Cantidad de interfaces SmartSlot™: 1

Panel de control: Visualizador de estatus LED con barras gráficas de carga y batería e indicadores de red Alarma audible

Interruptor de emergencia (EPO): Sí

Físico

Dimensiones de altura máxima: 85.00 mm

máxima: 432.00 mm

Dimensiones de profundidad máxima: 559.00 mm

Peso neto: 27.50 KG

Dimensiones de anchura

Altura del rack: 2U

Color: Negro

Ambiental

Ambiente operativo: 0 - 40 °C

Elevación de operación: 0-3000 metros

Ruido audible a 1 metro de la superficie de la unidad: 45.00 dBA

PROTOTIPO DEL SISTEMA DE VIGILANCIA IP

Para la comprobación del correcto funcionamiento del diseño de un sistema de Video vigilancia Inalámbrico para el mejoramiento de la seguridad del edificio administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, se utilizaron los siguientes equipos:

a) Cámara domo PTZ VIVOTEK SD8311E

CAMARA IP DOMO PTZ PARA EXTERIOR 18X ZOOM/ WDR PRO/60 FPS/ H.264&MPEG4&MJPEG/IP66/POE PLUS. La cual presenta las siguientes características:

- Hasta un 60 fps D1
- 18x de zoom
- 360° paneo continuo y 0° ~ 90° de inclinación
- Función Día/noche
- Compresión en tiempo real de de H.264, MPEG-4 y MJPEG
- Soporta audio bidireccional
- PoE

b) Switch Ethernet WS-C2960-24TT-L

Cisco Catalyst 2960-24TT 24 Port. El cual presenta las siguientes características:

- 24 x Network, Ethernet 10Base-T/100Base-TX, RJ-45
- 2 x Network, Ethernet 10Base-T/100Base-TX/1000Base-T, RJ-45
- Dispositivo Capa 2
- Protocolos remotos de administración: SNMP 1, RMON, Telnet, SNMP 3
- Tecnología de conexión: cableada

c) Radio de comunicación inalámbrica, Microhard 4.9 GHz Public Safety Broadband Ethernet Bridge/Serial Gateway. Entre sus principales características se encuentran:

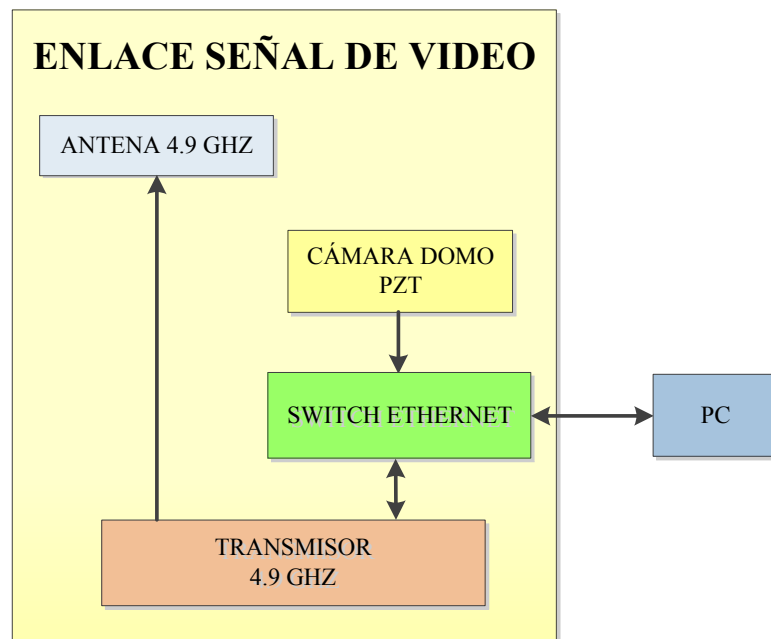
- Data rate de 54Mbps

- Puerto LAN y WAN
- Gateway serial (RS232/485/422)
- Soporte para encriptación
- Administración remota
- Se utilizará una antena omnidireccional de 4.9 GHz.

d) PC

- ***Parámetros de diseño e implementación***

Esquema físico: El esquema físico de conexión es el siguiente:



*Esquema de conexión físico del prototipo de sistema de vigilancia IP
Elaborado por: La Investigadora*

Medios de conexión:

Según los equipos se utilizará diferente cableado.

