



**UNIVERSIDAD TÉCNICA DE AMBATO**

**FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA  
E INDUSTRIAL**

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y  
COMUNICACIONES**

**Tema:**

---

**“RED DE VIDEO-VIGILANCIA CON TECNOLOGÍA GSM-GPRS PARA  
EL MONITOREO Y CONTROL DE ACCESOS A ZONAS DE ALTA  
VULNERABILIDAD EN LA BRIGADA SELVA N°17 PASTAZA”**

---

Trabajo de Graduación. Modalidad: TEMI. Trabajo Estructurado de Manera Independiente, presentado previo la obtención del título de Ingeniero en Electrónica y Comunicaciones

AUTOR: Franklin Ricardo Baldospin Llundo

TUTOR: Ing. Juan Pablo Pallo, Mg.

Ambato - Ecuador

Septiembre 2013

## **APROBACIÓN DEL TUTOR**

En mi calidad de tutor del trabajo de investigación sobre el tema:

“RED DE VIDEO-VIGILANCIA CON TECNOLOGÍA GSM-GPRS PARA EL MONITOREO Y CONTROL DE ACCESOS A ZONAS DE ALTA VULNERABILIDAD EN LA BRIGADA SELVA N°17 PASTAZA”, del señor Franklin Ricardo Baldospin Llundo, 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 Septiembre, 2013

EL TUTOR

-----  
Ing. Juan Pablo Pallo, Mg.

## **AUTORÍA**

El presente trabajo de investigación titulado: “RED DE VIDEO-VIGILANCIA CON TECNOLOGÍA GSM-GPRS PARA EL MONITOREO Y CONTROL DE ACCESOS A ZONAS DE ALTA VULNERABILIDAD EN LA BRIGADA SELVA N°17 PASTAZA”. 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 Septiembre, 2013

-----  
Franklin Ricardo Baldospin Llundo

C.I.: 180369218-3

## APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Santiago Manzano, Ing. Patricio Encalada, revisó y aprobó el Informe Final del trabajo de graduación titulado “Red de video-vigilancia con tecnología GSM-GPRS para el monitoreo y control de accesos a zonas de alta vulnerabilidad en la Brigada Selva N°17 Pastaza”, presentado por el señor Franklin Ricardo Baldospin Llundo de acuerdo al Art. 17 del Reglamento de Graduación para obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato Junio, 2013

XXXXXXXXXXXXXXXXXXXXXXXXXXXX  
PRESIDENTE DEL TRIBUNAL

-----  
Ing. Santiago Manzano

-----  
Ing. Patricio Encalada

## **DEDICATORIA**

*Dedico este proyecto de tesis al ser más grande Dios, a mis padres, a mi pedazo de cielo mi hija y a todas aquellas personas quienes de alguna manera me ayudaron en este largo camino rumbo a esta meta. A Dios porque ha estado conmigo a cada paso que doy, sobre todo cuidándome y dándome la fortaleza para continuar, a mis padres, quienes a lo largo de mi vida han velado por mi bienestar y educación en especial a mi bella madre de la cual su apoyo en todo momento ha sido incondicional a pesar de aquellos tropiezos y destrozos los cuales me enseñaron la dura realidad en la que todo ser humano se desarrolla, a mi padre quien depositó su entera confianza en cada reto que se presentaba sin dudar ni un solo momento en mi inteligencia y capacidad. Al sol de mis días Emily la cual con su mirada inocente me impulsa a seguir de pie luchando sin desmayar hasta el final y sin olvidar de aquellos seres de luz comparados con ángeles los cuales con una palabra o un gesto incondicional me demostraron lo que es una verdadera amistad y compañerismo además de diferentes sentimientos los cuales me hicieron crecer en valores Gracias, Gracias a todos. Es por todo este universo de personas las cuales me rodea que soy lo que soy ahora. Les amo.*

*Franklin Ricardo Baldospin Llundo*

## **AGRADECIMIENTO**

*A la Universidad Técnica de Ambato, en especial a la Facultad de Ingeniería en Sistemas, Electrónica e Industrial por haberme permitido llegar a cumplir una de mis metas académicas.*

*A la Brigada de Selva N. 17 “PASTAZA” por abrirme las puertas de su Institución para demostrar mis conocimientos y dejarlos plasmados en este proyecto.*

*Franklin Ricardo Baldospin Llundo*

## ÍNDICE

<b>CARÁTULA</b> .....	<b>i</b>
<b>UNIVERSIDAD TÉCNICA DE AMBATO</b> .....	<b>i</b>
<b>APROBACIÓN DEL TUTOR</b> .....	<b>ii</b>
<i>DEDICATORIA</i> .....	<b>v</b>
<i>AGRADECIMIENTO</i> .....	<b>vi</b>
<b>ÍNDICE DE GRÁFICOS</b> .....	<b>xii</b>
<b>ÍNDICE DE TABLAS</b> .....	<b>xv</b>
<b>RESUMEN EJECUTIVO</b> .....	<b>xvi</b>
<b>INTRODUCCIÓN</b> .....	<b>xvii</b>
<b>CAPÍTULO I</b> .....	<b>1</b>
<i>PROBLEMA</i> .....	<i>1</i>
1.1.    TEMA DE INVESTIGACIÓN .....	1
1.2.    PLANTEAMIENTO DEL PROBLEMA .....	1
1.2.1.    Contextualización.....	1
1.2.2.    Árbol del Problema.....	3
1.3    ANÁLISIS CRÍTICO .....	4
1.4    PROGNOSIS .....	4
1.5    FORMULACIÓN DEL PROBLEMA.....	5
1.6    PREGUNTAS DIRECTRICES .....	5
1.7    DELIMITACIÓN DEL PROBLEMA.....	5
1.8    JUSTIFICACIÓN .....	6
1.9    OBJETIVOS .....	6
1.9.1    Objetivo General .....	6
1.9.2    Objetivos específicos.....	7

<b>CAPÍTULO II.....</b>	<b>8</b>
<i>MARCO TEÓRICO</i> .....	8
2.1 ANTECEDENTE INVESTIGATIVO.....	8
2.2 FUNDAMENTACIÓN LEGAL.....	10
2.3 CATEGORÍAS FUNDAMENTALES .....	10
2.3.1 Red de Inclusiones conceptuales .....	10
2.3.2 Constelación de ideas .....	11
2.3.3 Sistemas de Comunicaciones .....	12
2.3.4 Características de un Sistema de Comunicaciones.....	13
2.3.5 Convergencia tecnológica .....	13
2.3.6 Prestaciones QoS .....	14
2.3.7 Comunicaciones M2M .....	14
2.3.8 Elementos de una Comunicación Máquina a Máquina .....	14
2.3.9 Características de Comunicaciones M2M .....	15
2.3.10 Ventajas de un Modelo Máquina a Máquina.....	16
2.3.11 Supervisión Local.....	16
2.3.12 Supervisión Remota.....	16
2.3.13 Tecnología GSM .....	16
2.3.13.1 Arquitectura de una Red GSM .....	17
2.3.13.2 Ventajas y Desventajas de la Red GSM.....	19
2.3.14 Tecnología GPRS .....	19
2.3.15 Ventajas.....	20
2.3.16 Sistemas de Supervisión.....	20
2.3.17 Sistemas de seguridad.....	21
2.3.18 Clasificación de los sistemas de seguridad.....	21
2.3.19 Sistemas de vigilancia .....	21
2.3.20 Características del Sistema de Vigilancia.....	22
2.3.21 Clasificación de los sistemas de Vigilancia.....	22
2.3.22 Sistemas de Monitoreo .....	23
2.3.23 Elementos de un sistema de Monitoreo.....	23
2.3.24 Cámaras .....	23
2.3.24.1 Características de la Cámaras IP .....	24



2.3.24.2	Visión en vivo .....	25
2.3.25	Grabadores y Almacenadores de imagen. ....	25
2.3.25.1	Servidores de video .....	25
2.3.25.2	Codificadores y Decodificadores .....	26
2.3.25.3	Grabadores Digitales de Red / Network Video Recorders.....	26
2.3.26	Control de accesos.....	26
2.3.27	Ventajas de un sistema de control de accesos .....	27
2.4	HIPÓTESIS .....	28
2.5	SEÑALAMIENTO DE VARIABLES .....	28
<b>CAPÍTULO III</b>	<b>.....</b>	<b>29</b>
	<i>MARCO METODOLÓGICO</i> .....	29
3.1	ENFOQUE DE LA INVESTIGACIÓN .....	29
3.2	MODALIDAD BÁSICA DE INVESTIGACIÓN.....	29
3.2.1	Investigación de Campo .....	29
3.2.2	Investigación Bibliográfica .....	29
3.3	TIPOS DE INVESTIGACIÓN.....	30
3.3.1	Exploratorio.....	30
3.3.2	Descriptivo .....	30
3.4	POBLACIÓN Y MUESTRA.....	30
3.5	OPERACIONALIZACIÓN DE VARIABLES .....	31
3.6	TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN .....	33
3.7	RECOLECCIÓN DE DATOS.....	33
3.8	PROCESAMIENTO DE LA INFORMACIÓN .....	34
3.9	ANÁLISIS E INTERPRETACIÓN DE RESULTADOS .....	34
<b>CAPÍTULO IV</b>	<b>.....</b>	<b>35</b>
4.1	ANÁLISIS DE RESULTADOS E INTERPRETACIÓN .....	35
<b>CAPÍTULO V</b>	<b>.....</b>	<b>45</b>
	<i>CONCLUSIONES Y RECOMENDACIONES</i> .....	45
5.1	Conclusiones .....	45
5.2	Recomendaciones.....	46

<b>CAPÍTULO VI</b> .....	<b>48</b>
<i>PROPUESTA</i> .....	48
6.1 TEMA.....	48
6.2 DATOS INFORMATIVOS .....	48
6.3 ANTECEDENTES DE LA PROPUESTA .....	49
6.4 JUSTIFICACIÓN.....	49
6.5 OBJETIVOS.....	50
6.5.1 Objetivo General .....	50
6.5.2 Objetivos Específicos .....	50
6.6 ANÁLISIS DE FACTIBILIDAD .....	51
6.6.1 Factibilidad Técnica .....	51
6.6.2 Factibilidad Operativa .....	51
6.6.3 Factibilidad Económica.....	51
6.7 FUNDAMENTACIÓN CIENTÍFICO – TÉCNICA.....	51
6.7.1 Establecimiento geográfico del proyecto .....	51
6.7.2 Diseño de Sistema de Video-Vigilancia.....	52
6.7.3 Visualización del video .....	53
6.7.4 Almacenamiento de Información .....	54
6.7.5 Componentes del Sistema de Video-Vigilancia.....	54
6.8 METODOLOGÍA MODELO OPERATIVO.....	54
6.8.1 Análisis Preliminar .....	56
6.8.2 Situación Actual del Batallón Selva N°17 .....	56
6.8.3 Requerimientos de Usuarios.....	60
6.8.4 Requerimientos de Red .....	60
6.8.3 Planificación.....	61
6.8.4 Descripción del diseño .....	61
6.8.5 Análisis y Elección de los dispositivos del sistema a utilizar .....	61
6.8.6 Descripción de los dispositivos del Sistema .....	63
6.8.6.1 Grabador de Video Digital (DVR) TopBand TBO-9716E .....	63
6.8.6.2 Cámara Fija Q-see 3,6mm.....	64
6.8.6.3 Cámara Topband 3,6 mm .....	65
6.8.6.4 Cámara Domo TopBand TBO-506IR .....	65

6.8.6.5 Cámara PTZ Zmodo CM-Z2213GY .....	66
6.8.6.6 Alarma Canadiense DSC 1832.....	67
6.8.6.7 Transmisor de alarma por IP universal TL250.....	67
6.8.6.8 Detector infrarrojo pasivo LC-100-PI.....	68
6.8.6.9 Teclado DSC LCD 5511 .....	69
6.8.7 Diseño del prototipo .....	69
6.8.7.1 Campo de visión.....	72
6.8.7.2 Profundidad de Campo.....	73
6.8.7.3 Sensibilidad Lumínica.....	74
6.8.7.4 Cálculo de la iluminación.....	75
6.8.7.5 Cálculo de distancia focal.....	75
6.8.7.6 Eliminación de reflejos.....	76
6.8.7.7 Ubicación de las Cámaras .....	77
6.8.8 Ejecución.....	85
6.8.9 Configuración.....	85
6.8.10 Control de Accesos.....	96
6.8.11 Pruebas y Fallas del Sistema de Video–Vigilancia.....	109
6.9 Conclusiones y Recomendaciones.....	114
6.10 Bibliografía .....	117
6.11 Anexos .....	119

## ÍNDICE DE GRÁFICOS

Gráfico 1. 1 Relación Causa Y Efecto .....	3
Gráfico 2. 1 Categorías Fundamentales .....	10
Gráfico 2. 2 Variable Independiente .....	11
Gráfico 2. 3 Variable dependiente .....	12
Gráfico 2. 4 Arquitectura de una Red GSM.....	17
Gráfico 2. 5 Sistema de Supervisión .....	20
Gráfico 2. 6 Componentes Cámara .....	23
Gráfico 2. 7 Diseño de Red Básica .....	25
Gráfico 2. 8 Servidor de Video .....	26
Gráfico 4. 1 Sistema de Supervisión .....	36
Gráfico 4. 2 Método de Obtención de Información .....	37
Gráfico 4. 3 Autenticación Personal.....	38
Gráfico 4. 4 Sucesos no Grabados .....	39
Gráfico 4. 5 Acciones Preventivas .....	40
Gráfico 4. 6 Normas y Estándares.....	41
Gráfico 4. 7 Dispositivos de Seguridad.....	42
Gráfico 4. 8 Información en Tiempo Real .....	43
Gráfico 4. 9 Método de Control .....	44
Gráfico 6. 1 Componentes de un Sistema de Video en Red .....	54
Gráfico 6. 2 Diagrama de Fases .....	55
Gráfico 6. 3 Estructura de la Brigada Selva N°17 Pastaza .....	57
Gráfico 6. 4 Central de Comunicaciones .....	58
Gráfico 6. 5 Ingreso principal .....	59
Gráfico 6. 6 Bodegas.....	59
Gráfico 6. 7 DVR TopBand .....	64
Gráfico 6. 8 Cámara Q-see 3,6 mm.....	65
Gráfico 6. 9 Cámara TopBand 3,6mm .....	65
Gráfico 6. 10 Cámara Domo TopBand .....	66

Gráfico 6. 11 Cámara PTZ blindada .....	66
Gráfico 6. 12 Kit Alarma DSC.....	67
Gráfico 6. 13 T-Link 250 DSC .....	68
Gráfico 6. 14 Sensor de Movimiento .....	68
Gráfico 6. 15 Teclado LCD 5511.....	69
Gráfico 6. 16 Red de Datos Actual .....	70
Gráfico 6. 17 Diseño de Red de Video-Vigilancia .....	71
Gráfico 6. 18 Gran Angular, Vista Normal, Telefoto .....	73
Gráfico 6. 19 Profundidad de Campo .....	73
Gráfico 6. 20 Apertura del Iris .....	74
Gráfico 6. 21 Iluminación IR .....	75
Gráfico 6. 22 Reflejos .....	76
Gráfico 6. 23 Bodega 1 Rio Pastaza.....	78
Gráfico 6. 24 Bodega 2 Sector BOES .....	79
Gráfico 6. 26Bodega 4 Sector CAL .....	81
Gráfico 6. 27 Esquema de Conexión de Equipo Grabador DVR.....	83
Gráfico 6. 28 Esquema de Conexión PC 1832.....	84
Gráfico 6. 29 Menú Principal.....	85
Gráfico 6. 30 NC sin RFL.....	86
Gráfico 6. 31 Sensores NC y NO con resistencia RFL .....	87
Gráfico 6. 32 NC sin RFL con detección de Sabotaje .....	87
Gráfico 6. 33 NC con Sabotaje y Corte.....	88
Gráfico 6. 34 Submenú Alarma .....	90
Gráfico 6. 35 Configuración PTZ .....	92
Gráfico 6. 36 Control PTZ .....	92
Gráfico 6. 37 Submenú RED .....	93
Gráfico 6. 38 Ingreso CMD .....	94
Gráfico 6. 39 Habilidad ActiVex .....	94
Gráfico 6. 40 Programa NetView.....	95
Gráfico 6. 41 Visualización del Sistema de Vigilancia.....	95
Gráfico 6. 42 Aplicación iTunes .....	96
Gráfico 6. 43 Ingreso DLS .....	103

Gráfico 6. 44 Nueva Carpeta Shell .....	104
Gráfico 6. 45 PC 1832.....	104
Gráfico 6. 46 IP PC 1832 .....	105
Gráfico 6. 47 Modem Configuración .....	105
Gráfico 6. 48 Dispositivos en Línea.....	106
Gráfico 6. 49 Tipo de Conexión.....	106
Gráfico 6. 50 Estado del sistema.....	106
Gráfico 6. 51 Base de Datos y Claves.....	107
Gráfico 6. 52 Datos Recolectados.....	108
Gráfico 6. 53 Visualización en la Central de Monitoreo .....	109
Gráfico 6. 54 Ubicación PTZ.....	109
Gráfico 6. 55 Vistas PTZ .....	110
Gráfico 6. 56 Infraestructura Existente .....	111
Gráfico 6. 57 Control de Accesos .....	112
Gráfico 6. 58 Bodegas 1,2,3,4.....	119

## ÍNDICE DE TABLAS

Tabla 3. 1 Variable Independiente .....	31
Tabla 3. 2 Variable Dependiente.....	32
Tabla 3. 3 Recolección de datos.....	33
Tabla 4. 1 Sistema de Supervisión .....	35
Tabla 4. 2 Método de Obtención de Información .....	36
Tabla 4. 3 Sistema de Autenticación de Personal.....	37
Tabla 4. 4 Infracciones No corroboradas .....	38
Tabla 4. 5 Acciones Preventivas .....	39
Tabla 4. 6 Normas y Estándares.....	40
Tabla 4. 7 Dispositivos de Control y Vigilancia .....	41
Tabla 4. 8 Información Fiable y Exacta .....	42
Tabla 4. 9 Control de Personal.....	43
Tabla 6. 1 Cuadro Comparativo Cámaras .....	62
Tabla 6. 2 Cuadro Comparativo Equipo Grabador .....	62
Tabla 6. 3 Cuadro Comparativo Alarmas .....	63
Tabla 6. 4 Valores Lumínicos .....	74
Tabla 6. 5 Distancia Focal.....	76
Tabla 6. 6 Campos Activos .....	97
Tabla 6. 7 Fallas .....	100
Tabla 6. 8 Base de datos.....	107
Tabla 6. 9 Costos Materiales.....	112
Tabla 6. 10 Costos Equipos.....	113
Tabla 6. 11 Presupuesto General.....	113

## **RESUMEN EJECUTIVO**

El presente proyecto tiene como objetivo proponer un nuevo diseño de red para optimizar la comunicación dentro de la Brigada de Selva N.17 “PASTAZA”, con el fin actualizar la red con una de las nuevas tecnologías existentes.

En el Capítulo I se expone el problema de la Institución que se define como, “Deficiente sistema de supervisión a zonas sensibles de la BRIGADA SELVA N°17 PASTAZA”, debido al problema encontrado surge la necesidad de implementar una red de video vigilancia remoto aplicando la tecnología GSM-GPRS para el monitoreo y control de accesos.

En el Capítulo II se define el Marco teórico, en el cual se expone diferentes trabajos relacionados con el proyecto, además la explicación de las variables correspondientes a las Categorías Fundamentales.

En el Capítulo III se describen los diferentes tipos de investigación que se utilizaron a lo largo de la parte investigativa, se detalla la población y muestra con la que se trabaja y se plantea el plan de recolección de datos para la investigación.

En el Capítulo IV se muestran la tabulación y análisis de los resultados obtenidos en la investigación, permitiendo así comprobar si la hipótesis es aceptada.

En el Capítulo V se detalla las conclusiones y recomendaciones que se obtuvo al realizar las encuestas dentro de la Institución, convirtiéndose en guías eficientes que servirán como una herramienta para el mejoramiento de la seguridad.

El Capítulo VI propone el desarrollo de la propuesta planteada, con la finalidad de implementar la red de video vigilancia remoto aplicando la tecnología GSM-GPRS para el monitoreo y control de accesos a zonas de alta vulnerabilidad en la Brigada de Selva N.17 “Pastaza”.



## INTRODUCCIÓN

La vigilancia es un tema universal en el ámbito de la seguridad, razón por la cual hoy en día cada institución sea pública como privada avanza de acuerdo al desarrollo de la tecnología aprovechando las ventajas que brindan los equipos actuales.

El desarrollo económico, social y cultural de una institución depende en su mayoría del tipo de tecnología que éste posea, por ende las compañías con la más reciente tecnología alcanzan estándares más altos tanto de productividad como eficiencia, lo ideal sería contar con un sistema de vigilancia moderno, ágil, dimensionado y escalable para aumentar la eficiencia en un futuro cercano.

El propósito que tienen todas las instituciones a nivel internacional es obtener beneficios a partir del desempeño los recursos existentes. El personal adecuado mediante un análisis de la situación actual de la empresa podrá determinar las necesidades prioritarias tomando los correctivos necesarios a través de los medios informáticos, que hoy en día es uno de los aspectos que está dando empuje a la evolución de los países, especialmente el nuestro.

Tomando en cuenta todos estos factores a continuación se proporciona los detalles de la presente investigación que tiene por objetivo presentar una Propuesta de diseño y prototipo de una red de video vigilancia remoto dentro de la Brigada de Selva N.17 “PASTAZA”, señalando las zonas más vulnerables del recinto.

La red de video vigilancia cumple con los requisitos necesarios tanto en diseño, infraestructura, equipos, normas y estándares con el fin de satisfacer la problemática planteada, es así que se busca implementar un prototipo de una central de monitoreo y control de accesos aplicado a dispositivos remotos, mediante el cual se podrá integrar los dos sistemas, promoviendo así el desarrollo tecnológico del Batallón N°17 Selva.

## **CAPÍTULO I**

### **PROBLEMA**

#### **1.1.TEMA DE INVESTIGACIÓN**

“Red de Video-Vigilancia con Tecnología GSM-GPRS para el monitoreo y control de accesos a zonas de alta vulnerabilidad en la BRIGADA SELVA N°17 PASTAZA”

#### **1.2. PLANTEAMIENTO DEL PROBLEMA**

##### **1.2.1. Contextualización**

En la actualidad, la video-vigilancia a través del Internet es una realidad en muchas empresas, instituciones y demás organismos tanto públicos como privados, mismas que están utilizando esta aplicación, obteniendo el máximo aprovechamiento de los recursos que brinda el avance de esta tecnología y manteniéndose a la vanguardia en vigilancia remota.

A nivel mundial las nuevas tecnologías, ofrecen una gran variedad de convergencia de servicios, la posibilidad de controlar todo un sistema de seguridad con un dispositivo móvil garantizando confidencialidad, integridad y disponibilidad; han demostrado la capacidad de reducir cualquier acción delictiva y ayudar a una pronta reacción ante la misma.

En el Ecuador se ha expuesto un alto índice en los sectores públicos, y privados que demandan, servicios de monitoreo y control remoto lo que ha constituido en un ente fundamental para el avance de la economía y comercio,

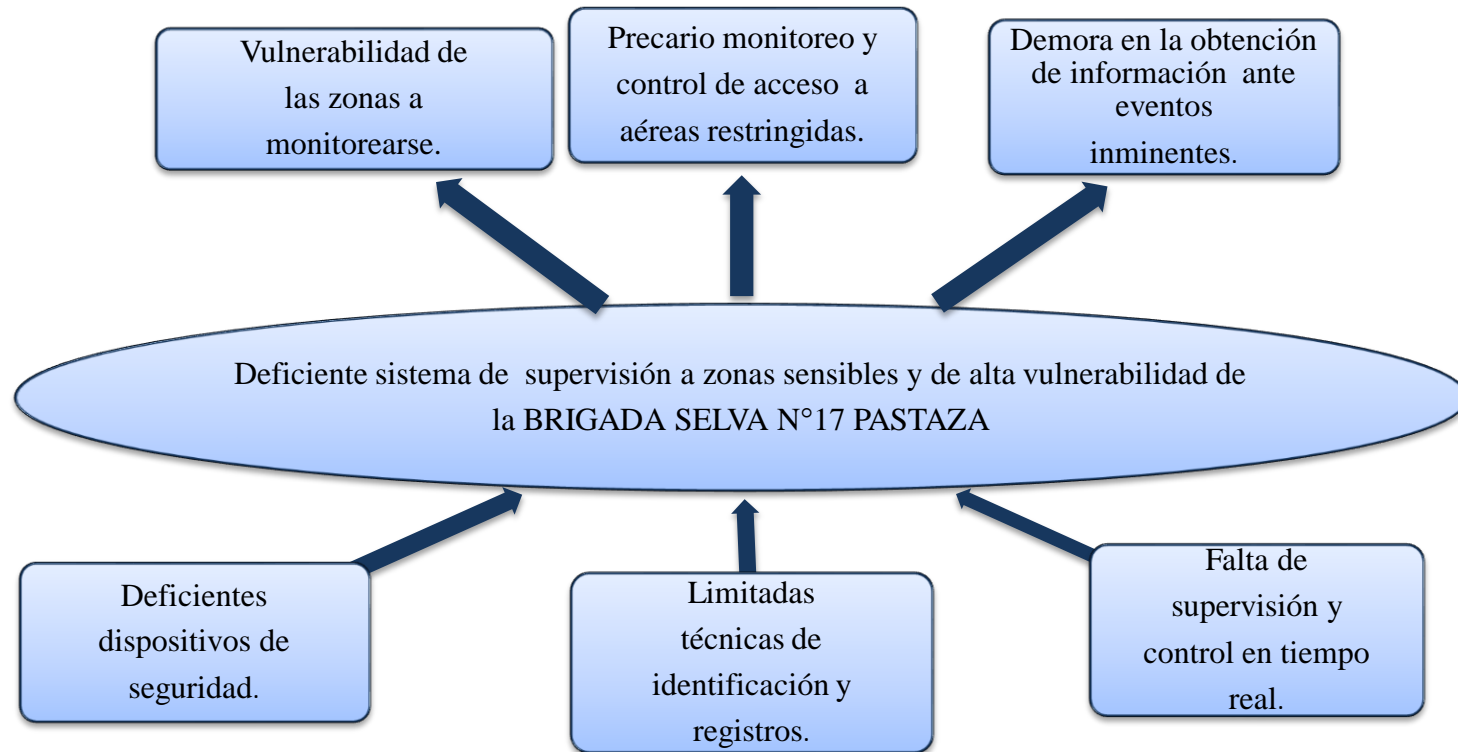
gracias a la disponibilidad tanto de la infraestructura, equipos y operadoras de servicio móvil.

En la provincia de Pastaza está acantonada la BRIGADA SELVA N°17, la cual no dispone de una red de video vigilancia debido principalmente a la falta de recursos y equipos; actualmente cuentan con una infraestructura de red simple para la transmisión de datos.

El mecanismo deficiente de vigilancia tanto del personal como de las zonas restringidas ha originado un constante pérdida de recursos, los limitados sistemas de identificación y control no permite una adquisición real y confiable de los datos necesarios para mantener la seguridad, el orden y el correcto funcionamiento del Batallón

El clima en la región es inestable lo cual dificulta la búsqueda de dispositivos que se ajusten a las condiciones climáticas, así limitando el control de actividades que necesitan supervisión en las distintas unidades de la entidad.

### 1.2.2. Árbol del Problema



**Gráfico 1. 1 Relación Causa Y Efecto**

**Elaborado por: Franklin Baldospin**

### **1.3 ANÁLISIS CRÍTICO**

El presente trabajo de investigación de carácter investigativo, descriptivo, analiza la situación actual del sistema de supervisión de los lugares sensibles y de alta vulnerabilidad de la BRIGADA SELVA N°17 PASTAZA.

Los deficientes dispositivos de seguridad existentes en el Batallón, ocasiona una alta vulnerabilidad de las zonas no expuestas a un monitoreo continuo de la brigada como son bodegas de armamento, recursos logísticos, y objetos de manejo apropiado.

Por otra parte las limitadas técnicas de identificación y registro de personal, provoca la intromisión de personas no autorizadas a zonas restringidas del Batallón; además considerando el deficiente monitoreo y la inexistencia de un control de acceso permite el libre ingreso de posibles autores de robo o comportamiento indebido.

En cuanto a la falta de supervisión y control de los procedimientos de seguridad en tiempo real, brindan por efecto una demora en la toma de información necesaria al presentarse un evento inminente.

Puntualizando a la Brigada N° 17 se tiene como fin salvaguardar la integridad del personal militar como de los recursos que están presentes en la recinto, teniendo en cuenta que las zonas a desarrollarse el estudio se encuentran en sitios remotos y aislados lo cual requieren de un control más cuidadoso y oportuno al presentarse un evento.

### **1.4 PROGNOSIS**

La Brigada N°17 Selva al mantener un sistema de supervisión deficiente, continuará generando factores de muy alto riesgo en seguridad, por la existencia en la zona de armamentos y explosivos, de igual manera la falta de un sistema de control de los accesos da lugar a una limitada adquisición de información en

tiempo real, imposibilitando una rápida y eficiente respuesta al posible evento delictivo.

### **1.5 FORMULACIÓN DEL PROBLEMA**

¿Cómo afecta el deficiente sistemas de supervisión en el monitoreo y control de acceso a zonas sensibles y de alta vulnerabilidad de la BRIGADA SELVA N°17 PASTAZA?

### **1.6 PREGUNTAS DIRECTRICES**

- ¿Existe alguna red de seguridad para el monitoreo de zonas sensibles de la BRIGADA SELVA N°17 PASTAZA?
- ¿Con que sistemas de monitoreo y control de acceso cuenta la BRIGADA SELVA N°17 PASTAZA para las zonas vulnerables?
- ¿Cómo beneficiará la implementación de una red de video-vigilancia remota en las zonas sensibles de la BRIGADA SELVA N°17 PASTAZA?

### **1.7 DELIMITACIÓN DEL PROBLEMA**

Delimitación del contenido

<b>Área:</b>	Comunicación
<b>Línea de Investigación:</b>	Tecnologías de Comunicación
<b>Sublíneas:</b>	Seguridad de la Información

#### **Delimitación Espacial**

El estudio se llevó a cabo en la Brigada de Selva N°17 ubicada en la ciudad de Shell perteneciente a la provincia de Pastaza.

#### **Delimitación Temporal**

La actual investigación se realizó en el periodo de seis meses a partir de la aprobación del Honorable Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

## **1.8 JUSTIFICACIÓN**

Este proyecto permitirá a la Brigada N°17 optimizar recursos al emplear los actuales sistemas de video-vigilancia, así obteniendo un modelo más confiable, accesible y simple que los antiguos CCTV, por lo que resulta de suma importancia aplicar a las necesidades requeridas en la zona referenciada.

Cabe mencionar que la utilidad de estos sistemas permiten un óptimo manejo y tratamiento de la información a obtenerse, demostrando ser un soporte e impulso para el desarrollo de las nuevas tecnologías; brindando soluciones urgentes y adecuadas para el monitoreo y control de accesos.

La vigilancia de zonas sensibles, como la seguridad del armamento existente revela la necesidad de una solución que permite garantizar una asistencia oportuna, bajo demanda; en un breve periodo de tiempo, con el acceso remoto, cualquier evento es advertido en el momento que se da la señal de alarma; inmediatamente es analizada y comunicada para la toma de acciones pertinentes reduciendo los tiempos y recursos antes utilizados.

La presente investigación beneficiara tanto al Batallón N°17 como al personal de cada unidad supervisando de forma local y remota las zonas sensibles; así evitando y detectando a tiempo eventos inminentes o peligrosos.

## **1.9 OBJETIVOS**

### **1.9.1 Objetivo General**

Analizar el sistema de supervisión en la zonas sensibles y de alta vulnerabilidad para determinar la incidencia en el monitoreo y control de la BRIGADA SELVA N°17 PASTAZA.

### **1.9.2 Objetivos específicos**

- Evaluar el sistema de supervisión aplicado en la BRIGADA SELVA N°17 PASTAZA
- Investigar el proceso de monitoreo y control de acceso de la BRIGADA SELVA N°17 PASTAZA
- Plantear una propuesta que permita mejorar el monitoreo y control de accesos en la BRIGADA SELVA N°17 PASTAZA mediante un sistema de video-vigilancia remoto.



## **CAPÍTULO II**

### **MARCO TEÓRICO**

#### **2.1 ANTECEDENTE INVESTIGATIVO**

Revisado los trabajos de tesis en la biblioteca de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial se encontró los siguientes temas relacionados a este proyecto:

- U.T.A. (Universidad Técnica de Ambato) Ambato – Ecuador “SISTEMAS DE MONITOREO Y CONTROL REMOTO UTILIZANDO EL SERVICIO DE MENSAJES DE TEXTO DE LA RED GSM”

Autor: Santiago Villacis.

La presente investigación tiene como conclusión principal lo siguiente:

“El Sistema GSM es complejo, sin embargo permiten acceder a una amplia gama de servicios adicionales, que dependerá del tipo de plan contratado, de la gama de servicios del operador y de la potencia del teléfono”

- U.T.A. (Universidad Técnica de Ambato) Ambato – Ecuador “DISEÑO DE UN SISTEMA DE VIDEO VIGILANCIA IP PARA EL CONTROL Y MONITOREO REMOTO DE FISEI DE LA UTA”

Autor: Washington Amancha

La presente investigación tiene como conclusión principal lo siguiente:

“La video- vigilancia permite la integración de redes complejas de cámaras para garantizar una vigilancia continua de zonas estratégicas como una ciudad; utilizadas también para protección de vidas humanas en lugares donde se produce accidentes”

- ESPE-L ( Escuela Politécnica del Ejército Sede Latacunga) “DISEÑO DE UN SISTEMA DE VIDEO VIGILANCIA IP INALÁMBRICO CON INTEGRACIÓN A LA RED EXISTENTE EN EL CAMPUS DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE LATACUNGA”

Autor: Chafla Franklin, Cachiguango, Lasluisa Héctor

La presente investigación tiene como conclusión principal lo siguiente:

“La vigilancia IP es un sistema que tiene una finalidad clara, la monitorización, vigilancia y almacenamiento basada en videos digitalizados. El sistema de video vigilancia IP crea un instrumento imprescindible para la administración efectiva de la seguridad con la finalidad de proteger a importantes instalaciones existentes en la ESPEL”

- ESPOCH ( Escuela Superior Politécnica de Chimborazo) “Desarrollo de Video- Vigilancia IP con Análisis de Técnicas de Encolamiento Dirigido a QoS en Transmisión de Video en la ESPOCH-DESITEL”

Autor: Poveda Cáceres, Mentor Iván, Pontón Baldeón, Jorge Rodrigo

La presente investigación tiene como conclusión principal lo siguiente:

“Al poder comparar las diferentes técnicas de encolamiento en base al parámetro de retraso temporal, se ha logrado establecer que existe una diferencia en la manera como gestionan el trafico cada una de ellas. Pese a que todas estas técnicas tratan de brindar una Calidad de Servicio a un tráfico determinado, se establece que para el caso específico video-IP la disciplina de encolamiento Custom Queueing (CG) es la que mejor se ajusta a los requerimientos en la transmisión de este tipo de tráfico en la red de la ESPOCH-DESITEL.”

## 2.2 FUNDAMENTACIÓN LEGAL

Se basará en la Ley Especial de Comunicaciones, en las normas y reglamentos de la Brigada de Selva N.17 “Pastaza”, en las normas y leyes de propiedad intelectual y en las leyes y reglamentos de la Universidad Técnica de Ambato.

## 2.3 CATEGORÍAS FUNDAMENTALES

### 2.3.1 Red de Inclusiones conceptuales

Variable Independiente



Variable Dependiente

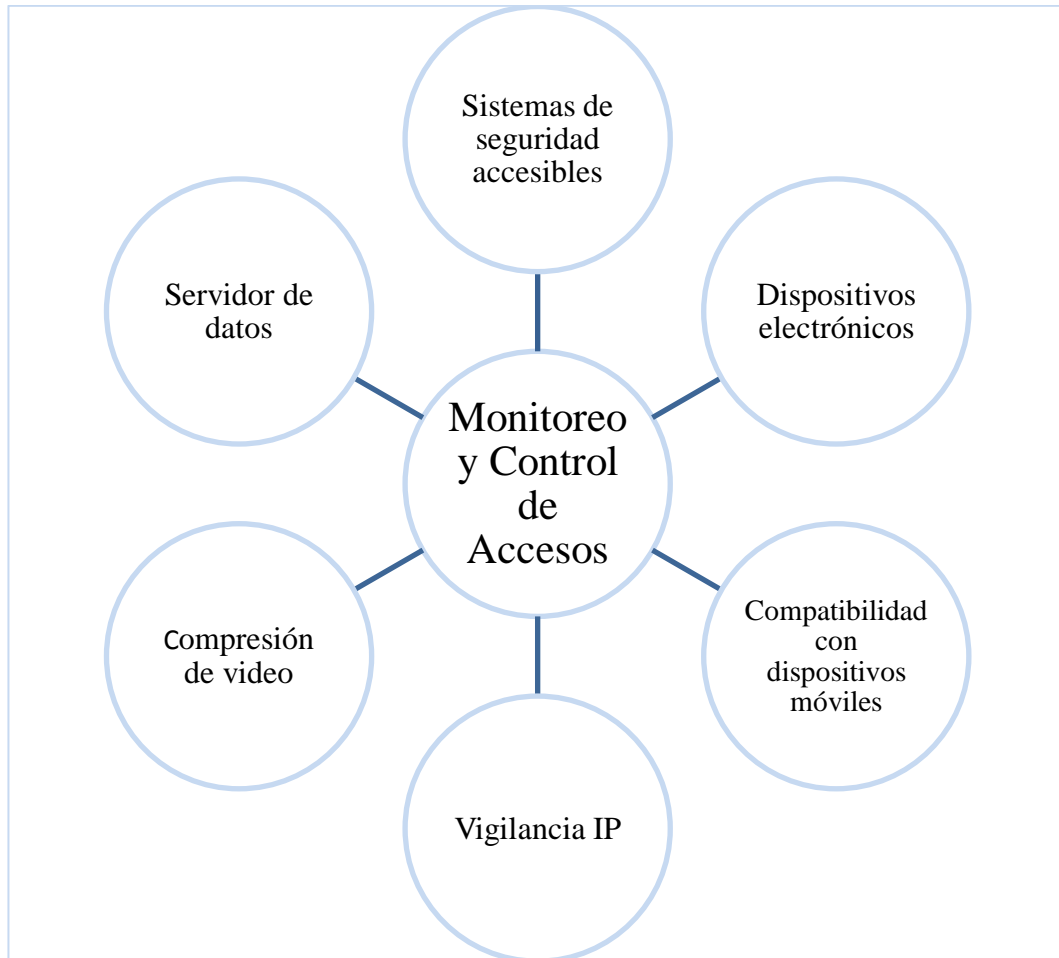


**Gráfico 2. 1 Categorías Fundamentales**  
**Elaborado por: Franklin Baldospin**

### 2.3.2 Constelación de ideas



**Gráfico 2. 2 Variable Independiente**  
Elaborado por: Franklin Baldospin



**Gráfico 2. 3 Variable dependiente**  
**Elaborado por: Franklin Baldospin**

### 2.3.3 Sistemas de Comunicaciones

“El sistema de comunicaciones es el conjunto de elementos que intervienen en el proceso de intercambio de información de un lugar a otro”<sup>1</sup>

La información que se transmite entre receptor y emisor debe adaptarse al canal de transmisión, ello implica disponer de un soporte adecuado a través del cual pueda viajar la información. Los sistemas de comunicaciones utilizan básicamente dos tipos de soporte descritos a continuación:

---

<sup>1</sup> **SANTILLANA**, *Los Sistemas de Comunicación*, Primera Edición. Grupo Prisa, España, Marzo 2000.

- Comunicación cableada, tiene lugar a través de líneas o cables (cobre) que unen emisor y receptor. La información se transmite mediante impulsos eléctricos.

La fibra óptica permite transmitir de forma simultánea miles de señales utilizando señales lumínicas en diferentes modulaciones sin pérdida.

- Comunicación inalámbrica tiene lugar en el propio espacio, concretamente en la atmósfera terrestre, el aire. La información se transmite mediante ondas de radio.

### **2.3.4 Características de un Sistema de Comunicaciones**

Las características de todo sistema de comunicaciones son:

- Convergencia tecnológica
- Prestaciones QoS (calidad)
- Óptima fidelidad
- Transmitir una gran cantidad de información
- Ocupar lo mínimo de ancho de banda
- Bajo costo (complejidad)

### **2.3.5 Convergencia tecnológica**

“La convergencia tecnológica es la tendencia de diferentes sistemas de comunicaciones a adaptarse a la evolución en cuanto a dispositivos y sus tecnologías, creando nuevas posibilidades”<sup>2</sup>

Hoy en día estamos rodeados por un mundo multimedia convergente con dispositivos remotos (Ipad, Iphone, Readers, Smartphones) adaptándose continuamente para satisfacer la demanda.

---

<sup>2</sup> **Convergencia tecnológica**, *Creative Commons*; [http://Convergencia\\_tecnologica.blogspot.com/](http://Convergencia_tecnologica.blogspot.com/)

### **2.3.6 Prestaciones QoS**

QoS o Calidad de Servicio son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado, brindando una calidad de servicio excelente, especialmente importante para ciertas aplicaciones tales como la transmisión de datos, video o voz.