- Medio guiado UTP CAT 5E. Conexión: Switch-Radio, Switch-PC, Switch-Cámara PTZ
- Medio guiado Cable de cobre RG58. Conexión Radio-Antena

Topología:

Se utilizó una topología estrella, para la comunicación de los diferentes equipos a través de la conmutación del Switch Ethernet.

Ubicación de la cámara de red:

- Cámara, se encuentra ubicada en la esquina superior del HANGAR principal frente a la entrada principal del CIDFAE (Centro de Investigación y Desarrollo de la FUERZA AÉREA ECUATORIANA), ubicado en la Parroquia Izamba.

Con el objetivo de tener un campo de visión amplio, el cual cubre la entrada principal del hangar, entrada a las diferentes oficinas, y área de trabajo del hangar.

En las siguientes dos figuras se muestra la ubicación de la cámara dentro del hangar.

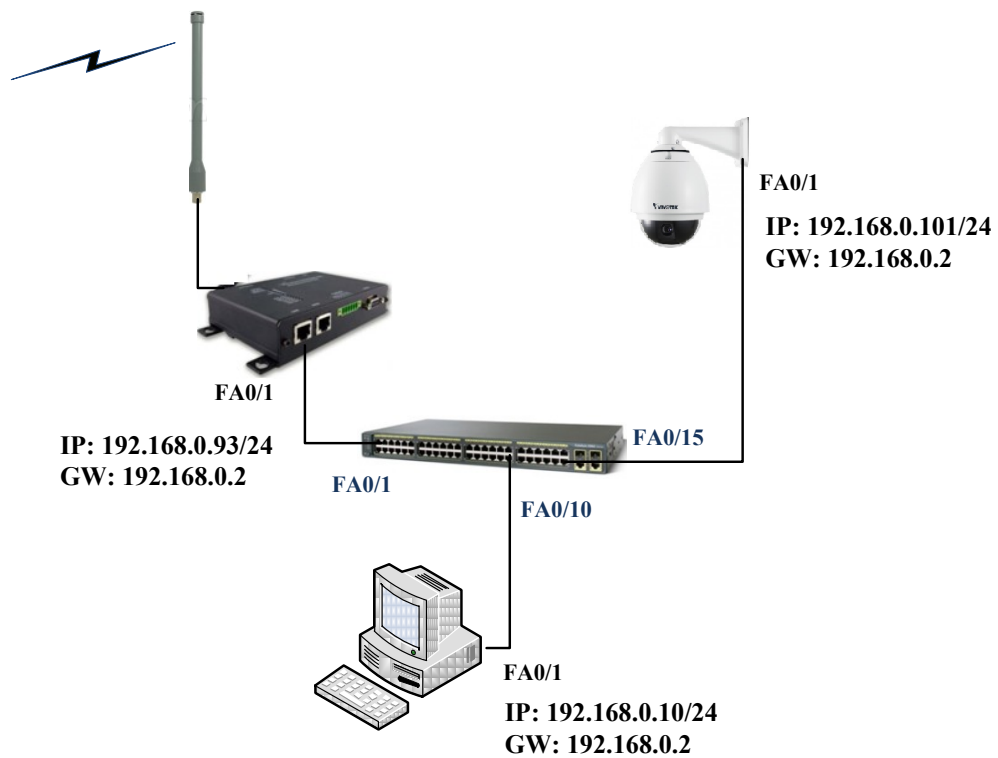


*Ubicación de la cámara PTZ
Elaborado por: La Investigadora*



*Vista de la ubicación de la cámara PTZ
Elaborado por: La Investigadora*

Esquema lógico: la topología lógica del prototipo es la siguiente:



*Esquema de conexión lógico del prototipo de sistema de vigilancia IP
Elaborado por: La Investigadora*

- ***Configuración de la cámara PTZ***

Para la configuración de los parámetros de la cámara de red se utiliza un programa de gestión que viene en el CD de instalación de la cámara.