### **2.3.7 Comunicaciones M2M**

“La comunicación M2M (máquina a máquina) es un sistema de comunicaciones que permite el intercambio de datos entre dos máquinas remotas, controlando y supervisando diferentes procesos automatizados”<sup>3</sup>.

Las comunicaciones M2M usan una variedad de medios, red local (LAN), red híbrida y red remota (WLAN), con distintos dispositivos conectados, incluyendo sensores, etiquetas de identificación, portátiles y máquinas.

### **2.3.8 Elementos de una Comunicación Máquina a Máquina**

Los elementos fundamentales que aparecen en todos los entornos máquina a máquina son los siguientes:

- Máquinas que gestionan: Alarmas, sensores, paneles informativos, cámaras, tele comando de video.
- Dispositivo Máquina a máquina: dispositivo conectado alámbrica o inalámbrica a un servidor remoto.
- Red de comunicación: pueden ser de dos naturalezas principalmente, a través de cable PLC, Ethernet, RTC, RDSI, ADSL o bien a través de redes inalámbricas GSM/UMTS/HSDPA, Wifi, Bluetooth, RFID.

---

<sup>3</sup> DELGADO, Antonio. Comunicaciones M2M, Grupo EROSKY, Bizkaia. Febrero 2010

### **2.3.9 Características de Comunicaciones M2M**

Las características de las Comunicaciones M2M son las siguientes:

#### **a) Calidad de servicio (QoS)**

La calidad de servicio son tecnologías que garantizan la transmisión de cierta información en un tiempo dado, es necesario especificar cuál es la apropiada a cierta aplicación, por ejemplo, en la vídeo-vigilancia se requiere una mayor prioridad que otros sistemas. Los elementos de red pueden priorizar el reenvío de paquetes para asegurar la recepción de datos específicos.

#### **b) Alta fiabilidad**

Es un protocolo del sistema y su implementación asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado, la alta fiabilidad se obtendrá desplegando centros de datos geo-redundantes, también se pueden desplegar herramientas de supervisión de red para medir indicadores de resultados.

#### **c) Operaciones y desarrollo simplificados**

El uso de herramientas de red seleccionadas puede simplificar operaciones y desarrollo de aplicaciones, proporcionando un Gateway o proxy permitiendo un uso más eficiente de la red y escalabilidad mejorada.

#### **d) Gestión de dispositivos**

La gestión de dispositivos incluye configuración, supervisión y diagnósticos así como actualizaciones de software y firmware, permitiendo el monitoreo remoto y obteniendo información general del lugar a vigilarse.



### **2.3.10 Ventajas de un Modelo Máquina a Máquina**

Con la introducción de Internet, los módems GSM y la amplia cobertura de los operadores celulares, el modelo M2M muestra las siguientes ventajas:

- Reducción de las interfaces manuales.
- Reducción del personal de control e inspección.
- Aceleración de los procesos.
- Control remoto.
- Amplio espectro en tecnologías.

### **2.3.11 Supervisión Local**

La red de comunicación que utiliza el modelo máquina a máquina localmente difiere según el tipo de equipo, se puede emplear desde una conexión por cable, como ADSL con los protocolos RTC, RDSI, PLC, o una red híbrida en conjunto con tecnologías GPRS, 3G o Wifi las mejores para la conectividad.

### **2.3.12 Supervisión Remota**

La supervisión remota permite acceder al vídeo en tiempo real en cualquier momento desde cualquier dispositivo, las tecnologías más utilizadas son las siguientes:

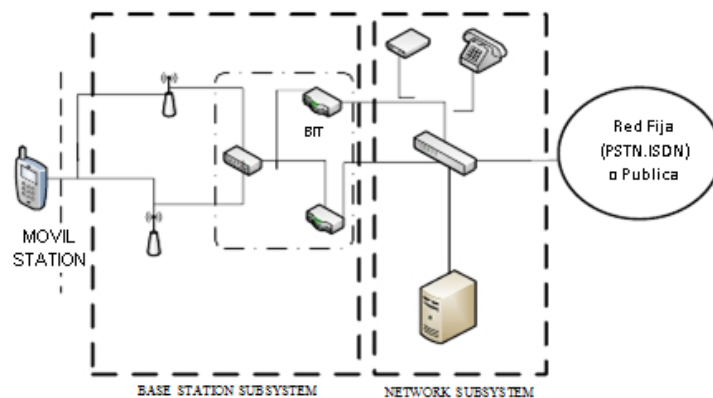
### **2.3.13 Tecnología GSM**

El sistema global para las comunicaciones móviles (GSM), es un sistema estándar, libre de telefonía móvil digital, constituido por todos los medios de transmisión y conmutación necesarios que permiten conectarse a través de su teléfono, computador a los diferentes servicios que oferta el internet. “GSM se

considera, por su velocidad de transmisión y otras características, un estándar de segunda generación (2G)<sup>4</sup>.

### 2.3.13.1 Arquitectura de una Red GSM

Una red GSM es constituida por tres elementos: el terminal, la estación- base (BSS) y el subsistema de red o nudo. Adicionalmente existen centros de operación establecidos por las operadoras, para monitorizar el estado de la red como a continuación se muestra en el gráfico 2.4:



**Gráfico 2. 4 Arquitectura de una Red GSM**  
**Elaborado por: Franklin Baldospin.**

#### a) MS (Mobile Station)

Terminal de abonado. Hace referencia al dispositivo (teléfono móvil), pero no a la identidad del suscriptor, que es facilitada por la tarjeta SIM.

#### b) BTS (Base Station)

Es un emisor/receptor de radio capaz de enlazar las estaciones móviles con la infraestructura fija de la red. Una estación base garantiza la cobertura radioeléctrica en una célula de la red, proporcionando el punto de entrada a la red. Las estaciones base pueden ser controladas localmente o bien remotamente a través de su controlador de estación base.

<sup>4</sup> **JAIRO Amaya**, *SISTEMAS GSM-GPRS*, Salamanga, Tercera Edición, Marzo 2009

**c) MSC (Mobile Switching Centre)**

Conmutador de red encargado de interconectar la red de telefonía convencional con la red radiotelefónica. Se encarga además de acceder al centro de autenticación para verificar derechos de los clientes, así como de participar en la gestión de movilidad de los abonados y su localización en la red.

**d) BSC (Base Station Controller)**

Controlador encargado de gestionar una o varias estaciones base. Actúa como un concentrador para el tráfico de los abonados y como un enrutador hacia la estación base destinataria en caso de tráfico proveniente de un conmutador.

**e) HLR (Home Location Register)**

Base de datos que contiene información relativa a los abonados de una red. Describe a su vez las opciones y servicios contratados por el abonado y aquellas opciones a las que tiene acceso. Se almacena además la última localización conocida del abonado y el estado de su terminal (fuera de servicio, encendido, en comunicación...). Para identificar a un abonado asociado a un terminal móvil se utiliza cierta información almacenada en la tarjeta SIM.

**f) VLR (Visitor Location Register)**

Base de datos asociada a un conmutador MSC (centro de conmutación móvil) que almacena la identidad de los abonados itinerantes de la red. Su funcionalidad es importante, ya que se utiliza para controlar la ubicación de un abonado.

**g) AUC (AUthentication Centre)**

Base de datos que almacena información confidencial de cada abonado de la red. Para autenticarse en dicha base de datos es necesario que el abonado acceda a su tarjeta SIM (mediante su código PIN) para que ésta, mediante un protocolo de petición-respuesta, sea capaz de dar por válida la identidad del usuario en la red, momento en el cual no se deniega el acceso a la red y se consulta al HLR para conocer las opciones y servicios con los que el usuario puede contar.

### **2.3.13.2 Ventajas y Desventajas de la Red GSM**

Ventajas:

- Identificación de los usuarios de los móviles mediante el uso de un chip denominado Simcard.
- Posibilidad de almacenar información en la tarjeta SIM, que facilita el traspaso de diferentes servicios (Mensajería, Agenda).
- Extensa área de cobertura, utilizando Roaming obteniendo cobertura para realizar y recibir llamadas desde diferentes partes del mundo con tu mismo dispositivo y misma línea.
- Provee claridad y calidad en los servicios de voz
- Permite la transición y recepción de información multimedia
- Múltiples servicios de mensajería, identificador, correo de voz

Desventajas

- Los usuarios comparten el mismo ancho de banda, por lo que existen interferencias.
- Puede presentar interferencia con determinados dispositivos electrónicos.
- El nivel de seguridad respecto a otras tecnologías como CDMA es de menor calidad.
- Falta de cobertura en ciertas zonas agrestes.
- Requiere un número considerado de radios base para garantizar una gran cobertura.

### **2.3.14 Tecnología GPRS**

La tecnología GPRS o servicio general de paquetes vía radio es una extensión del GSM para la transmisión de datos no conmutada, o por paquetes, permite velocidades de transferencia de 56 a 144 kbps.

Con GPRS se pueden utilizar servicios como Wireless Application Protocol (WAP), servicio de mensajes cortos (SMS), servicio de mensajería multimedia (MMS) e Internet.

La migración de una red GSM a una red UMTS es sencilla puesto que las antenas sufren sólo ligeros cambios y los elementos nuevos de red necesarios para GPRS serán compartidos en el futuro con la red UMTS.

### 2.3.15 Ventajas

- Utilización de la voz y los datos a través del teléfono móvil, por medio de la separación de canales que transmiten de forma paralela. Podrá mantener conversaciones sin cortar la transmisión de datos.
- Velocidad de transmisión de datos, igualándose a la líneas fijas, la velocidad cuadruplicara el rendimiento de la tecnología GSM.
- Facturación basada en volumen de datos transferidos no por el tiempo de conexión.

### 2.3.16 Sistemas de Supervisión

Un sistema de supervisión permite gestionar toda la información relativa al estado de nuestras redes; la cual, debe ser ágil para garantizar que el flujo de datos optimice el funcionamiento del mismo, de este modo se reduzca las probabilidades de fallos, a continuación se representa en el gráfico 2.5 el proceso:



**Gráfico 2. 5 Sistema de Supervisión**

**Elaborado por: Phil Bartle, PhD<sup>5</sup>**

---

<sup>5</sup> **PHIL Bartle, PhD.** *Red y Redes*, España (1999), p. 127

### **2.3.17 Sistemas de seguridad**

Un sistema de seguridad es un conjunto de dispositivos colocados estratégicamente en el perímetro de un sitio específico para detectar la presencia, irrupción, o invasión del mismo.

### **2.3.18 Clasificación de los sistemas de seguridad**

La clasificación de los sistemas de seguridad electrónica (SSE) se realiza básicamente desde dos criterios, la cantidad de sitios a proteger y la aplicación del sistema así:

- SSE locales, diseñado para la seguridad de un lugar puntual,
- SSE distribuido es un conjunto de SSE locales adaptados a cada sitio protegido que además trabajan en conjunto a través de un sistema de Telecomunicación.

Los cuatro grandes bloques de aplicación de los sistemas de seguridad son, robo, atraco, anti hurto, incendios y sistemas especiales.

- Sistemas contra robo/asalto
- Circuitos Cerrados de Televisión (CCTV)
- Sistemas de control de los accesos
- Sistemas de aviso de incendio

### **2.3.19 Sistemas de vigilancia**

Los sistemas de vigilancia dan seguridad a las personas, vigilan espacios de posible intromisión o controlar ciertas áreas públicas, no son autónomos, sino que van compaginados con los sistemas de alarma, dispositivos de detección (sensores, detectores).

### 2.3.20 Características del Sistema de Vigilancia

Las características de un sistema de vigilancia son las siguientes:

- a) **Robustez:** Actualmente el sistema de vigilancia cuenta con VPN y dispositivo de gestión de vídeo que controla todas las cámaras del sistema y a través del cual se pueden visualizar las imágenes en tiempo real sin generar fallos o bloquearse.
- b) **Seguridad:** Para asegurarse que nadie sin permiso pueda visualizar las imágenes del sistema de tele vigilancia, el dispositivo de gestión de vídeo está provisto de un sistema de seguridad basado en usuario/contraseña.
- c) **Flexibilidad:** La capacidad de adaptación del sistema de video vigilancia es posible ya que su flexibilidad permite conectar varias cámaras a la vez con diferentes características (cámaras fijas, cámaras con detección de movimiento, mini-cámaras, cámaras motorizadas, etc.), incluso se puede llegar a controlar las cámaras que tengan funcionalidades de zoom y/o de movimiento.
- d) **Accesibilidad:** Acceso a distintas aplicaciones del sistema, utilizando la red existente en el lugar de monitoreo, o se puede ingresar con una IP fija que hace posible un control remoto desde cualquier lugar mediante internet.

### 2.3.21 Clasificación de los sistemas de Vigilancia

Los sistemas de vigilancia se pueden clasificar en dos grandes grupos dependiendo de su utilización así:

- Los CCTV, o circuitos cerrados de televisión, se pueden encontrar trabajando como apoyo del vigilante de seguridad.
- En sistemas automáticos o independientes, los equipos almacenan información de los eventos como son imágenes, datos (sensores, detectores), alertas a eventos (alarmas); las cuales se pueden monitorear desde cualquier lugar.

### 2.3.22 Sistemas de Monitoreo

“Los sistemas de monitoreo tienen como finalidad el minimizar las falsas alarmas y asegurar el efectivo funcionamiento del sistema o sistemas adyacentes en todo momento”<sup>6</sup>

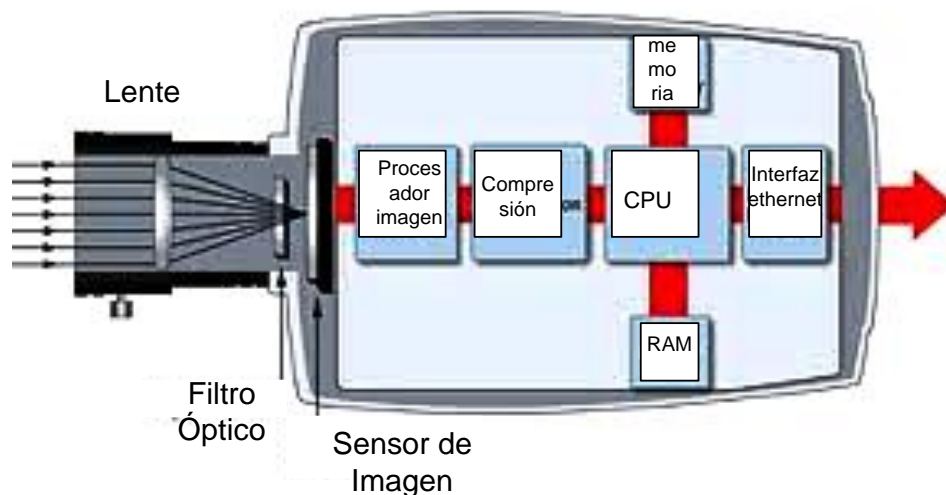
### 2.3.23 Elementos de un sistema de Monitoreo

Los sistemas de monitoreo se componen de los siguientes dispositivos:

- Cámaras de video (fijas, domo, PTZ).
- Componentes grabadores y almacenadores de imagen.
- Componentes de transmisión de la señal de vídeo.

### 2.3.24 Cámaras

Una cámara es un dispositivo diseñado para enviar las señales (video, audio) hacia un equipo receptor sea esto mediante una red local (LAN), o inalámbricamente a continuación se muestra los componentes de una cámara IP en el gráfico 2.6:



**Gráfico 2. 6 Componentes Cámara**  
**Elaborado por: Franklin Baldospin**

<sup>6</sup> Ing. CONSENTINO Luis, *Control de Accesos*, Editorial RNDS, México, Abril 2000.



Primero, la luz que proviene de la óptica es descompuesta al pasar por un prisma o filtros ópticos, ajustados automáticamente por el sensor de imagen seguido están los captadores y procesadores de imagen, circuitos integrados con tecnología CCDs o CMOS los cuales se encargan de la compresión, amplificación, codificación y almacenar temporalmente en su memoria RAM de la información para enviarla a través de su interfaz de comunicación.

La salida básica, video compuesto VBS, sigue siendo la del sistema analógico de TV elegido: PAL, NTSC o SECAM. Todas las funciones de la cámara están controladas con un procesador, el cual se comunica con los paneles de control, tanto de ingeniería (MSP) como de explotación (OCP), y es el encargado de realizar los ajustes automáticos y/o manuales pertinentes.

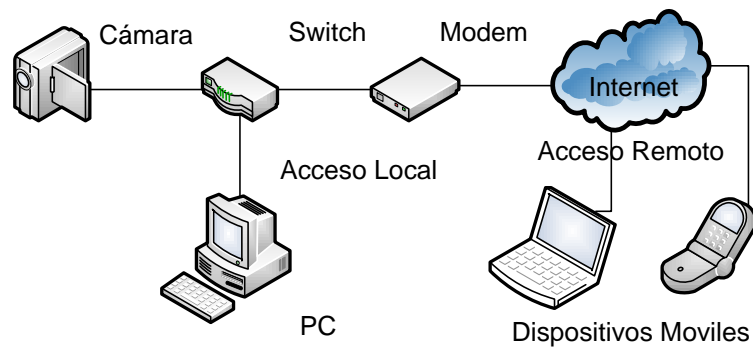
#### **2.3.24.1 Características de la Cámaras**

Una cámara tiene una gran variedad de funciones como:

- Activación mediante movimiento de la imagen
- Activación mediante movimiento de sólo una parte de la imagen
- Creación una máscara en la imagen, ocultar rostros
- Activación a través de otros sensores
- Control remoto para mover la cámara y apuntar a una zona
- Programación de una secuencia de movimientos en la propia cámara
- Posibilidad de guardar y emitir los momentos anteriores a un evento

La imagen y audio capturadas por las cámaras y micrófonos, se comprimen y transmiten por una red de datos Local o Internet ( LAN / WAN ) a través del equipo grabador el cual necesariamente debe estar conectado a internet y poder acceder desde uno o varios puntos en cualquier lugar del mundo (acceso remoto), y generar acciones de manera automática en respuesta a diferentes eventos a voluntad de un operador.

A continuación una red LAN con cámara en el gráfico 2.7:



**Gráfico 2. 7 Diseño de Red Básica**  
**Elaborado por: Franklin Baldospin**

#### 2.3.24.2 Visión en vivo

La visión en vivo es posible mediante el acceso remoto, la cámara se conecta a través de Internet a una dirección IP con las siguientes características.

- Las cámaras permiten al usuario visualizar el vídeo en vivo por Internet.
- El acceso a estas imágenes es totalmente restringido, su acceso es mediante una dirección IP, nombre de usuario y contraseña.

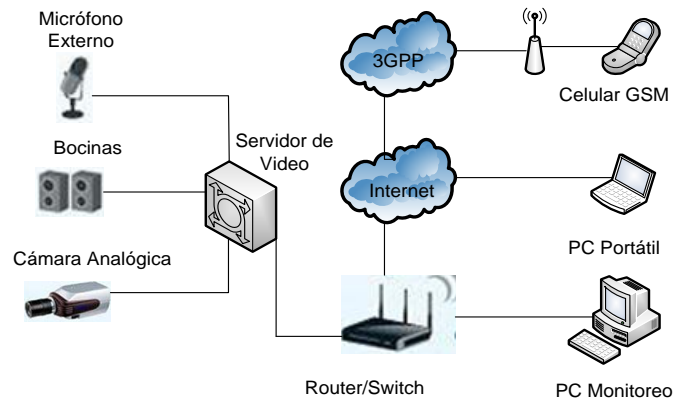
#### 2.3.25 Grabadores y Almacenadores de imagen.

Los componentes necesarios son:

- Servidores de Video / IP Video Servers
- Decodificadores de Video IP / IP Video Decoders

##### 2.3.25.1 Servidores de video

Los servidores de video son dispositivos que permiten la transición tecnológica entre los sistemas análogos de vigilancia (CCTV) y Vigilancia IP, permiten convertir una cámara análoga en una cámara IP, útil para usuarios análogos, que desean hacer la transición a Vigilancia IP.



**Gráfico 2. 8 Servidor de Video**  
**Elaborado por: Franklin Baldospin**

### 2.3.25.2 Codificadores y Decodificadores

Un codificador de vídeo digitaliza las señales de vídeo analógico y envía imágenes digitales directamente a través de una red IP.

### 2.3.25.3 Grabadores Digitales de Red / Network Video Recorders

Un Grabador digital de red es un equipo de almacenamiento de imágenes o vídeo además de arreglo de discos externos y un bus interno de mucha velocidad, con conexiones de red de alta velocidad segmentadas o totalmente separadas de otras redes (voz y datos) para no interferir anchos de banda.

### 2.3.26 Control de accesos

Un control de accesos es un dispositivo que tiene por objeto impedir el libre acceso del público en general a diversas áreas que denominaremos protegidas.

Son de dos tipos a continuación descriptos:

- Autónomos
- Con conexión a una PC

### **Sistemas Autónomos**

Los sistemas autónomos no necesitan ser conectados a una computadora para su funcionamiento tan solo mantiene una base de códigos en su memoria, dentro de estos sistemas podemos encontrarlos utilizados para el acceso vehicular a edificios.