Para obtener las características de conectividad, sonido y video deseadas, se realizaron las configuraciones para el funcionamiento de la cámara como PTZ que se mencionan a continuación:

Sistema. Se configura:

Zona horaria: GMT+08:00

Nombre de la cámara: Outdoor Network Speed Dome Camera

Conectividad. Los parámetros que se ingresan son los siguientes:

IP: 192.168.0.101

Máscara de subred: 255.255.255.0

Gateway: 192.168.0.92

Audio y video

Orientación de video: Normal

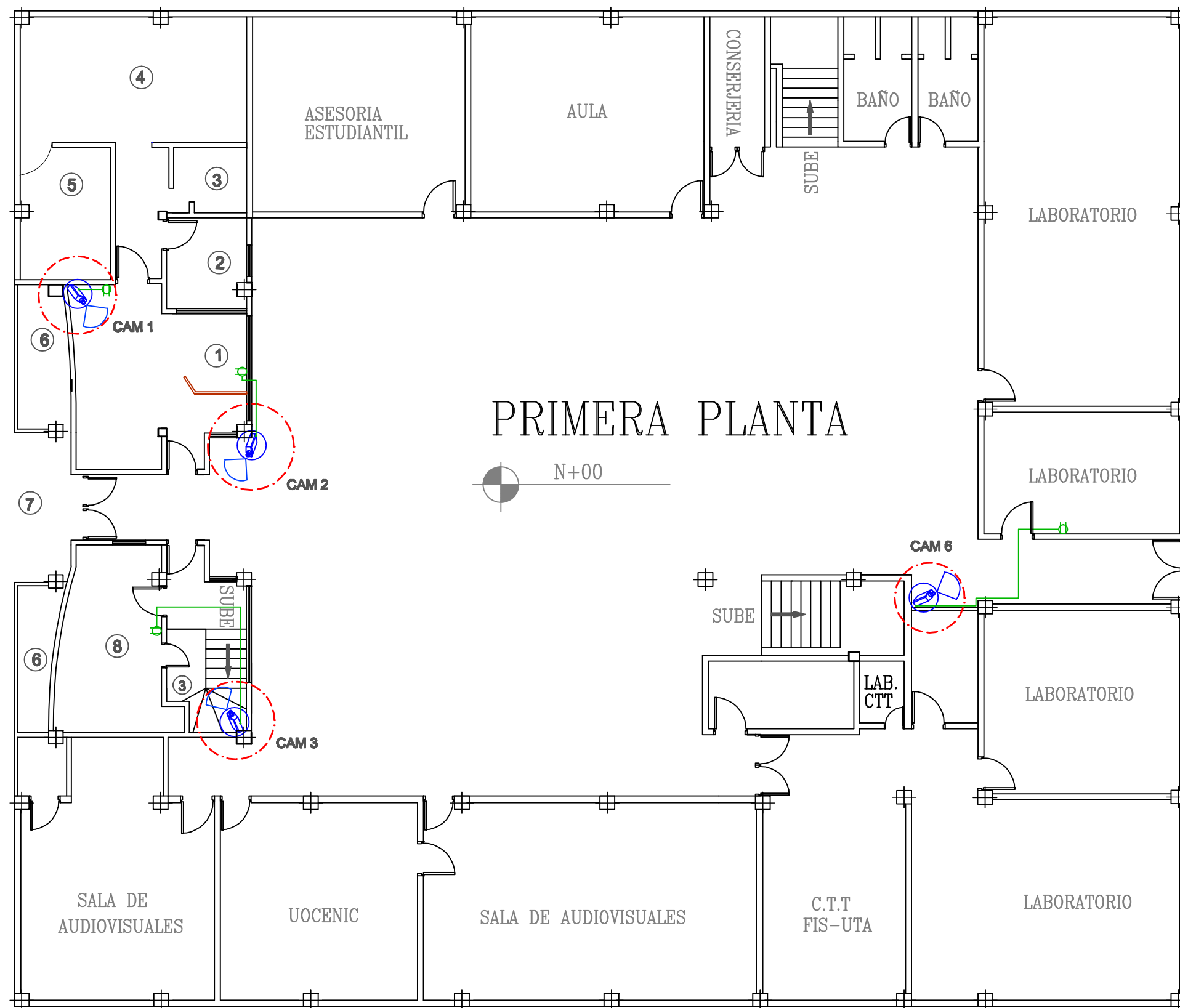
Tipo de audio: GSM: AMR, con un Bit rate de 12.2 Kbps

Para visualizar las imágenes y el sonido que área que cubre la cámara se debe ingresar al programa de visualización, a través de un explorador con la URL configurada en la IP de la cámara. En el programa de visualización se puede realizar el movimiento de la cámara en el sentido deseado (izquierda, derecha, arriba, abajo), además se puede visualizar a detalle a través de la característica de zoom.