### **Sistemas con conexión**

Los sistemas con conexión a la computadora, vienen generalmente con un software y se diferencian del número de puertas que controla, así como de su capacidad de conexión con la red del cliente. Estos sistemas disponen de una memoria que mantiene la base de datos de los usuarios, así como una unidad de back up en caso de pérdida de energía, pueden también funcionar como autónomos.

Un sistema típico se compone de los siguientes componentes:

- Lectora de proximidad
- Tarjetas de proximidad
- Módulo o tarjeta de control
- Cerradura eléctrica, chapa electromecánica
- Botón de emergencia
- Una computadora de control

#### **2.3.27 Ventajas de un sistema de control de accesos**

Las siguientes ventajas de un control de accesos:

- Seguridad de sus instalaciones
- Ahorro del tiempo dedicado a la gestión

- Incremento de ingresos
- Modernización de la imagen de sus instalaciones
- Aumento de competitividad y servicio

## **2.4 HIPÓTESIS**

¿El deficiente sistema de supervisión en la zonas sensibles de alta vulnerabilidad incide en el monitoreo y control de la BRIGADA SELVA N°17 PASTAZA?

## **2.5 SEÑALAMIENTO DE VARIABLES**

**Variable Independiente:** Sistema de Supervisión

**Variable Dependiente:** Monitoreo, y Control de Accesos

## **CAPÍTULO III**

### **MARCO METODOLÓGICO**

#### **3.1 ENFOQUE DE LA INVESTIGACIÓN**

La presente investigación tuvo un enfoque cualitativo ya que la obtención de los datos fue participativa para los diferentes departamentos de la brigada brindando una perspectiva desde el interior del problema y asumiendo una realidad dinámica de la misma y cuantitativo debido a que la indagación fue objetiva, normativa, externa, explicativa, realista, encaminada a la comprobación de la hipótesis.

#### **3.2 MODALIDAD BÁSICA DE INVESTIGACIÓN**

##### **3.2.1 Investigación de Campo**

La presente investigación tuvo una modalidad de investigación de campo para recolectar información del problema antes descrito obteniendo datos precisos y concretos de los requerimientos de la Brigada N°17 Selva siendo la herramienta más adecuada, la encuesta realizada.

##### **3.2.2 Investigación Bibliográfica**

La investigación se basó en la búsqueda de información científica relacionada con la video-vigilancia y control de acceso remoto, esta técnica se la llevo a cabo en Bibliotecas, Internet, con lo cual se analizó y evaluó los diferentes temas de investigación.

### **3.3 TIPOS DE INVESTIGACIÓN**

#### **3.3.1 Exploratorio**

Esta investigación permitió reconocer y sondear el problema desde una mejor óptica; como acción preliminar para obtener una idea general del problema y la factibilidad para solucionarlo eficazmente.

#### **3.3.2 Descriptivo**

Fue descriptivo ya que brindó la oportunidad para detallar y explicar las particularidades del problema es decir sus causas y consecuencias.

### **3.4 POBLACIÓN Y MUESTRA**

Para el desarrollo de la investigación se trabajó con los puntos de vigilancia en todo el Batallón por el cual se consideró una población total de 30 personas, pertenecientes a la unidad las cuales son encargadas de las comunicaciones dentro y fuera del batallón; al ser la población pequeña todos pasan a ser parte de la muestra.

### 3.5 OPERACIONALIZACIÓN DE VARIABLES

#### 3.5.1 Operacionalización de la variable independiente: Sistemas de Supervisión

CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ITEMS BASICOS	INSTRUMENTO
Encargada de gestionar toda la información perteneciente al sistema la cual debe ser ágil para garantizar que los informes nos sirva para optimizar el funcionamiento, reduciendo las probabilidades de errores en la misma.	<p>Gestionar</p> <p>Información</p> <p>Garantizar</p> <p>Optimizar el funcionamiento</p> <p>Reduciendo errores</p>	<p>Proceso de administrar los recursos eficientemente</p> <p>Conjunto de datos organizados</p> <p>Asegurar en mantener el funcionamiento de un sistema.</p> <p>Procurar que una acción se ejecute y funcione más rápidamente</p> <p>Disminuir las acciones mal tomadas</p>	<p>¿Es necesario un sistema de gestión para la seguridad y vigilancia en la institución?</p> <p>¿Cuál es el método utilizado para la obtención de la información en el Batallón?</p> <p>¿El sistema existente garantiza la veracidad y exactitud de la información obtenida en la zona monitoreada?</p> <p>¿Se cuenta con un sistema que procure optimizar el funcionamiento del mismo en tiempo real?</p> <p>¿Se cuenta con acciones preventivas en el Batallón para la reducción de errores a nivel de supervisión?</p>	ENCUESTA

**Tabla 3. 1 Variable Independiente**  
**Elaborado por: Franklin Baldospin**



### 3.5.2 Operacionalización de la variable dependiente: Monitoreo, Control de Accesos

CONCEPTUALIZACION	DIMENSIONES	INDICADORES	ITEMS BASICOS	INSTRUMENTO
<p>Es la acción de ver el avance y eficacia de la información obtenida mediante los dispositivos de seguridad, para permitir o denegar el uso de un recurso particular hacia la protección de bienes y personas</p>	Avance y eficacia	Seguimiento y cumplimiento de objetivos	¿Existe un seguimiento de la información con el fin de lograr el cumplimiento de los objetivos propuestos por el batallón?	<b>ENCUESTA</b>
	Información obtenida	Almacenamiento y tratamiento de la información	¿La información obtenida es tratada y almacenada para su posterior utilización?	
	Dispositivos de seguridad	Cámaras Sensores Detectores	¿El batallón cuenta con cámaras, sensores y detectores de seguridad dentro recinto?	
	Permitir o denegar	Autenticación del personal	¿Cuál es el método de autenticación de personal a zonas sensibles del Batallón?	
	Protección de bienes y personas	Normas y Estándares de seguridad militar	¿Se está aplicando las normas y estándares adecuados para el manejo de la seguridad militar en el batallón?	

**Tabla 3. 2 Variable Dependiente**  
**Elaborado por: Franklin Baldospin**

### 3.6 TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN

La técnica que se utilizó en el presente proyecto fue la encuesta. Esta nos permitió establecer datos e información confiable por escrito. Fue realizada al personal que está directamente involucrado en el proyecto así como a los departamentos participativos en el mismo.

### 3.7 RECOLECCIÓN DE DATOS

PREGUNTAS BÁSICAS	
¿Para qué?	Para lograr los objetivos de la investigación
¿De qué personas u objetos?	Departamento de redes, y brigadistas
¿Sobre qué aspectos?	Realidad actual de la Institución en seguridad
¿Quién?	Investigador: franklin baldospin
¿Cuándo?	Seis meses a partir de la aprobación por parte del Honorable Consejo Directivo.
¿Dónde?	Instalaciones de la brigada selva N17
¿Cuántas veces?	Las necesarias
¿Qué técnicas de recolección?	Observación, entrevista y encuesta
¿Con qué?	Cuestionarios

**Tabla 3. 3 Recolección de datos  
Elaborado por: Franklin Baldospin**

### **3.8 PROCESAMIENTO DE LA INFORMACIÓN**

- Revisión crítica de la información recogida en la encuesta, de esta forma eliminar información defectuosa, contradictoria, incompleta, no pertinente, etc.
- Repetición de la recolección, en casos para corregir las fallas de contestación
- Para el procesamiento y análisis de la información se utilizó cuadros estadísticos para interpretar los resultados tabulados de las encuestas, posteriormente se determinó los recursos, para finalmente obtener los resultados sobre las deficiencias en el plan operativo de seguridad en la institución

### **3.9 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS**

Análisis de los resultados estadísticos, destacando tendencias relacionadas fundamentalmente de acuerdo con los objetivos e hipótesis.

- Interpretación de los resultados porcentuales, gráficos y estadísticos con apoyo del marco teórico, en el aspecto pertinente.
- Comprobación de hipótesis, para la investigación estadística conviene seguir la asesoría de un especialista en el tema.
- Restablecimiento de conclusiones y recomendaciones.

## CAPÍTULO IV

### 4.1 ANÁLISIS DE RESULTADOS E INTERPRETACIÓN

Luego de realizada la encuesta a las personas involucradas en los puntos de vigilancia del Batallón, se recogieron y procesaron los datos, de los cuales se obtuvieron los siguientes resultados:

Encuesta realizada al personal de turno en los puntos de vigilancia del Batallón Selva N° 17

#### Preguntas

1. ¿Considera usted que es necesario un sistema de supervisión actualizado para la seguridad y vigilancia en la Brigada Selva N°17?

ALTERNATIVA	PERSONAS	PORCENTAJE
SI	21	70%
NO	9	30%
TOTALES	30	100%

**Tabla 4. 1 Sistema de Supervisión**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**



**Gráfico 4. 1 Sistema de Supervisión**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**

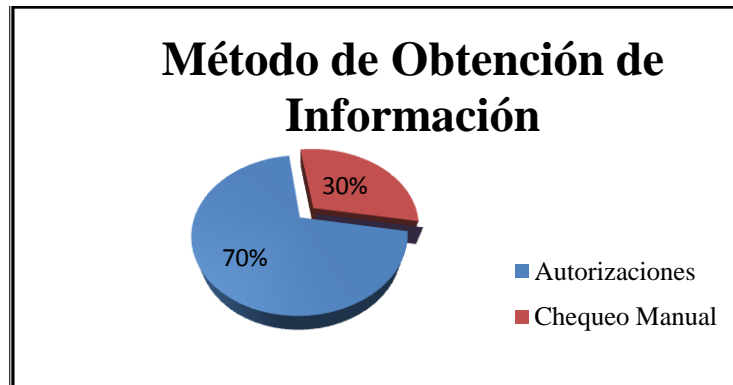
**Análisis**

De las 30 personas encuestadas; 21 contestaron que si correspondiente al 70%, y 9 personas contestaron que no correspondiente al 30%. La mayoría de las personas encuestadas opinan que existe la necesidad de un sistema de supervisión actualizado para la seguridad y vigilancia en la Brigada Selva N°17, ya que el método existente es obsoleto y precario, mientras que un mínimo de personas no considera necesario el sistema.

2. ¿Cuál es el método más utilizado para la obtención de la información relevante a seguridad en el Batallón?

<b>ALTERNATIVA</b>	<b>PERSONAS</b>	<b>PORCENTAJE</b>
Solicitud de Autorizaciones	<b>20</b>	<b>70%</b>
Chequeo manual	<b>10</b>	<b>30%</b>
<b>TOTALES</b>	<b>30</b>	<b>100%</b>

**Tabla 4. 2 Método de Obtención de Información**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**



**Gráfico 4. 2 Método de Obtención de Información**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**

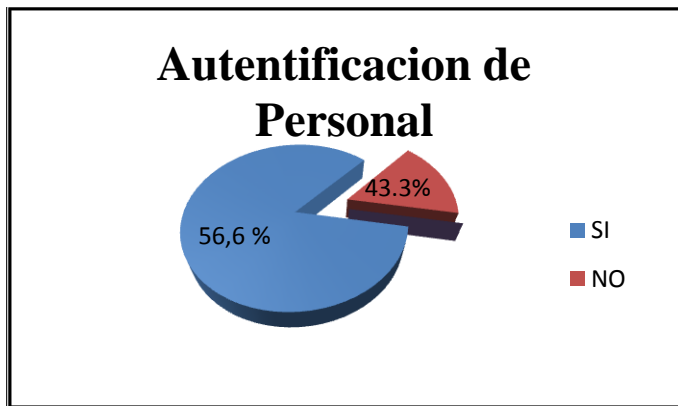
### **Análisis**

Los valores obtenidos mediante la encuesta exponen un 70% del personal el cual está en concordancia que el método para la obtención de datos es una solicitud de autorización remitida por la persona a cargo en cuanto al 30% opina que simplemente se utiliza un chequeo manual como método de control.

3. ¿Estaría usted de acuerdo con la implementación de un sistema de autenticación de personal a zonas sensibles del batallón?

<b>ALTERNATIVA</b>	<b>PERSONAS</b>	<b>PORCENTAJE</b>
SI	<b>17</b>	<b>56,6%</b>
NO	<b>13</b>	<b>43.3%</b>
<b>TOTALES</b>	<b>30</b>	<b>100%</b>

**Tabla 4. 3 Sistema de Autenticación de Personal**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**



**Gráfico 4.3 Autenticación Personal**  
**Fuente: La encuesta**  
**Elaborado por: Franklin Baldospin**

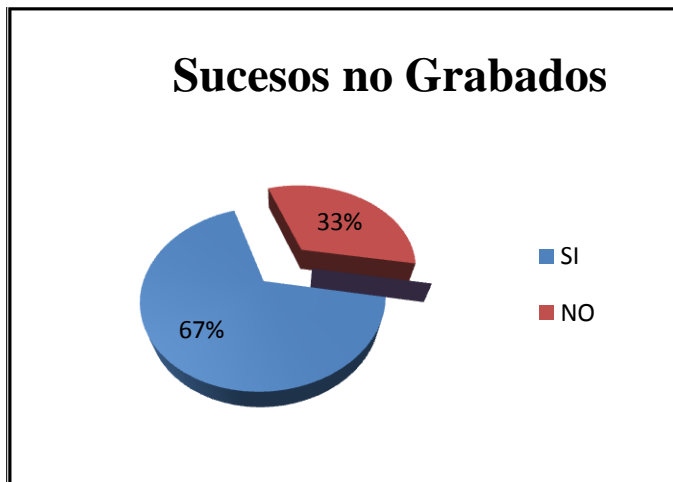
**Análisis**

Realizada la encuesta se obtiene como resultado: 17 individuos contestaron que si correspondiente al 56,6%, y 13 encuestados contestaron que no correspondiente al 43,3%, resultados que indican la opinión mayoritaria; la cual está de acuerdo con la implementación de un sistema de autenticación de personal a zonas sensibles del batallón, mientras que un mínimo de personas considera que es innecesaria la implementación del sistema.

4. ¿Tiene usted conocimiento de sucesos indebidos que se hayan efectuado en la institución, a los cuales no se les haya aplicado la respectiva sanción debido a la falta de pruebas que corroboren dicha infracción?

ALTERNATIVA	PERSONAS	PORCENTAJE
SI	20	67%
NO	10	33%
TOTALES	30	100%

**Tabla 4.4 Infracciones No corroboradas**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**



**Gráfico 4. 4 Sucesos no Grabados**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**

### Análisis

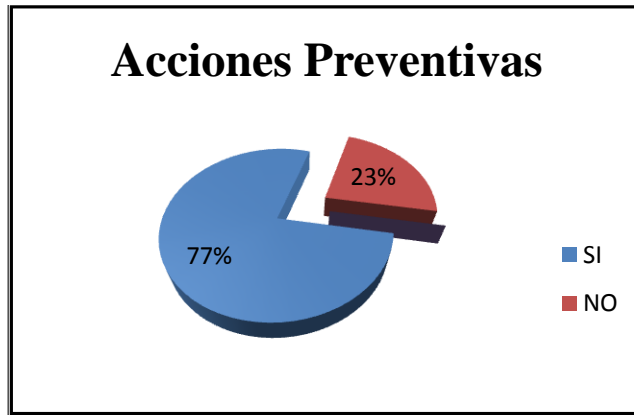
La existencia de hechos delictivos en la institución, de los cuales no exista pruebas que corroboren dicha infracción para su respectiva sanción es la percepción del 67% de las personas encuestadas, mientras que el 33% opinan que dichas infracciones no existen dentro de la institución de manera que no es necesario un sistema de vigilancia

5. ¿Se cuenta con acciones preventivas en el Batallón para la reducción de errores a nivel de supervisión?

ALTERNATIVA	PERSONAS	PORCENTAJE
SI	23	77%
NO	7	23%
TOTALES	30	100%

**Tabla 4. 5 Acciones Preventivas**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**





**Gráfico 4. 5 Acciones Preventivas**

**Fuente: La encuesta**

**Elaborado por: Franklin Baldospin**

**Análisis**

De acuerdo a las normas de seguridad del Batallón Selva N°17 existe un plan de acción preventivo referente a la reducción de errores a nivel de supervisión antecedente del cual 23 personas están de acuerdo correspondiente al 77%, y 7 personas contestaron que no correspondiente al 23%, por razones de falta de conocimiento en cuanto a la existencia de aquel plan.

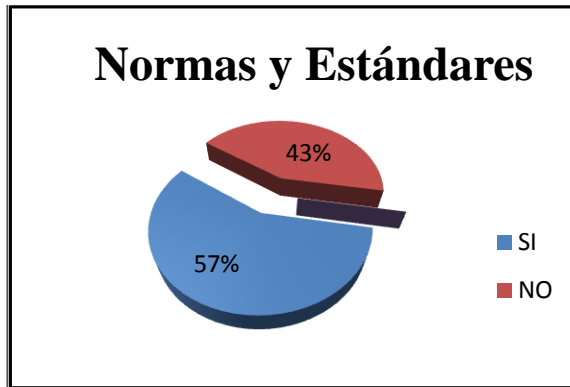
6. ¿Se está aplicando las normas y estándares adecuados para el manejo de la seguridad militar en el batallón?

ALTERNATIVA	PERSONAS	PORCENTAJE
SI	17	57%
NO	13	43%
TOTALES	30	100%

**Tabla 4. 6 Normas y Estándares**

**Fuente: La Encuesta**

**Elaborado por: Franklin Baldospin**



**Gráfico 4. 6 Normas y Estándares**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**

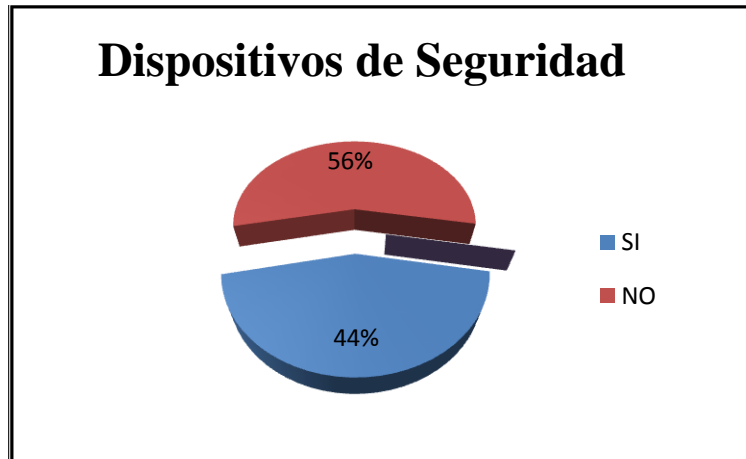
**Análisis**

La seguridad militar en el Batallón se rige en base a normas y estándares específicos de los cuales el 57% del personal correspondiente a 17 personas encuestadas opinan que se está cumpliendo con las normas de seguridad; en cuanto al 43% contestaron que no se aplican debido al creciente índice de errores existentes en las bodegas de material bélico.

7. ¿El Batallón cuenta con cámaras, sensores y detectores de seguridad dentro del recinto para la vigilancia y control del mismo?

ALTERNATIVA	PERSONAS	PORCENTAJE
SI	13	44%
NO	17	56%
TOTALES	30	100%

**Tabla 4. 7 Dispositivos de Control y Vigilancia**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**



**Gráfico 4. 7 Dispositivos de Seguridad**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**

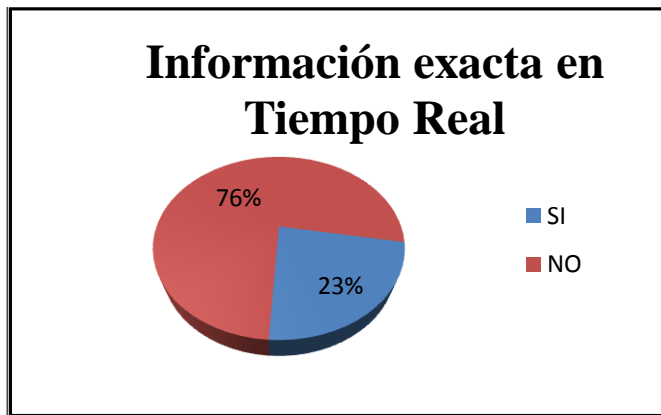
**Análisis**

La encuesta revela la existencia de varios dispositivos de seguridad existentes y funcionando opinión manifestada por el 44% del personal, por otro lado el 56% opinan que no existe dispositivo alguno y de existir se encuentran en un mal funcionamiento por la falta de un mantenimiento en los mismos.

8. ¿El sistema existente garantiza la veracidad y exactitud de la información obtenida en la zona monitoreada en tiempo real?