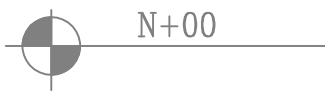
En la siguiente figura se muestra la escena que visualiza la cámara en tiempo real:



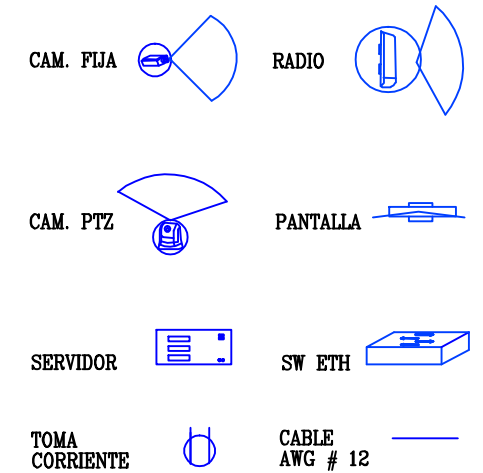
*Captura de pantalla de la escena captada por la cámara PTZ
Elaborado por: La Investigadora*



PRIMERA PLANTA



SIMBOLOGIA



DISTRIBUCIÓN DE AREAS

- ① SECRETARIA CARRERA
- ② INFORMACION MAESTRIAS PASANTIAS SEMINARIOS
- ③ BAÑO
- ④ SECRETARIA ACADEMICA
- ⑤ ARCHIVO
- ⑥ JARDIN
- ⑦ ENTRADA
- ⑧ SECRETARIA POST-GRADO

UNIVERSIDAD TÉCNICA DE AMBATO

CONTIENE: PLANTA ARQUITECTÓNICA, DISTRIBUCIÓN Y CÁMARAS

GABRIELA CIPUENTES DOMÍNGUEZ

FECHA: JULIO 2012

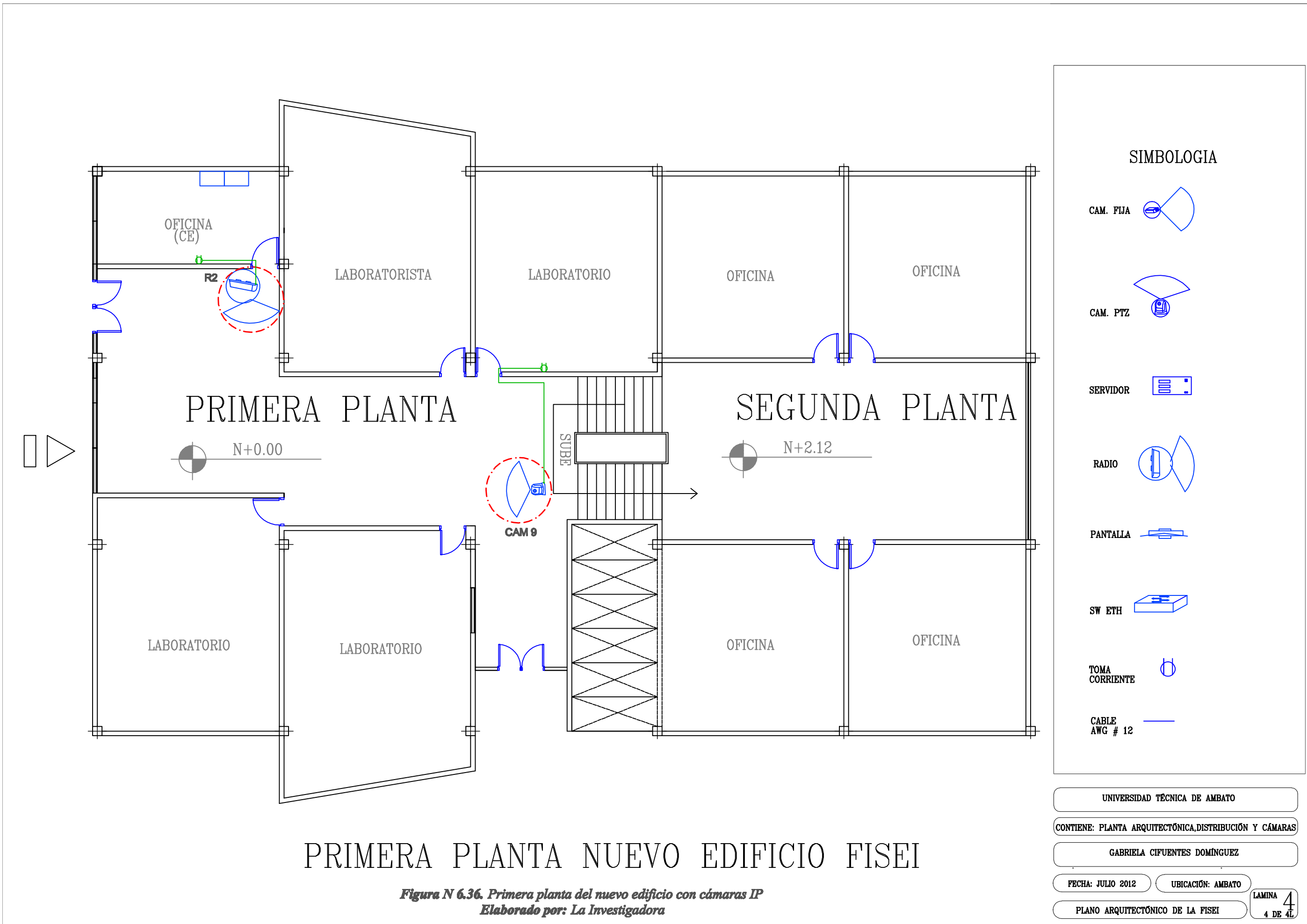
UBICACIÓN: AMBATO

PLANO ARQUITECTÓNICO DE LA FISEI

LAMINA 1 DE 4L

PRIMERA PLANTA EDIFICIO PRINCIPAL FISEI

Figura N 6.33. Primera planta del edificio principal con cámaras IP
Elaborado por: La Investigadora



PRIMERA PLANTA NUEVO EDIFICIO FISEI

*Figura N 6.36. Primera planta del nuevo edificio con cámaras IP
Elaborado por: La Investigadora*