ALTERNATIVA	PERSONAS	PORCENTAJE
SI	7	23,3
NO	23	76,6
TOTALES	30	100%

**Tabla 4. 8 Información Fiable y Exacta**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**



**Gráfico 4. 8 Información en Tiempo Real**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**

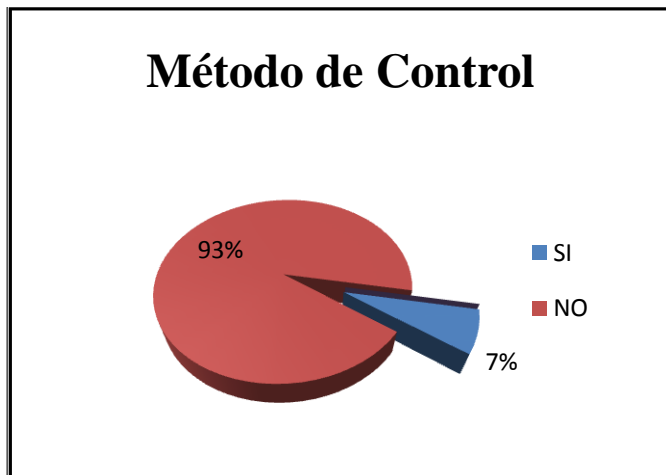
**Análisis**

Realizada la encuesta el resultado es: 7 personas contestaron que si correspondiente al 23,3%, y 23 individuos contestaron que no correspondiente al 76,6%, resultados que indican la opinión mayoritaria; la cual cree que el sistema existente no garantiza la veracidad y exactitud de la información ya que puede ser manipulada e inexacta, conservada de manera manual convirtiéndose en una manera engorrosa y no eficiente, mientras que un mínimo de personas considera que es fiable y veras la información recopilada.

9. ¿Existe algún método de control de personal actual a zonas sensibles del batallón?

ALTERNATIVA	PERSONAS	PORCENTAJE
SI	2	6.7%
NO	28	93.3%
TOTALES	30	100%

**Tabla 4. 9 Control de Personal**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**



**Gráfico 4. 9 Método de Control**  
**Fuente: La Encuesta**  
**Elaborado por: Franklin Baldospin**

#### **Análisis**

Un porcentaje del 93% de total de encuestados opinan que no existe método de control de personal actual del cual se pueda obtener datos veraces y un 6% en este caso indica q si existe método, acotando la ineficaz y obsoleto del mismo; lo cual revela la necesidad y disponibilidad, de la implementación de un sistema de control en el batallón tanto para la seguridad interna de las zonas más vulnerables del mismo.

## **CAPÍTULO V**

### **CONCLUSIONES Y RECOMENDACIONES**

Luego del proceso de investigación realizado, se apuntan las siguientes conclusiones y recomendaciones

#### **5.1 Conclusiones**

- El factor responsable del deficiente sistema de supervisión existente es la falta de actualización y empleo de nuevas tecnologías asociadas a la video-vigilancia motivo por el cual la Brigada Selva N°17 no posee un eficaz control y monitoreo de las zonas más sensibles como bodegas de material peligroso siendo fundamental para el batallón la integridad y seguridad de su personal es por tal motivo se presenta un prototipo el cual cumple con las normas y estándares de seguridad adecuados.
- El método utilizado para el control de accesos sobre todo en las áreas que es necesario un registro estricto debido al material existente es totalmente ineficaz; ya que el chequeo manual da lugar a errores y fallas ocasionando que no se pueda obtener datos reales y confiables.

- De acuerdo a los datos obtenidos por medio de la encuesta realizada al personal de la Unidad de Comunicaciones del Batallón Selva N°17, se confirmó la total aceptación en cuanto a la implementación de un prototipo de un Sistema de Monitoreo y Control remoto mediante internet a la Bodega N°3, ya que el mismo contribuirá a un control eficaz y adecuado del material allí almacenado, alcanzando altos niveles de seguridad.
- La mayoría del personal concuerda que a pesar de existir procedimientos preventivos para la reducción de errores en el manejo de control de acceso de personal y seguimiento del mismo ha acontecido sucesos o infracciones deliberadas las cuales por falta de una información real y datos fiables que corrobore dicha infracción no se ha podido llevar a cabo la sanción correspondiente.

## **5.2 Recomendaciones**

- Se recomienda destinar los recursos necesarios para mejorar el deficiente sistema de monitoreo existente invirtiendo en tecnología 4G actual como lo plantea el prototipo de red de video-vigilancia totalmente funcional, por lo cual el Batallón deberá presupuestar el dinero siendo de vital importancia para la toma de decisiones de acuerdo a los requerimientos de seguridad existentes y a su vez alcanzar los objetivos planteados.
- Se debe aplicar un sistema de control de accesos adecuado con el fin de controlar el accesos de personal a zonas restringidas como bodegas de armamento, así se podrá coordinar las acciones a tomar en caso de existir algún evento que ponga en peligro al recinto, evaluando el grado de rapidez, seguridad y confiabilidad del sistema permitiendo cumplir con las normas militares ya establecidas.

- Adóptese un mecanismo actual de Control de Acceso beneficiándose de la tecnología de monitoreo local o remoto mediante red o internet con el cual se podrá brindar mayor seguridad a la Bodega N°3 del recinto la cual almacena armamento de uso diario.
- Se recomienda analizar los procedimientos actuales para el control de personal y así considerar la utilización de equipos y dispositivos de seguridad tanto en video-vigilancia como control de accesos para el monitoreo, los cuales ayudaran al correcto manejo de información real optimizando tiempo y recursos.



## **CAPÍTULO VI**

### **PROPUESTA**

#### **6.1 TEMA**

“Red de Video-Vigilancia con Tecnología GSM-GPRS para el monitoreo y control de accesos a zonas de alta vulnerabilidad en la BRIGADA SELVA N°17 PASTAZA”

#### **6.2 DATOS INFORMATIVOS**

**Institución Ejecutora:** Brigada Selva N °17 Pastaza

**Ubicación:** Oriente Ecuatoriano

**Parroquia:** Shell

**Cantón:** Puyo

**Provincia:** Pastaza

**Calle:** Av. Padre Luis Jácome cc 17pastaza@hotmail.com

#### **Beneficiarios**

El principal beneficiario será la Brigada Selva N°17 Pastaza, y todo el personal involucrado en el monitoreo y control de las bodegas del recinto militar

#### **Equipo Técnico Responsable**

El desarrollo de la propuesta lo realizo el autor del presente trabajo investigativo Franklin Baldospin, Unidad de Comunicaciones Cap. Franklin Oña Toapanta.

### **6.3 ANTECEDENTES DE LA PROPUESTA**

Después de haber recolectado la información y analizarla se observó la necesidad de evaluar la red existente en cada una de las unidades; así se determinará los puntos más vulnerables de la Brigada.

Adicionalmente, la unidad de comunicaciones no cuenta con un monitoreo tanto de las unidades operativas, bodegas de almacenamiento bélico, bodegas de equipos y zonas restringidas lo que con lleva a la demora en la comunicaciones y coordinación en cada una de la unidades del recinto ya que si bien es cierto se aplica procedimientos de vigilancia y seguridad, estos métodos no ayudan a la optimización de recursos.

No existe un control de accesos adecuado, sea este interno en cada celda de armamento, correspondiente a la unidad o bodega, y externo tanto en acceso principal como ventanas de ventilación; por lo cual es necesario una investigación aplicando las normas de seguridad y procedimientos que permitan la implementación de dispositivos de control, efectivos y eficaces.

### **6.4 JUSTIFICACIÓN**

La finalidad de la presente propuesta es proporcionar a las autoridades de la Brigada una solución al deficiente sistema de supervisión de las zonas sensibles y de alta vulnerabilidad, desarrollando una red de video-vigilancia que permita monitorear y controlar las diferentes áreas de la misma tanto de forma local como remotamente, alcanzando un nivel de seguridad y vigilancia óptimo, lo cual se traducirá en eficiencia en las futuras decisiones a tomarse.

El estudio de la red de video-vigilancia remoto ayuda a monitorear y controlar todas las actividades del recinto con el fin de fortalecer la seguridad del mismo,

conduciendo a la institución a los beneficios que brindan la tecnología GSM Y GPRS.

En la Brigada Selva N°17 se ha considerado realizar un monitoreo mediante dispositivos de seguridad existentes en el mercado, con los cuales se realiza un tratamiento de la información, determinando las acciones necesarias en caso de presentarse una acceso no autorizado al recinto de igual manera se trabajara con un control de accesos para cada zona mediante un código de ingreso.

Con la aplicación de esta propuesta se obtendrá un eficiente monitoreo y control de accesos a las zonas más vulnerables de la Brigada, tomando las correctas decisiones que ayuden al óptimo funcionamiento de la seguridad en el batallón aplicando normas y reglamentos adecuados.

## **6.5 OBJETIVOS**

### **6.5.1 Objetivo General**

Implementar un prototipo de una red de Video-Vigilancia con tecnología GSM-GPRS para el monitoreo y control de accesos a zonas de alta vulnerabilidad en la Brigada Selva N°17.

### **6.5.2 Objetivos Específicos**

- Determinar los equipos adecuados para el monitoreo y control de accesos utilizando tecnología GSM-GPRS para el control de los mismos
- Realizar el análisis de la red de vigilancia y alarmas existente para determinar los puntos más vulnerables y la incidencia en la seguridad del Batallón
- Implementar un prototipo de una red de video-vigilancia para el monitoreo y control de accesos aprovechando los recursos de cada unidad del Batallón.

## **6.6 ANÁLISIS DE FACTIBILIDAD**

### **6.6.1 Factibilidad Técnica**

Es factible ya que los equipos necesarios y la documentación respectiva para la implementación del prototipo de red de video-vigilancia se encuentran disponibles en el mercado, sin duda la variedad de alternativas permite escoger el equipo más apropiado y el mejor que se adapte a las necesidades, además el software es totalmente libre, con lo cual se administra la red y plataformas en caso de accesos remotos.

### **6.6.2 Factibilidad Operativa**

Desde el punto de vista operativo, es posible la implementación ya que el Batallón 17-BS, cuenta con la infraestructura tanto física como tecnológica requerida para la instalación de la red. Además la institución cuenta con el personal necesario para el monitoreo, control de los equipos y dispositivos que serán instalados en la zona.

### **6.6.3 Factibilidad Económica**

Es viable desde el punto de vista económico, ya que el prototipo implementado es de bajo costo en cuanto a equipos y materiales, los cuales están a disponibilidad en el mercado existente brindando una alta gama de beneficios al 17BS.

## **6.7 FUNDAMENTACIÓN CIENTÍFICO – TÉCNICA**

### **6.7.1 Establecimiento geográfico del proyecto**

La Brigada Selva N°17 acantonada en la parroquia Shell de provincia de Pastaza, es uno de los sitios más estratégicos para la actividad militar, petrolera, aérea, comercial de espera y descanso para las personas que ingresan por vía aérea

### **6.7.2 Diseño de Sistema de Video-Vigilancia**

Al diseñar un Sistema de Video -Vigilancia es necesario considerar múltiples factores, los cuales pueden ser controlados a través del diseño, como son los factores externos y sus entornos justificándolos adecuadamente:

- **Redes**

Dado que el sistema se implementará con una red totalmente independiente de las existentes, se realiza de ante mano un adecuado estudio de distancias, posteo, anclajes recubrimientos terminales y cables a utilizarse dado que la información a transmitir es de suma importancia es necesario tener en cuenta posibles puntos de sabotaje de la red sin que estas lleguen a interferir con los sistemas ya existentes.

- **Seguridad de la Red**

El administrador de la red, tendrá un conjunto de políticas asociadas al uso de la red, las mismas incluyen aspectos como credenciales para el Login, procedimientos de back-up, autenticaciones, administración de la unidad de grabado.

- **Entornos Externos**

Las cámaras utilizan protección para las condiciones climatológicas persistentes en el ambiente como polvo y sobre todo temperaturas altas.

El lugar a instalarse debe ser lo más estratégico posible ya que el campo visual de la cámara (fija o con rotación) puede bloquearse en ciertas zonas por vegetación o por factores humanos, considerando que cada cámara debe tener una visión clara y directa del área en todo momento

- Factores Internos

La iluminación es un factor importante; mientras más luz exista mejor será la imagen, generalmente se precisan al menos 200 lux para capturar imágenes de buena calidad caso contrario se utilizara opciones como cámaras con infrarrojos para la noche.

Si la instalación es en un entorno de luz estática (bóvedas) o en un entorno dinámico (exteriores) donde la iluminación varía notablemente, la mejor opción es utilizar cámaras con un lente de ajuste automático del iris en función de la cantidad de luz.

Se debe evitar las áreas con mucho brillo ya que las imágenes se notan sobre expuestas y los objetos muy oscuros. El contraste de colores entre objetos y fondos afecta la calidad de la imagen.

Aspectos como excesiva humedad podrían afectar el lente de la cámara empañándolo, situación que se previene utilizando dispositivos que ayuden a corregir este problema o una climatización correcta del lugar de instalación

### **6.7.3 Visualización del video**

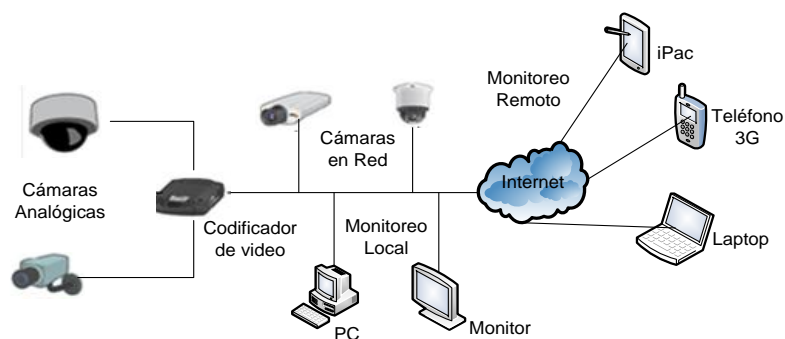
El estudio necesario para el 17-BS tiene dos tipos de visualización del video; uno cuando se precisa monitorear las imágenes en vivo con operarios vigilando activamente las zonas y objetivos, y otro punto de accesos en el cual se podrá gestionar y administrar dicha información por personal autorizado.

#### 6.7.4 Almacenamiento de Información

Las redes de seguridad permiten, que el vídeo se grabe y almacene, con el fin de obtener un backup de la información con la cual los usuarios puedan revisar cualquier incidente, tanto imágenes aisladas como secuencias de vídeo.

#### 6.7.5 Componentes del Sistema de Video-Vigilancia

Los componentes del sistema de Video-Vigilancia se exponen a continuación en el gráfico 6.1:



**Gráfico 6. 1 Componentes de un Sistema de Video en Red**  
**Fuente: Guía Técnica AXISS<sup>7</sup>**

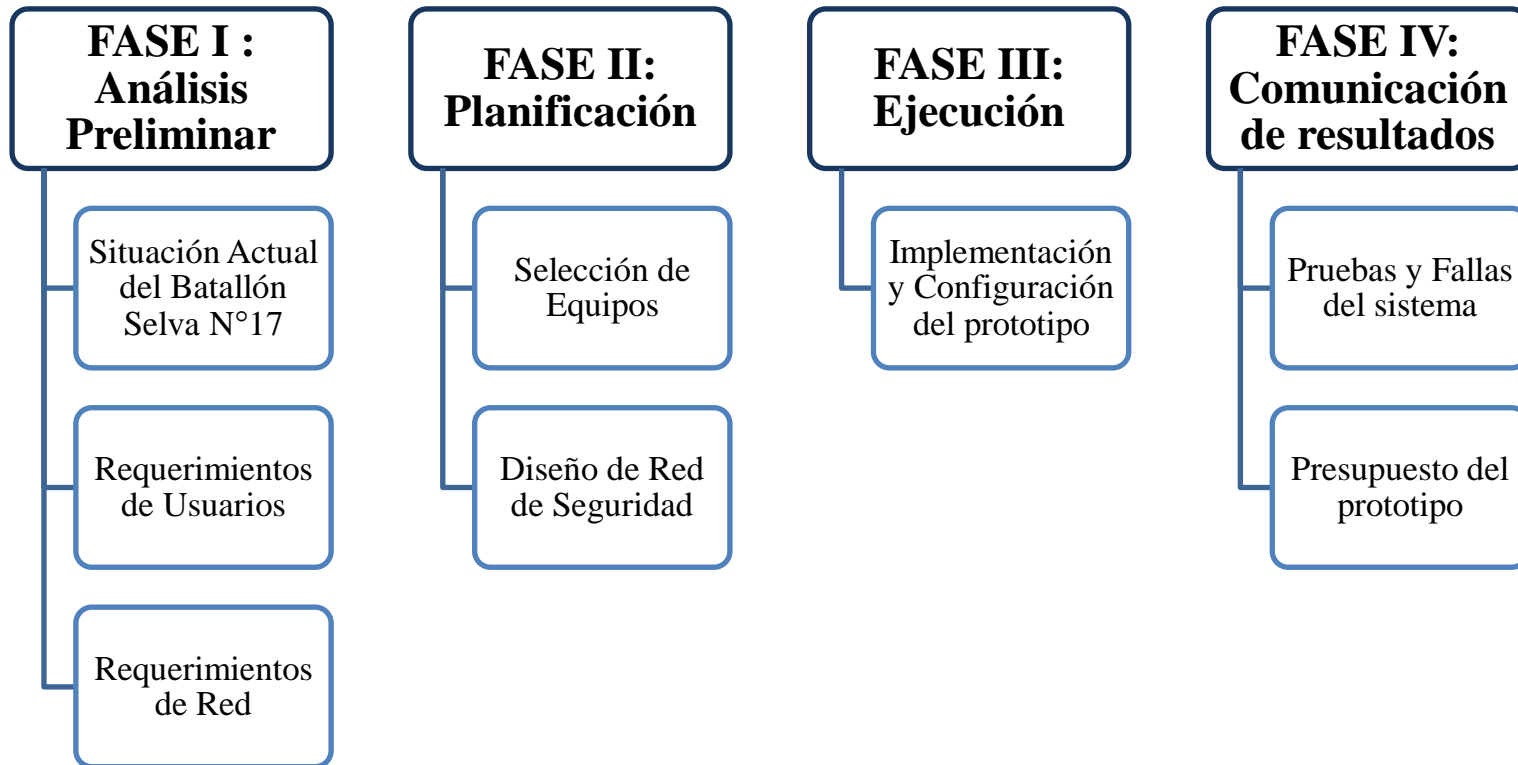
El primer paso es la captura de imágenes en tiempo real, estas transmisiones son enviadas a través de la red a una o varias estaciones para visualizarse en forma individual o simultáneamente.

El contenido es procesado y editado en un servidor de vídeo mediante un software de visualización.

#### 6.8 METODOLOGÍA MODELO OPERATIVO

Después de haber identificado el problema, causas y efectos, se procede a desarrollar la fundamentación detallando las fases descritas a continuación en el gráfico 6.2:

<sup>7</sup> AXIIS Communications, *Guía técnica IP*, Canadá Julio 2005, Cap.1, p.8



**Gráfico 6. 2 Diagrama de Fases**  
**Elaborado por: Franklin Baldospin**



## **FASE I**

### **6.8.1 Análisis Preliminar**

#### **6.8.2 Situación Actual del Batallón Selva N°17**

El viernes 21 de septiembre del año 2012, se realizó una visita técnica a las instalaciones del Batallón Selva N°17 ubicado en la provincia de Pastaza, cantón Shell, en el cual se recopiló la siguiente información:

#### **Reseña Histórica**

En el año de 1936, cuando la Compañía Petrolera Leonard Exploration abandona la zona, y con ello, en 1937, el gobierno entrega en concesión a la compañía Shell más de dos millones de hectáreas para la exploración petrolera en el Oriente, esta instala el campamento principal, donde se construye el campo de aviación que fue inaugurado en 1939, se agilitan los trabajos de la carretera desde Baños, que llega a Shell en 1945

Con el campo de aviación, hoy Aeropuerto Río Amazonas, Shell se convierte en un sitio estratégico para la actividad militar, petrolera, transporte aéreo, misionero y comercial, de espera y descanso para los viajeros que ingresan por vía aérea, con ello, las compañías de aviación

Comienza este sector a ser llamado “Base Pastaza” y luego, “Base Shell-Mera”. En 1949, la compañía petrolera Shell abandona el sector, las instalaciones son inicialmente ocupadas por la FAE, para luego, en 1945, ser entregadas al Ejército Ecuatoriano, que traslada su “Batallón 11 Quito.

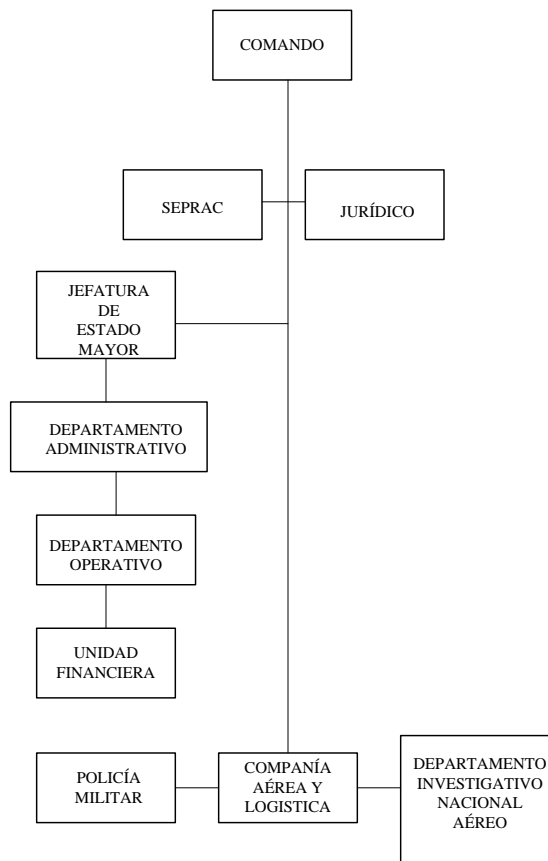
La 17 BS “PASTAZA” se encuentra organizada de la siguiente manera:

- Comando
- Órganos Técnicos Administrativos (Departamento de Seguridad y Prevención de Accidentes – SEPRAC)
- Órganos de Asesoramiento (Departamento Jurídico y Jefatura del Estado Mayor)

- Órganos de Planificación y Asesoramiento (Departamento Administrativo, Operativo y Unidad Financiera)
- Órganos Operativos (Compañía Policía Militar N.17, Compañía de Comunicaciones N.17, Comando de Apoyo Logístico N.17)

### Estructura Orgánica

A continuación se detalla en el gráfico 6.3 el organigrama estructural que mantiene la institución:



**Gráfico 6. 3 Estructura de la Brigada Selva N°17 Pastaza  
Elaborado por: Franklin Baldospin**

### Misión

“Desarrollar el poder terrestre para la consecución de los objetivos institucionales, que garanticen la defensa, contribuyan con la seguridad y desarrollo de la nación, a fin de alcanzar los objetivos derivados de la planificación estratégica militar.”<sup>8</sup>

<sup>8</sup> Ejército del Ecuador, <http://www.ejercitodelecuador.mil.ec/>

## **Visión**

“Institución de más alto nivel de credibilidad; sistemáticamente integrada, con personal profesional, ético y moralmente calificado, con capacidad para enfrentar los nuevos escenarios, que garantice la paz, seguridad y coadyuve al desarrollo de la nación.”<sup>9</sup>

El Batallón SelvaN°17 dispone de una infraestructura física para el monitoreo y administración de las comunicaciones, el gráfico 6.4 evidencia la central en donde se concentra toda la información y registro supervisado por personal militar, autorizado por el mando superior de la brigada.



**Gráfico 6. 4 Central de Comunicaciones**  
**Fuente: Franklin Baldospin**

El ingreso al 17-BS tanto peatonal o vehicular se lo realiza por la entrada principal como lo indica el gráfico 6.5 el cual está controlado por el personal de turno que verifica su identificación y motivo; este método deficiente no cumple las normas de seguridad militar que exigen el alto mando necesarias para prevenir posibles daños o atentados causados por personas dentro y fuera de las instalaciones.

---

<sup>9</sup>Ejercito del Ecuador, <http://www.ejercitodelecuador.mil.ec/>



**Gráfico 6. 5 Ingreso principal**  
**Fuente: El Investigador**

La seguridad con que cuenta la brigada en las bodegas es superficial, cuenta con dispositivos de alarma como cerco eléctrico y personal de vigilancia perimetral evidenciado en el gráfico 6.6 sistemas que no brindan una seguridad real, la falta de integración y automatización no permite el correcto funcionamiento de los filtros de seguridad para cada zona sensible.



**Gráfico 6. 6 Bodegas**  
**Fuente: El Investigador**

Para una mejor comprensión de la situación actual de cada bodega se detallan mediante imágenes en el **Anexo 1** en el cual se identifica la ubicación e infraestructura existente para la implementación en un futuro, del diseño propuesto.

### **6.8.3 Requerimientos de Usuarios**

Mediante la investigación realizada al personal involucrado en la Unidad Comunicaciones del Batallón se recopiló diversos requerimientos para la seguridad de la Bodega N°3 de armamento el cual se detalla a continuación:

- Monitoreo del Acceso Principal (calle)
- Vigilancia Perimetral de la Bodega
- Vigilancia del acceso Bodega CAL y BOES
- Control de Acceso a Bodega CAL y BOES
- Autenticación de personal al ingreso
- Generación de Claves con diferentes atributos
- Registro video gráfico de eventos registrados las 24h
- Generación de reportes en línea
- Acceso a la Red mediante Web
- Monitoreo desde dispositivos móviles

### **6.8.4 Requerimientos de Red**

Los requerimientos de red, los cuales satisfaga las necesidades del batallón son los siguientes:

- Equipo Grabador de Video DVR de 4 canales con control PTZ y salidas auxiliares para sensores externos
- Cámara Domo Blindada para exteriores de 3mm
- Cámara tubular Blindada para interiores de 6mm
- Cámara Pan Tilt Zoom (PTZ) con rotación de 360° y manejo remoto
- Disco duro HDD con capacidad de 1Tbyte para una grabación continua 24h
- Amplificador de Video (balun) color 500m y blanco y negro 600m
- Cable UTP Cat 6 (300m)

- Conectores BNC, RCA y RJ45
- Fuentes de poder Independientes de 12V, 5A
- Unidad de Control PC1832
- Teclado LCD 5511
- Sirena Sonora 20Watss
- Tarjeta de Transmisión T-Link 250

## **FASE II**

### **6.8.3 Planificación**

### **6.8.4 Descripción del diseño**

En la actualidad las Instituciones del estado han tenido cambios respecto a la seguridad tanto interna como externa.

Es por eso que, la tecnología trata de cubrir las necesidades de los clientes, ya que estas cada día son más exigentes y sus demandas van destinadas a:

- Confiabilidad y eficiencia
- Comunicación
- Reducción de costos

Por esta razón se presenta una solución sustentada bajo un estudio que permite una descripción detallada de la propuesta, que se obtiene al aplicar sistemas de video-vigilancia actual y eficiente, analizando equipos y sus ventajas.

### **6.8.5 Análisis y Elección de los dispositivos del sistema a utilizar**

De entre los fabricantes más conocidos en el mercado mundial se seleccionó aquellos con mayores ventajas y un mejor costo, cabe recalcar que en nuestro país existen una gran variedad de empresas que ofertan equipos de diversas ventajas y precios. Los criterios de elección se basan en las características técnicas y uso actual de los elementos.

Las reconocidas marcas como Q-SEE, ZMOD0 y DSC de prestigio mundial, tienen en el mercado equipos con características técnicas similares así como su calidad y compatibilidad, la decisión que se tome vendrá dada por la gama de productos, por la claridad de sus especificaciones técnicas, y ante todo por el uso actual en las diferentes instalaciones que se tiene para los sistemas de vigilancia y control de accesos que existen hoy en día, a continuación se detalla varios cuadros comparativos con las diferentes prestaciones según el equipo:

CÁMARAS								
Caract. Marca	Imágenes de alta calidad	Visión Nocturna	Rango de Visión	Angulo de Visión	Audio	TVL	PTZ	Precio
<b>Q-see</b>	alta	alta	33m	alta	si	540	si	alto
<b>Zmodo</b>	baja	baja	30m	media	no	420/480	si	bajo
<b>TopBand</b>	media	media	30m	media	si	420/480	si	medio

**Tabla 6. 1 Cuadro Comparativo Cámaras**  
Elaborado por: Franklin Baldospin

EQUIPO GRABADOR DIGITAL								
Caract. Marca	Modo de Operación	H.264	Backup	Clave	PTZ y Control	Zoom digital	Alertas Email	Precio
<b>TopBand</b>	si	si	si	si	si	si	si	medio
<b>Zmodo</b>	si	si	si	si	si	no	no	bajo
<b>Avitech</b>	si	si	si	si	si	si	si	alto

**Tabla 6. 2 Cuadro Comparativo Equipo Grabador**  
Elaborado por: Franklin Baldospin

ALARMAS							
Caract. Marca	Zonas	Partición	Teclado	PGM	Capacidad de eventos	Tarjeta expansora	Precio
DSC	32	4	8	2	500	si	medio
Paradox	32	2	2	NO	300	no	medio

**Tabla 6. 3 Cuadro Comparativo Alarmas  
Elaborado por. Franklin Baldospin**

Las marcas TopBand y Zmodo además de DSC han hecho un gran avance al implementar las más modernas tecnologías en diferentes tipos de dispositivos electrónicos para la recepción, transmisión y grabación de videos además del control remoto, es así que en estos últimos años ha existido un aumento de la presencia de estos productos en el mercado nacional, es por ello que en su mayoría se usó los productos TopBand y DSC beneficiándose por sus ventajas y precio que ofertan.

Existen otros fabricantes reconocidos en el tema de video vigilancia como Zmodo, Avitech, Mooms, Paradox etc., la utilización de estas marcas depende de las necesidades que se presentan en el diseño más adelante.

### **6.8.6 Descripción de los dispositivos del Sistema**

A continuación se procede con los detalles técnicos de los dispositivos más aptos para el sistema de video vigilancia, cabe recalcar que las especificaciones técnicas se encuentran detalladas en los **Anexos**

#### **6.8.6.1 Grabador de Video Digital (DVR) TopBand TBO-9716E**

DVR de vigilancia marca TopBand expuesto en el gráfico 6.7 incorpora una variedad de opciones para su fácil manejo, disponible entre 8 y 16 canales compatible con cámaras de cualquier otro fabricante, todas con diferentes



resoluciones de grabación, comprensión de video en H.264 y tamaño del disco duro adaptable hasta 2TeraBytes, las características operacionales incluyen el monitoreo remoto a través de Internet o teléfono móvil, alertas de correo electrónico, varios ajustes de grabación, y se puede utilizar con un monitor de computadora o un televisor para el monitoreo en vivo de las imágenes.

Además la compatibilidad entre las tecnologías como son symbian, android, iphone, blackberry y Windows mobile permite una mayor integración de los dispositivos móviles y una mayor versatilidad al momento de adaptarse al medio disponible del cliente.

Una característica especial del equipo grabador es la opción de integrar dispositivos de control de accesos interactuando al mismo tiempo con las cámaras, ventaja que nos permite manipular los dos equipos con un monitoreo constante y en tiempo real; obteniendo así un sistema eficiente y totalmente funcional, mayores especificaciones en el **Anexo 2**



**Gráfico 6. 7 DVR TopBand**  
**Fuente: TopBand, Products<sup>10</sup>**

#### **6.8.6.2 Cámara Fija Q-see 3,6mm**

Cámaras de vigilancia modelo QD5401B Q-see publicada en el gráfico 6.8 obtiene imágenes de alta calidad, visión nocturna de gran alcance y fácil conectividad, es resistente a la intemperie, blindada de estilo bala, con 3-ejes de montaje para una colocación en una pared, techo, o en otra superficie plana.

En su interior consta de 48 LEDs infrarrojos, para un rango de visión en la noche de 100 pies, lentes fijos 3,6 mm una apertura de visión de 50 ° a 60 °, y 540

---

<sup>10</sup> **TopBand Products**, [http://www.topband.com/products/product\\_description.php](http://www.topband.com/products/product_description.php)

líneas de resolución, también equipados con una fuente de alimentación y cable de 60 pies BNC, como se especifica mejor en el **Anexo 3**



**Gráfico 6. 8 Cámara Q-see 3,6 mm**  
Fuente: Q-See Products <sup>11</sup>

#### **6.8.6.3 Cámara Topband 3,6 mm**

La marca TopBand de origen japonesa (gráfico 6.9), brinda cámaras con sensores de tecnología SONY/SHARP CCD a color, 36 leds para grabaciones nocturnas a un rango de 30m, su lente tiene una apertura de entre 3,6mm a 6 mm y 420/480TVL, especificado en el **Anexo 4**



**Gráfico 6. 9 Cámara TopBand 3,6mm**  
Fuente: TopBand Products <sup>12</sup>

#### **6.8.6.4 Cámara Domo TopBand TBO-506IR**

La característica fundamental para la utilización de este tipo de cámaras es su resistencia a los movimientos además de su resistente blindaje anti vandalismos detallados en el gráfico 6.10, mayores especificaciones en el **Anexo5**

---

<sup>11</sup> **Q-See Products**, [http://www.q-see.com/products/product\\_description.php](http://www.q-see.com/products/product_description.php)

<sup>12</sup> **TopBand Products**, [http://www.topbandcctv.com/en/chi/products\\_info.aspx](http://www.topbandcctv.com/en/chi/products_info.aspx)



**Gráfico 6. 10 Cámara Domo TopBand**  
**Fuente: TopBand Products**<sup>13</sup>

#### **6.8.6.5 Cámara PTZ Zmodo CM-Z2213GY**

Zmodo brinda una solución en cámaras Pan Tilt Zoom (PTZ) gráfico 6.11 con una función de menú personalizado que permite un fácil control sobre las funciones, cuenta con seguimiento de objetivos, mayor velocidad, zoom óptico de 22x y zoom digital de 10X y sensores de la marca "Sony Super HAD CCD.

El Enfoque longitudinal y la velocidad de rotación se ajusta automáticamente de acuerdo a un punto de inicio programado, de igual manera cuenta con registro de seguimiento de ruta controlado por los controles manuales.

El ángulo de cobertura tanto en el día como en la noche es de 360° en horizontal y 180° en vertical con movimiento continuo, auto flip 180° de rotación e inclinación, su fuente de alimentación es de 120AC diferente a una cámara análoga.



**Gráfico 6. 11 Cámara PTZ blindada**  
**Fuente: Zmodo Products**<sup>14</sup>

<sup>13</sup> **TopBand Products**, [http://www.topbandcctv.com/en/chi/products\\_info.aspx](http://www.topbandcctv.com/en/chi/products_info.aspx)

<sup>14</sup> **Zmodo Products**, <http://www.zmododirect.com/>

#### 6.8.6.6 Alarma Canadiense DSC 1832

Alarma sonora, cuenta con 8 zonas en el panel y expandibles 32 cableadas, 32 inalámbricas, las salidas PGM son 2, expandibles a 14 con tarjetas PC5204, o PC 5208, capacidad de memoria de 500 eventos y conecta hasta 8 teclados supervisados, admite una zona por teclado, incluye una batería de respaldo ante cualquier violación de la alimentación o falla eléctrica revelada en el gráfico 6.12,



**Gráfico 6. 12 Kit Alarma DSC**  
**Fuente: DSC Products**<sup>15</sup>

#### 6.8.6.7 Transmisor de alarma por IP universal TL250

Tarjeta compatible con la mayoría de los paneles de control DCS que se comunican utilizando el formato Contact ID, la transmisión es por IP instantánea y siempre activada sobre redes LAN/WAN local o Internet, utilizando poco ancho de banda

Esta tarjeta nos informa de eventos ocurridos a 2 direcciones IP receptoras diferentes en un software T-Link Console o DLS 2012 actualizable por red; compatible con receptores de estación de monitoreo Sur-Gard System I/II/III visualizado en el gráfico 6.13:

---

<sup>15</sup> **DSC Products**, <http://www.dsc.com/index.php>



**Gráfico 6. 13 T-Link 250 DSC**  
**Fuente: DSC Products**<sup>16</sup>

#### **6.8.6.8 Detector infrarrojo pasivo LC-100-PI**

Productos DCS brinda un dispositivo en cuanto a sensores de movimiento con características de un análisis inteligente de señales digitales para asegurar una detección confiable, además de contar con un mecanismo anti-mascota de hasta 25 kg (55 libras)

Cuenta con un contacto de alarma e interruptor de seguridad con tecnología Quad de imagen lineal la cual brinda un análisis preciso de las dimensiones corporales, diferenciación de fondos y animales domésticos, además no requiere de calibración de altura para la instalación como lo muestra el gráfico 6.14:



**Gráfico 6. 14 Sensor de Movimiento**  
**Fuente: DSC Products**

---

<sup>16</sup> **DSC Products**, <http://www.dsc.com/index.php>

### 6.8.6.9 Teclado DSC LCD 5511

Teclado Power configurable como entrada de zona o seguimiento de una de las salidas PGM de la central, dispone de indicador acústico de activación de zona programable, con 4 tonos distintos supervisado, 4 teclas funcionales de acción directa programables (15 opciones), soporta 8 particiones, led indicador de Listo, Armado, teclas dobles para la activación de Alarma, Pánico y Fuego, teclado retro iluminado, consumo 100 mA máx como lo indica el gráfico 6.15 a continuación:



**Gráfico 6. 15 Teclado LCD 5511**  
**Fuente: DSC Products <sup>17</sup>**

### 6.8.7 Diseño del prototipo

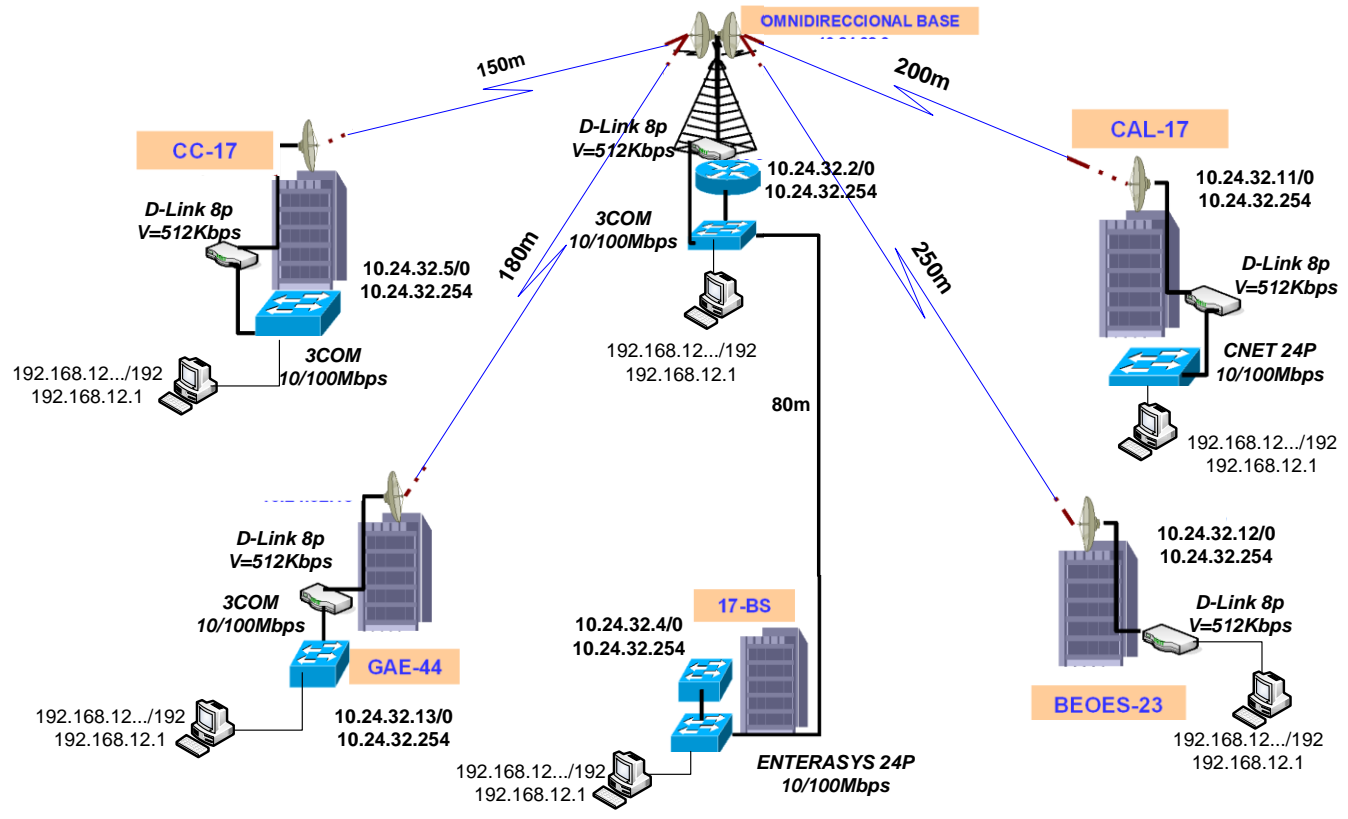
Antes de elaborar el diseño de la red se debe tomar en cuenta la red actual de conectividad existente en el Batallón con sus equipos como direcciones IP correspondientes, detallando la infraestructura física y los equipos o dispositivos existentes como lo muestra el gráfico:

A continuación se procede con el diseño de red a implementarse en el cual se detalla la ubicación de las diferentes bodegas, modo de transmisión de los datos, dispositivos de seguridad, los cuales son necesarios para el monitoreo y control en una red de video-vigilancia; como lo expone en el siguiente Gráfico 6.16:

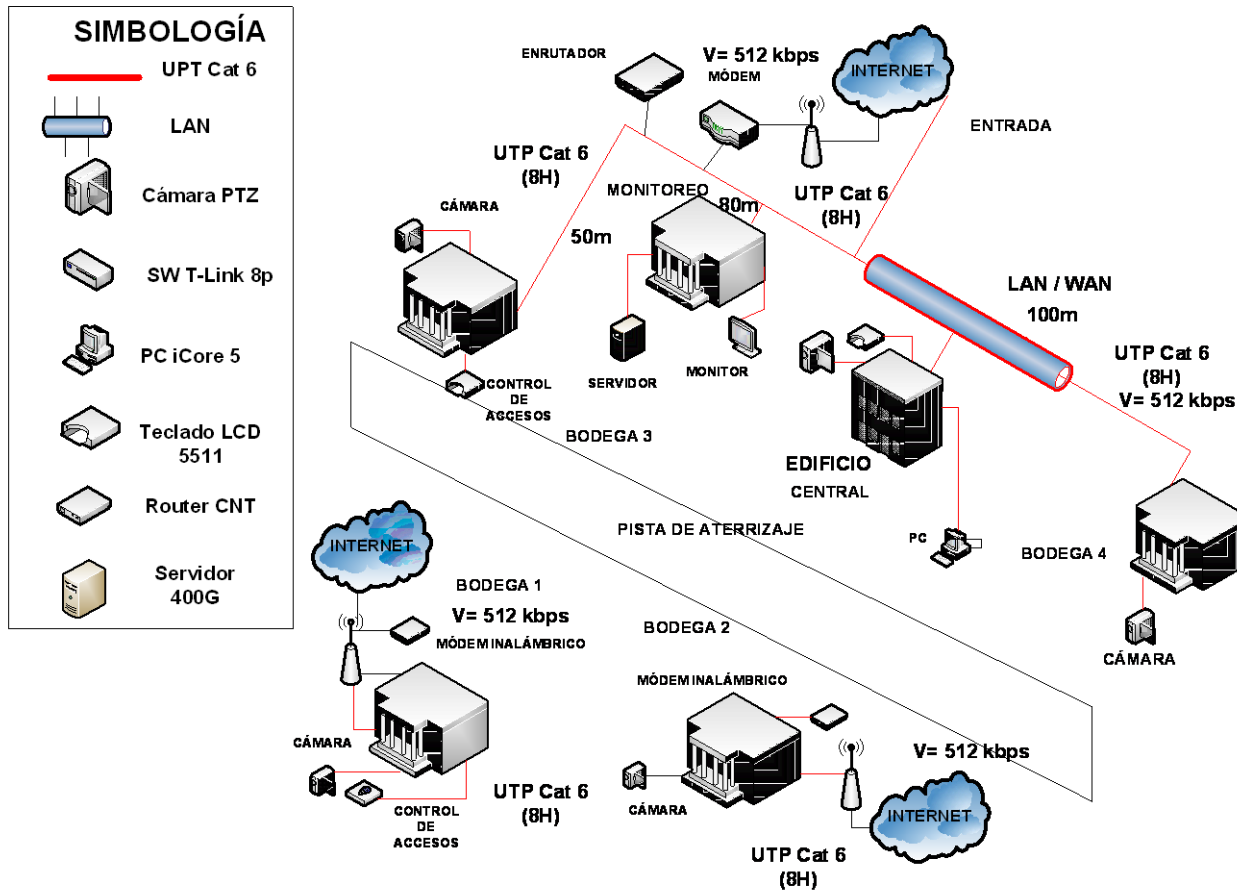
---

<sup>17</sup> **DSC Products**, <http://www.dsc.com/index.php>

## CONECTIVAD FUERTE MILITAR "AMAZONAS"



**Gráfico 6. 16 Red de Datos Actual**  
**Elaborado por: Franklin Baldospin**



**Gráfico 6. 17 Diseño de Red de Video-Vigilancia**  
**Elaborado por: Franklin Baldospin**



En el diseño se contempla una red cableada en cada bodega a la cual se conecta los dispositivos de seguridad (cámaras, alarmas, sensores) y equipos (DVR, PC1832, Modem) tanto para el video como control los cuales se transmitirán la información hacia un modem de internet inalámbrico proporcionado por CNT; la unidad de comunicaciones donde se encuentra la central de monitoreo tendrá acceso a la información mediante la web.

El diseño contempla cámaras perimetrales, blindadas tanto para prevenir ataques deliberados como la inclemencia del ambiente; contamos en cada bodega con un teclado para el control de accesos del cual se obtiene la información de los eventos registrados en cada alarma, esta se envía a través de la red o web hacia la central para su visualizarla y monitorearla.

La implementación del prototipo de un sistema para el batallón N°17 debe considerar diferentes factores que se encargan de brindar una calidad de la imagen excelente y definida los cuales son:

#### **6.8.7.1 Campo de visión**

El campo de visión viene determinado por la longitud focal del objetivo y el tamaño del sensor de imagen, cuando mayor es la longitud focal, más estrecho es el campo de visión.

La longitud focal se define como la distancia entre el objetivo de entrada y el punto en el que convergen todos los rayos de luz hacia un punto. El campo de visión se clasificar en tres tipos:

- **Vista normal:** Ofrece un campo de visión igual que el ojo humano
- **Telefoto:** Campo de visión más estrecho, detalles más precisos; utilizado cuando el objeto es pequeño

- **Gran Angular:** Campo de visión amplio y con menos detalles, ofrece una buena profundidad de campo y buen rendimiento en condiciones de poca luz

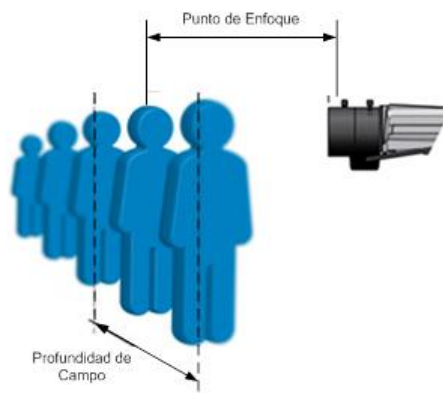
En el Gráfico 6.18 muestra la diferencia en cada tipo de campo de visión:



**Gráfico 6. 18 Gran Angular, Vista Normal, Telefoto**  
**Fuente: <http://blogdeseguridad.com/><sup>18</sup>**

#### 6.8.7.2 Profundidad de Campo

La profundidad de campo hace referencia a la distancia delante y más allá del punto de enfoque donde los objetos parecen ser nítidos de forma simultánea esta puede verse afectada por tres factores la longitud focal, el diámetro del iris y la distancia de la cámara al sujeto. Una longitud focal alargada, necesita una amplia apertura de iris o una distancia corta entre la cámara y el sujeto que limitará la profundidad de campo demostrada mediante el gráfico 6.19.

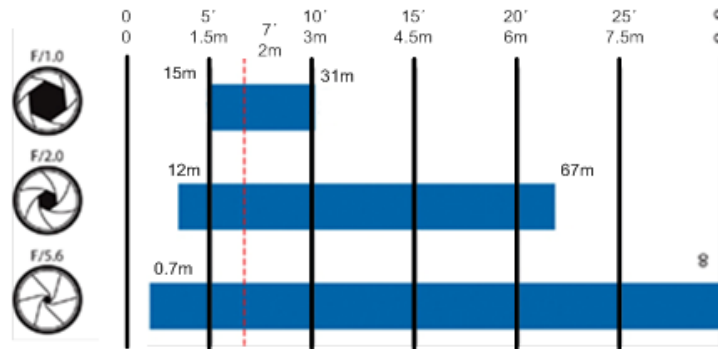


**Gráfico 6. 19 Profundidad de Campo**  
**Fuente: Guía Técnica AXISS<sup>19</sup>**

<sup>18</sup> **Sistemas de Seguridad**, <http://blogdeseguridad.com>

<sup>19</sup> **Guía Técnica AXISS**, AXISS Communications, Canadá Julio (2005) Cap. 3 p.33

Cuando el enfoque se sitúa en la mitad de cierto objeto a vigilar y es posible identificar claramente hasta 15 m (45 pies) hacia adelante y hacia atrás entonces existe una buena profundidad de campo como lo revela los datos del gráfico 6.20.



**Gráfico 6. 20 Apertura del Iris**  
Fuente: Guía Técnica AXISS <sup>20</sup>

### 6.8.7.3 Sensibilidad Lumínica

La sensibilidad lumínica se especifica en términos de lux, normalmente es necesario un mínimo de 200 lux para iluminar un objeto de manera que se pueda obtener una imagen de buena calidad, cuanto más luz reciba el sujeto, mejor será la imagen, con poca luz la imagen resulta granulada y oscura.

Los valores lumínicos difieren de acuerdo a las condiciones de iluminación existentes en el ambiente que se detallan en la siguiente Tabla 6.4:

ILUMINANCIA	CONDICIÓN DE ILUMINACIÓN
100,000 lux	Luz solar intensa
10,000 lux	Luz plena del día
500 lux	Luz de oficina
100 lux	Habitación con poca luz

**Tabla 6. 4 Valores Lumínicos**

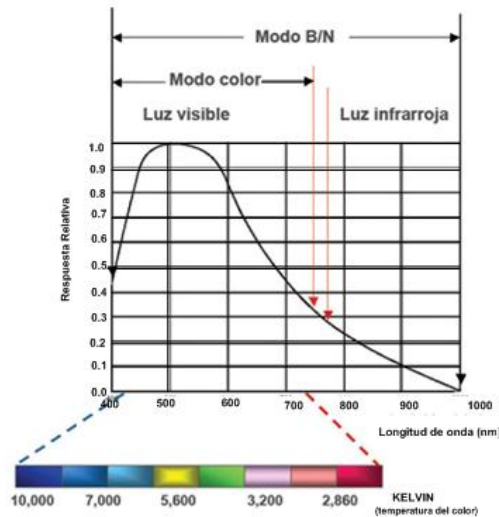
**Elaborado por: Franklin Baldospin**

<sup>20</sup> Guía Técnica AXISS, AXISS Communications, Canadá Julio (2005)Cap.3 p.33

#### 6.8.7.4 Cálculo de la iluminación

Como se explica anteriormente la sensibilidad lumínica de una cámara se especifica en lux que corresponde a un nivel de iluminación en el cual una cámara produce una imagen aceptable, según los fabricantes Q-see y Zmodo el rango mínimo es de 200lux que ilumine al objeto obteniendo una imagen de buena calidad, considerando el nivel de iluminación a luz solar intensa es de 100,000 lux y la de un día despejado es de 10.000lux valores que se aproximan a los reales del ambiente.

En casos de poca iluminación se utiliza luz IR o infrarrojos la cual se encuentra en el rango de 700 nanómetros (nm) hasta cerca de 1.000 nm, por debajo de la visión humana, cuando la cámara está en modo nocturno, el filtro IR permite que la sensibilidad lumínica de la cámara alcance los 0,001 lux o un nivel inferior como se muestra en el siguiente gráfico 6.21:



**Gráfico 6. 21 Iluminación IR**  
**Fuente: Guía técnica AXISS<sup>21</sup>**

#### 6.8.7.5 Cálculo de distancia focal

Para objetos cercanos es necesaria una apertura de óptica pequeña y para definir mejor la imagen en distancias largas es necesaria una apertura mayor, como referencia esta la siguiente Tabla 6.5:

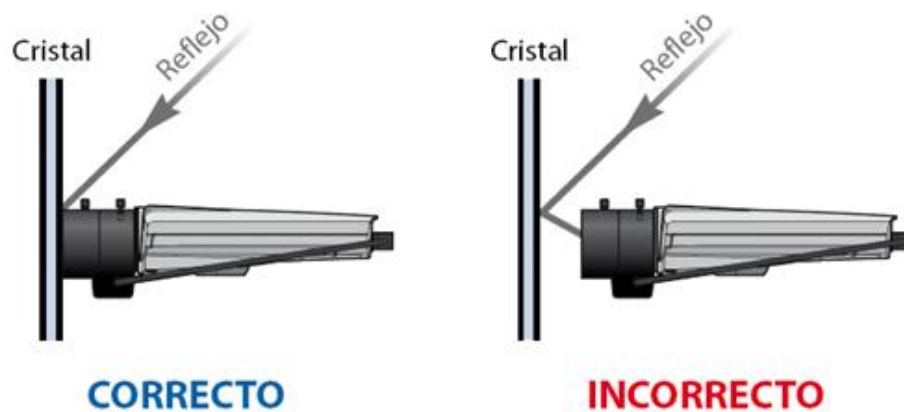
<sup>21</sup> **Guía Técnica AXISS**, *AXISS Communications*, Canadá Julio (2005), Cap.2 p.22

Distancia (m)	Apertura (mm)
2	2,8
6	5
12	8
25	50

**Tabla 6. 5 Distancia Focal**  
**Elaborado por: Franklin Baldospin**

### 6.8.7.6 Eliminación de reflejos

Al instalar una cámara fija en una protección, es importante que el lente se coloque directamente contra el vidrio para evitar deslumbramiento, en caso contrario, los reflejos de la cámara y el fondo aparecerán en la imagen; para reducirlos se aplican recubrimientos especiales en el cristal, como se muestra en el siguiente gráfico 6.22:



**Gráfico 6. 22 Reflejos**  
**Elaborado por: Franklin Baldospin**

Los reflejos también se producen al instalar una cámara frente a una radiación de luz natural como son ventanas o puertas además materiales de superficie lisa como baldosas o mármol, crean un reflejo el cual se corrige manipulando las opciones de color en la cámara expuesta.

### 6.8.7.7 Ubicación de las Cámaras

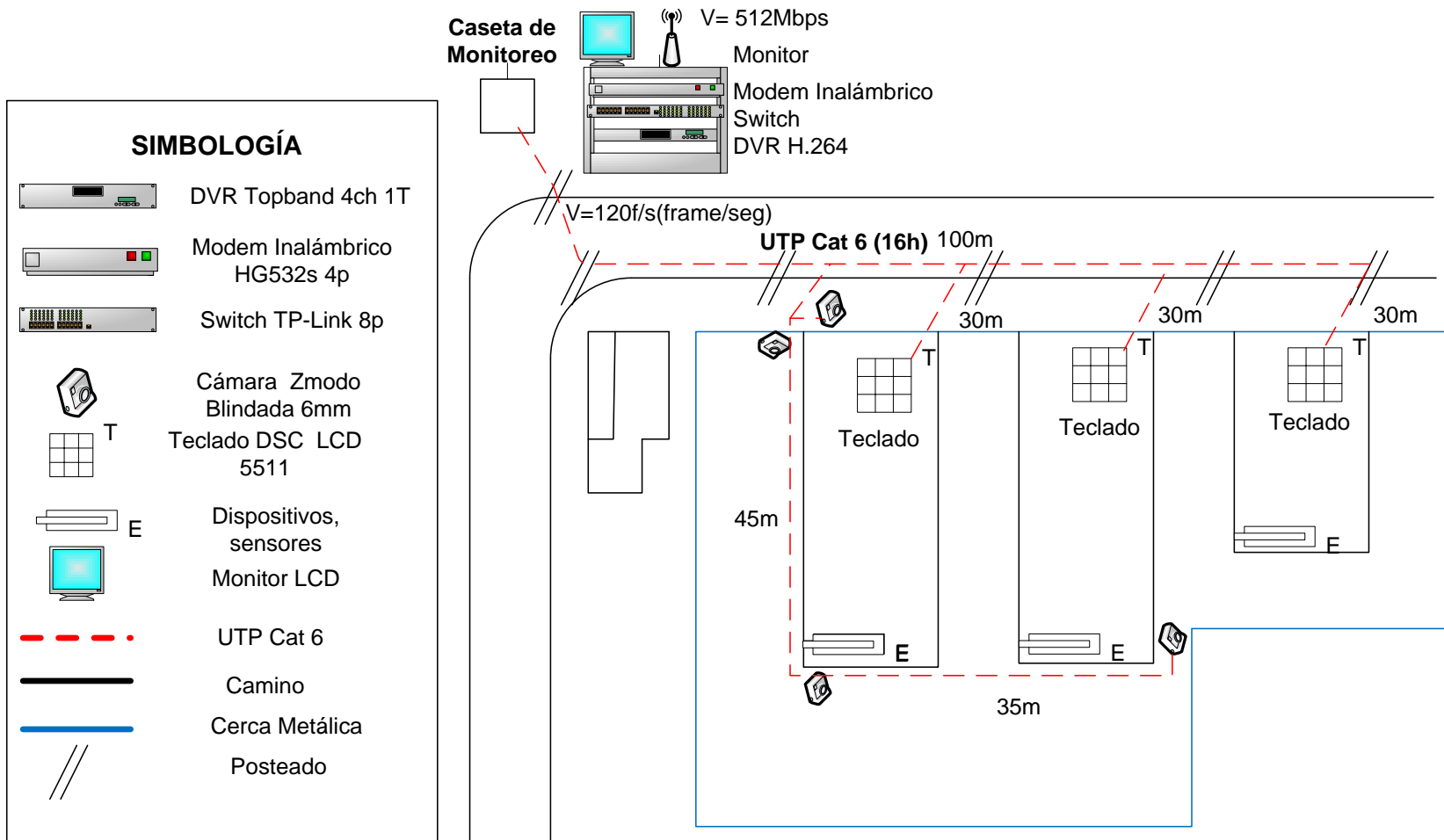
Definir la ubicación más adecuada de las cámaras es un aspecto muy importante en el diseño del sistema de video-vigilancia. Al ser las bodegas de gran altura y dimensiones, la ubicación es crucial para lograr una cobertura adecuada en las diferentes áreas del edificio.

A continuación se detalla las recomendaciones para lograr un resultado óptimo en función del posicionamiento de las cámaras.

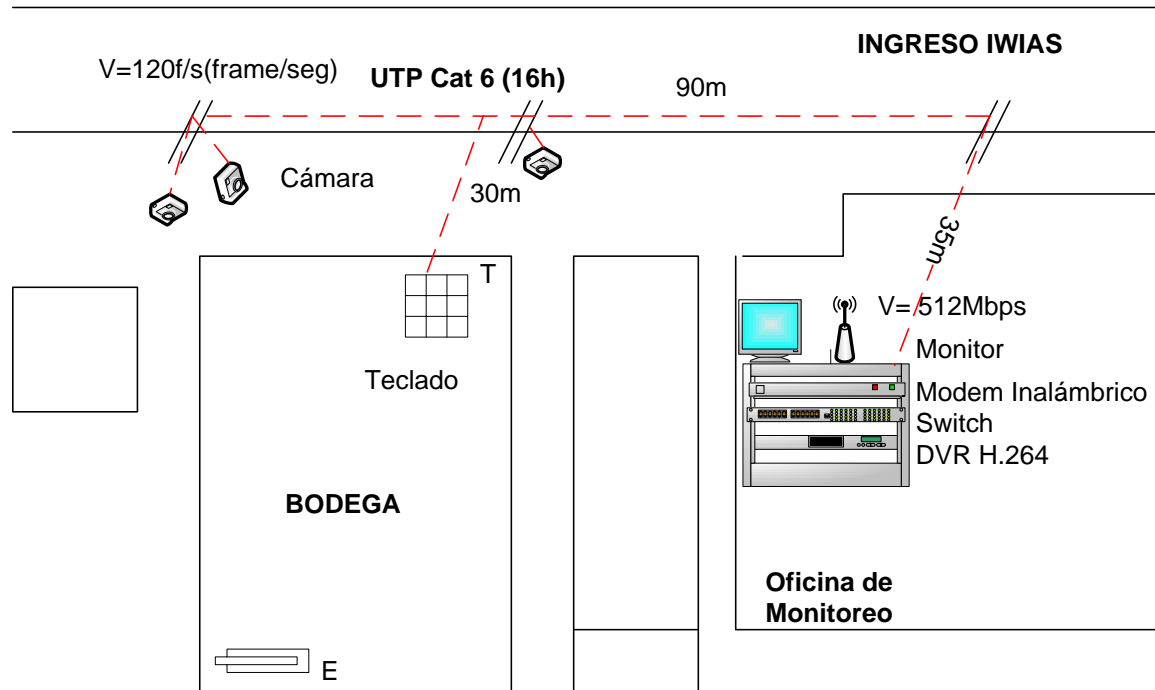
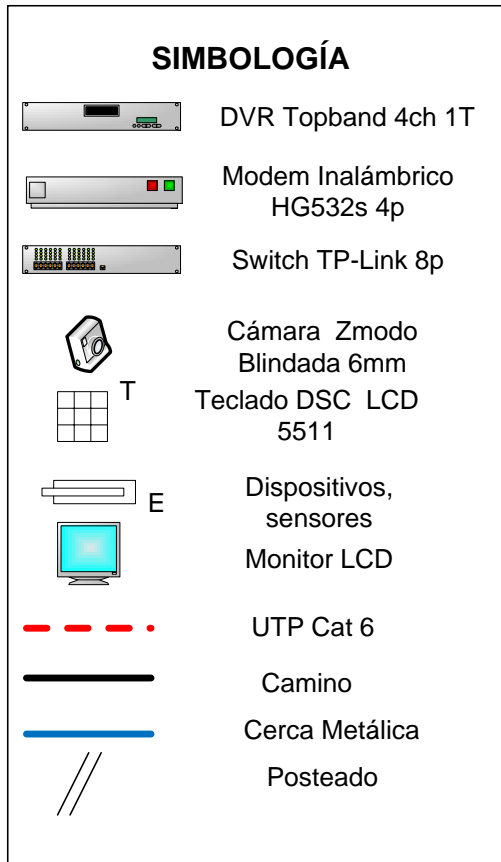
- Evitar el deslumbramiento directo desde la luminaria y reflejado en el piso o vidrio, este efecto puede producir una imagen saturada y no definida.
- Colocar las cámaras a una altura adecuada ya que si la colocamos a una altura excesiva la imagen se verá afectada a un solo punto y no cubrirá la zona necesaria.
- Utilizar Baluns adecuados CTV los cuales amplifican la señal y no permiten interferencia alguna.