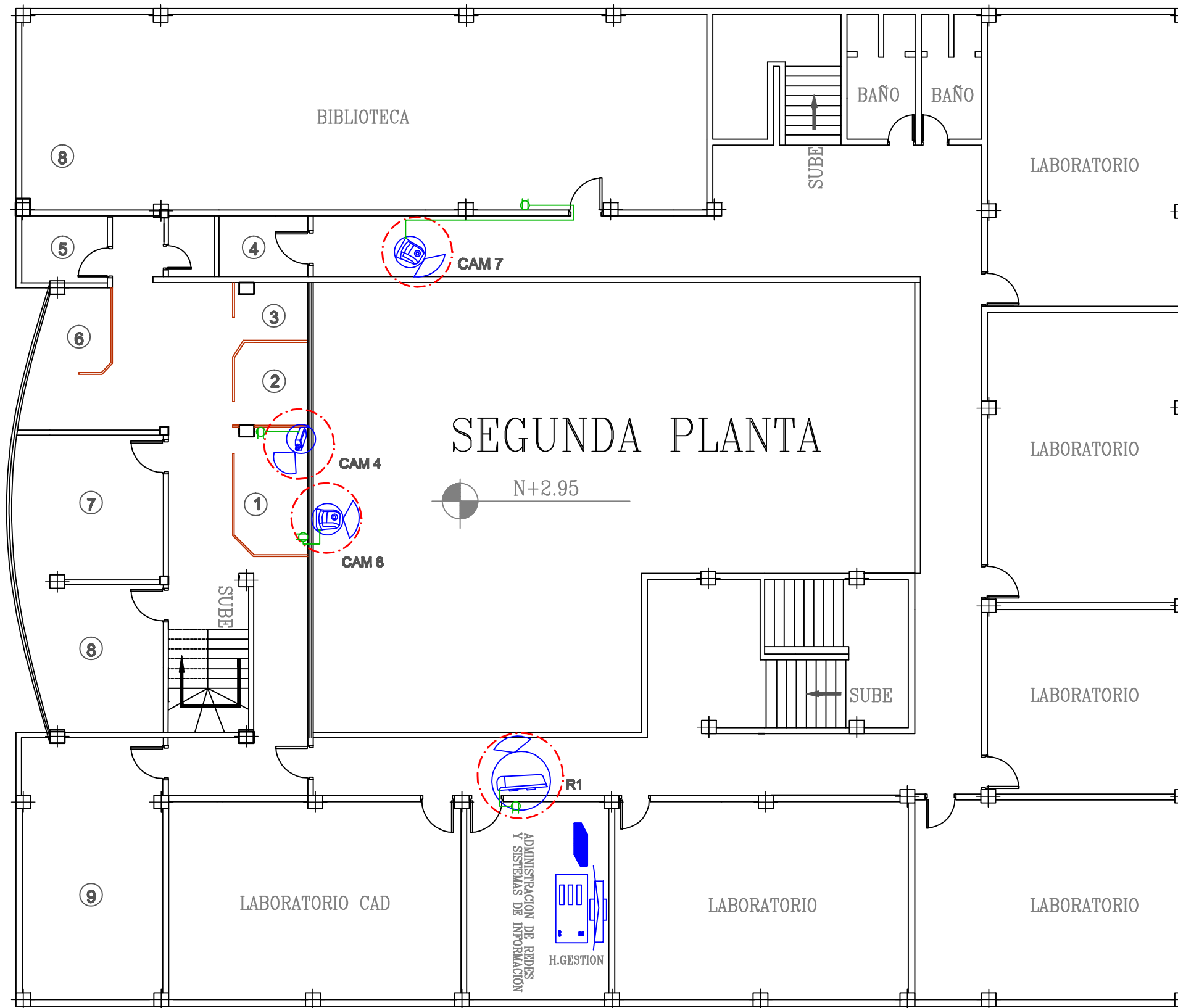
UNIVERSIDAD TÉCNICA DE AMBATO

CONTIENE: PLANTA ARQUITECTÓNICA, DISTRIBUCIÓN Y CÁMARAS

GABRIELA CIFUENTES DOMÍNGUEZ

FECHA: JULIO 2012 UBICACIÓN: AMBATO

PLANO ARQUITECTÓNICO DE LA FISEI LAMINA 4 DE 4L



SIMBOLOGIA

CAM. FIJA		RADIO	
CAM. PTZ		PANTALLA	
SERVIDOR		SW ETH	
TOMA CORRIENTE		CABLE AWG # 12	

DISTRIBUCIÓN DE AREAS

- ① SECRETARIA
- ② COORDINACIÓN ELECTRONICA
- ③ COORDINACIÓN INDUSTRIAL
- ④ BAÑO
- ⑤ ARCHIVO
- ⑥ COORDINACIÓN SISTEMAS
- ⑦ H. CONSEJO ACADEMICO
- ⑧ SUBDECANATO
- ⑨ ADMINISTRACIÓN BIENES

SEGUNDA PLANTA EDIFICIO PRINCIPAL FISEI

Figura N 6.34. Segunda planta del edificio principal con cámaras IP
Elaborado por: La Investigadora

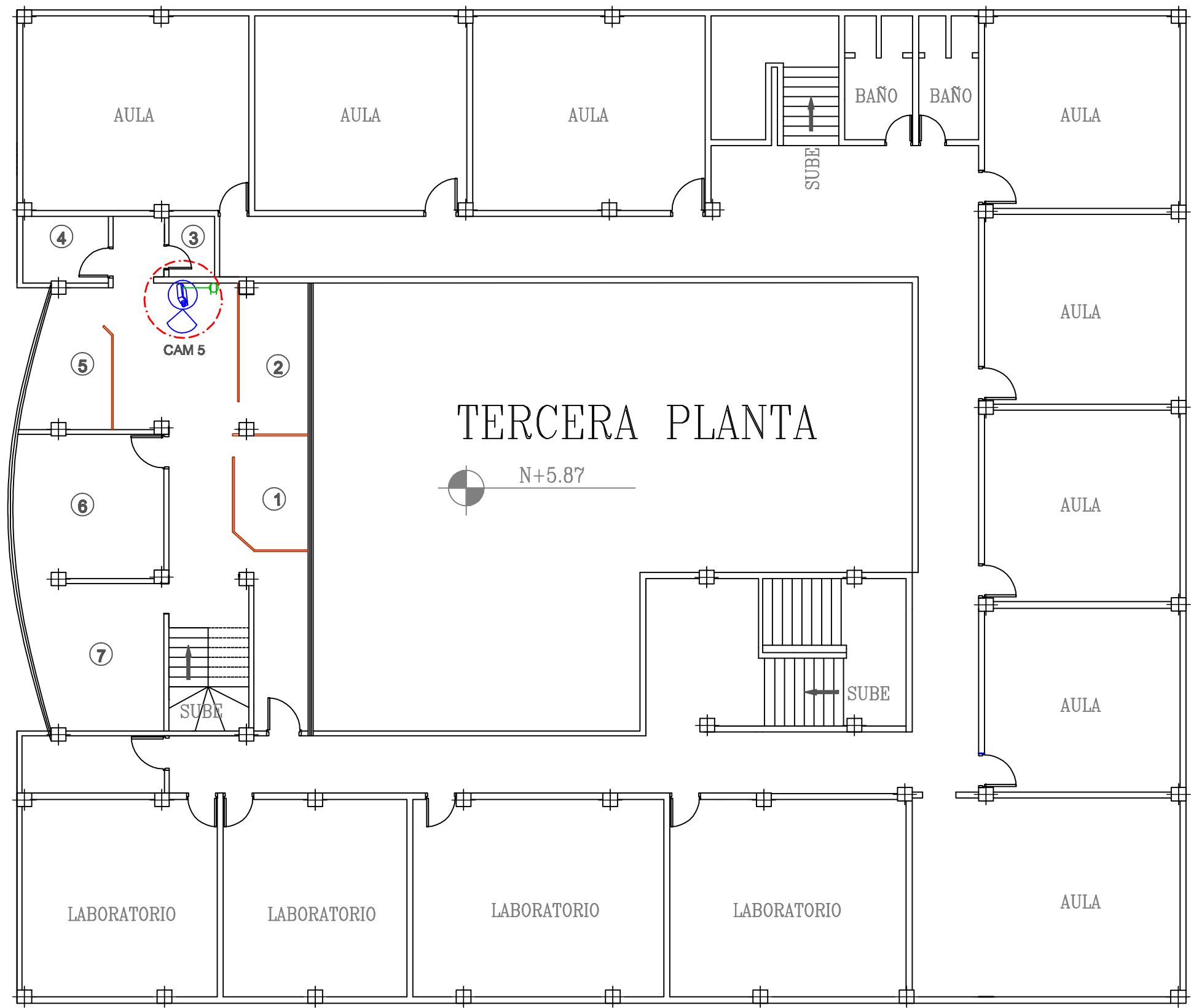
UNIVERSIDAD TÉCNICA DE AMBATO

CONTIENE: PLANTA ARQUITECTÓNICA, DISTRIBUCIÓN Y CÁMARAS

GABRIELA CIPUENTES DOMÍNGUEZ

FECHA: JULIO 2012 UBICACIÓN: AMBATO

PLANO ARQUITECTÓNICO DE LA FISEI LAMINA 2 DE 4L



SIMBOLOGIA

CAM. FIJA		RADIO	
CAM. PTZ		PANTALLA	
SERVIDOR		SW ETH	
TOMA CORRIENTE		CABLE AWG # 12	

DISTRIBUCIÓN DE AREAS

- ① SECRETARIA
- ② ASISTENTE SECRETARIA GENERAL
- ③ BAÑO
- ④ ARCHIVO
- ⑤ SECRETARIA GENERAL
- ⑥ H. CONSEJO SISTEMAS
- ⑦ DECANATO

TERCERA PLANTA EDIFICIO PRINCIPAL FISEI

*Figura N 6.35. Tercera planta del edificio principal con cámaras IP
Elaborado por: La Investigadora*

UNIVERSIDAD TÉCNICA DE AMBATO

CONTIENE: PLANTA ARQUITECTÓNICA, DISTRIBUCIÓN Y CÁMARAS

GABRIELA CIPUENTES DOMÍNGUEZ

FECHA: JULIO 2012 UBICACIÓN: AMBATO

PLANO ARQUITECTÓNICO DE LA FISEI LAMINA 3 DE 4L