Con las recomendaciones anteriores, en los gráficos 23, 24, 25, 26, se representa la ubicación en cada bodega y distribución de las cámaras, además los paneles para el control de accesos a fin de cubrir todos los sectores de las instalaciones.

Mediante la herramienta Auto CAD esquematizamos nuestra red en los planos actuales de la Brigada Selva N°17 incluyendo los dispositivos de seguridad y cableado, con su respectiva rotulación.

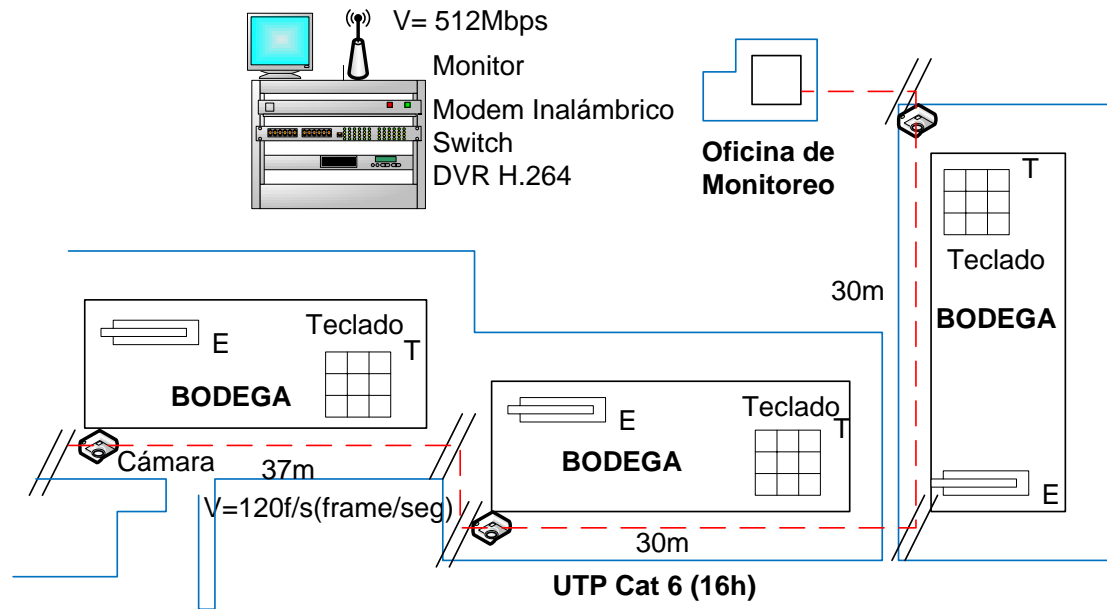
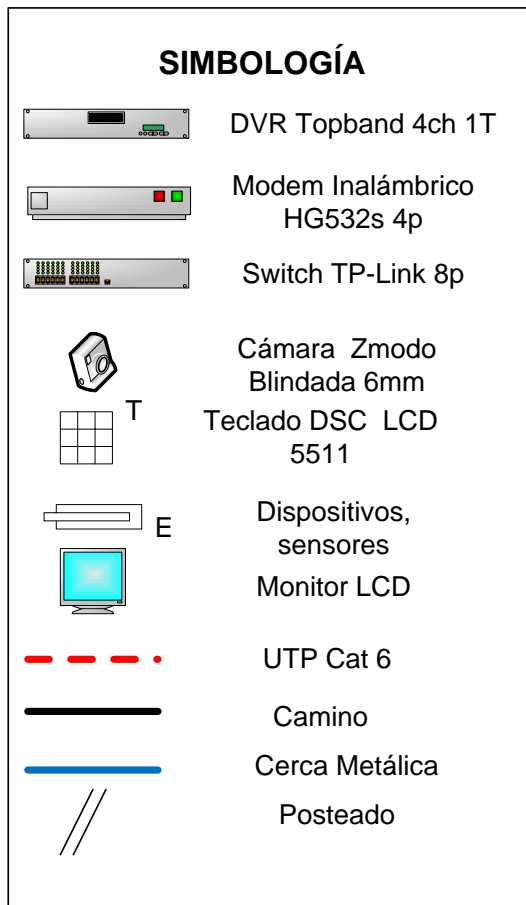


**Gráfico 6. 23 Bodega 1 Rio Pastaza**  
 Elaborado por: Franklin Baldospin

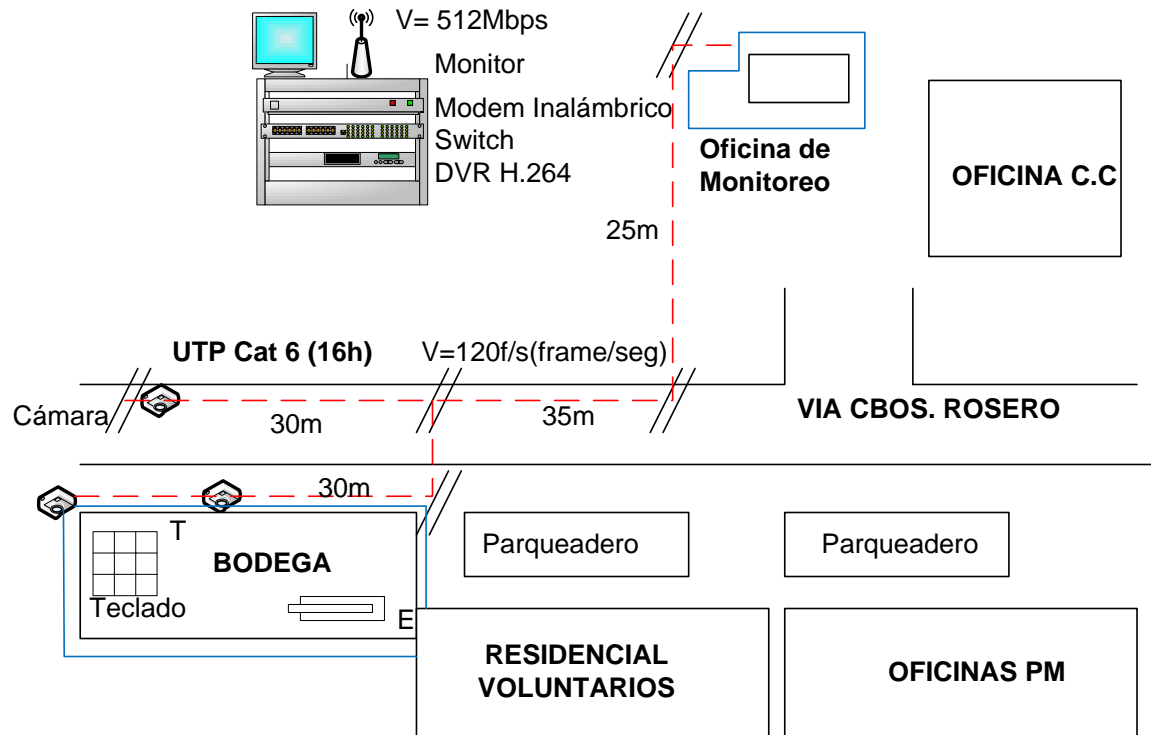
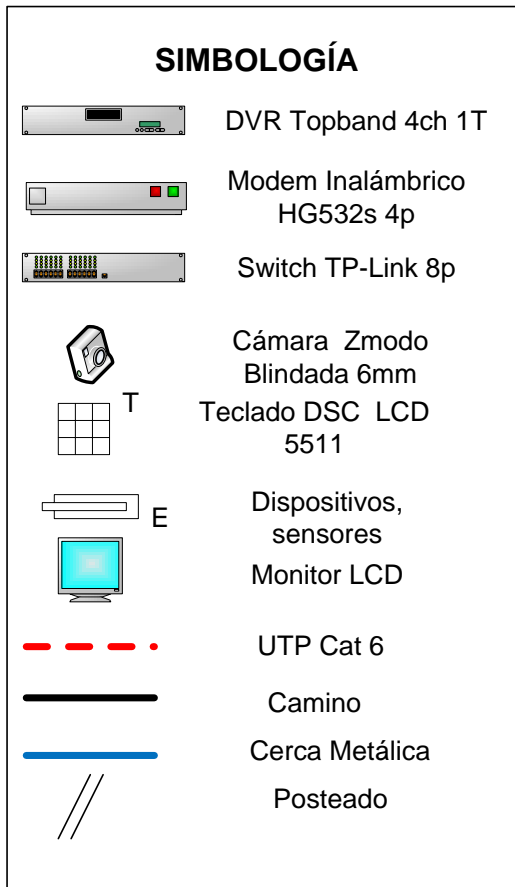


**Gráfico 6. 24 Bodega 2 Sector BOES**  
**Elaborado por: Franklin Baldospin**





**Gráfico 6. 25 Bodega 3 Bodegas Implementos**  
**Elaborado por: Franklin Baldospin**

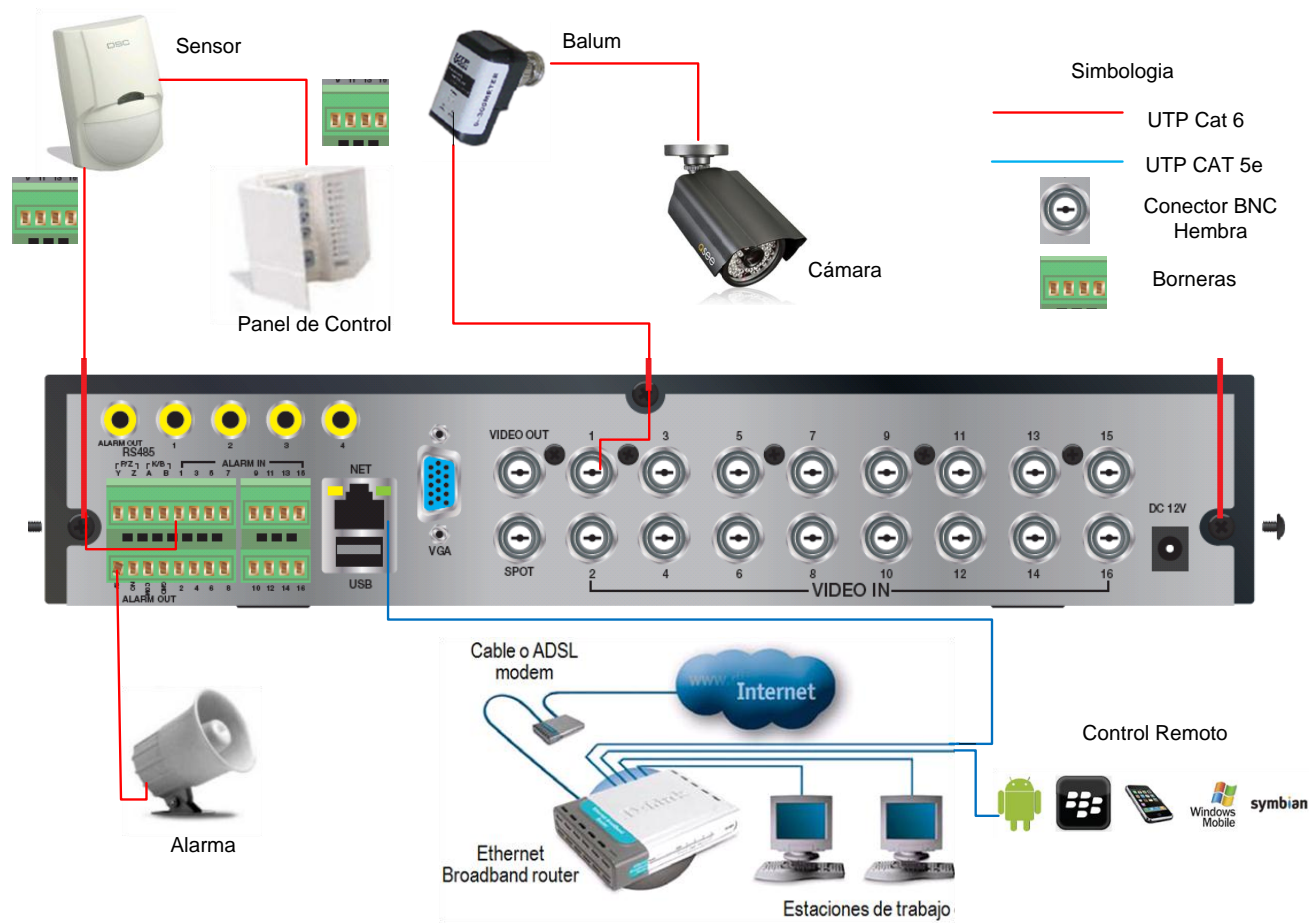


**Gráfico 6. 26Bodega 4 Sector CAL**  
**Elaborado por: Franklin Baldospin**

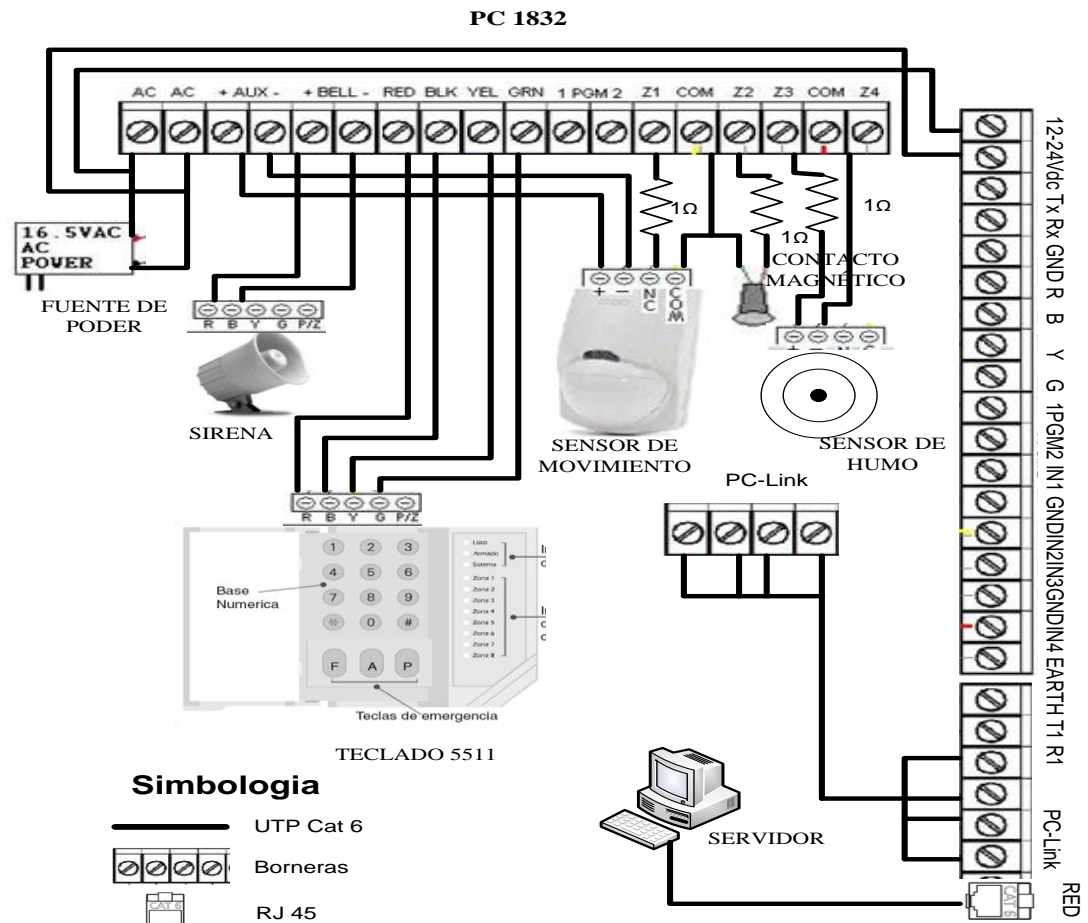
En el gráfico 6.27 se detalla la conexión de un grabador de video digital hacia las cámaras con cable UTP Cat 6, el conector BNC macho se encuentra hacia la cámara y el conector hembra hacia el DVR, en cada extremo cuenta con un balun, dispositivo amplificador de señal el cual soporta distancias de 600m en blanco y negro y 500m a color, cada equipo es conectado a la red mediante una conexión RJ45 todo controlado mediante programación y configuración NetView; se integra adicionalmente la alarma DCS1832 con sensores de movimiento y teclado para un control de accesos en cada puerta

Para el sistema de control de accesos se trabaja con los siguientes equipos; alarma DSC 1832, teclado DSC LCD 5511, tarjeta de red T-Link TL 250 para internet y demás accesorios necesarios para el funcionamiento. Se realiza un esquema de la conexión básica de la unidad central hacia los diferentes sensores

En el Gráfico 6.28 muestra una guía al conectar la unidad de control DSC1832 hacia cualquier dispositivo sea sensor (movimiento, humo, fuego, temperatura, humedad), contacto magnético (puerta, ventana), teclado (numérico, alfanumérico) y sirena en el cual se detalla cuantos hilos se utiliza y su conexión mediante código de colores hacia las borneras; la unidad de control se conecta a la tarjeta T-Link 250 que se encarga de transmitir todos los eventos relacionados a la alarma mediante un bus de datos a la salida PC-Link, gestionada mediante el programa DLS 2012 instalado en el servidor de la central de monitoreo.



**Gráfico 6. 27 Esquema de Conexión de Equipo Grabador DVR**  
**Elaborado por: Franklin Baldospin**



**Gráfico 6. 28 Esquema de Conexión PC 1832**  
**Elaborado por: Franklin Baldospin**

### FASE III

#### 6.8.8 Ejecución

#### 6.8.9 Configuración

##### Configuración del Equipo Grabador

La configuración del grabador tiene una interfaz amigable ante el usuario por lo tanto se ofrece una guía rápida de los aspectos básicos enfocándose en submenús de importancia para el correcto funcionamiento del prototipo:

1.- En primer lugar las funciones básicas tales como idioma, fecha/hora, contraseña, exhibición, video/audio se modifican ingresando al menú principal en la pestaña **BASICO** como lo muestra en el gráfico 6.29 siguiente:

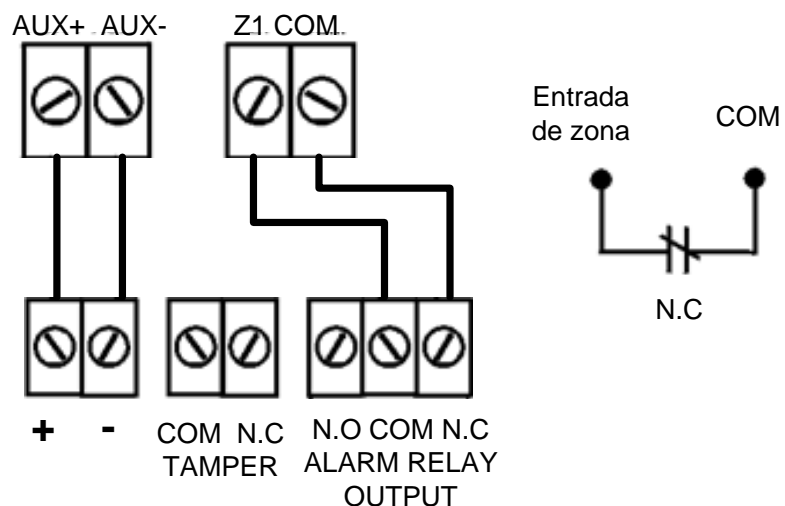


**Gráfico 6. 29 Menú Principal**  
**Fuente: DVR TopBand TBO-9716E**

2.- La pestaña **ALARMAS** permite configurar la activación de cualquier canal al detectar algún movimiento, mediante el tipo de sensor con el cual va a interactuar sea este normalmente cerrado (NC) o normalmente abierto (NO), de acuerdo a estas consideraciones se utiliza cargas resistivas al fin de línea (RFL) conectadas en la central PC1832 de este modo se integra los sensores con la grabación del video activándose tanto en la central de alarma como en el equipo grabador a continuación se detalla la manera correcta de conectar los distintos tipos de detectores para su correcto funcionamiento así:

- **Contactos N.C., Sin Resistencia RFL**

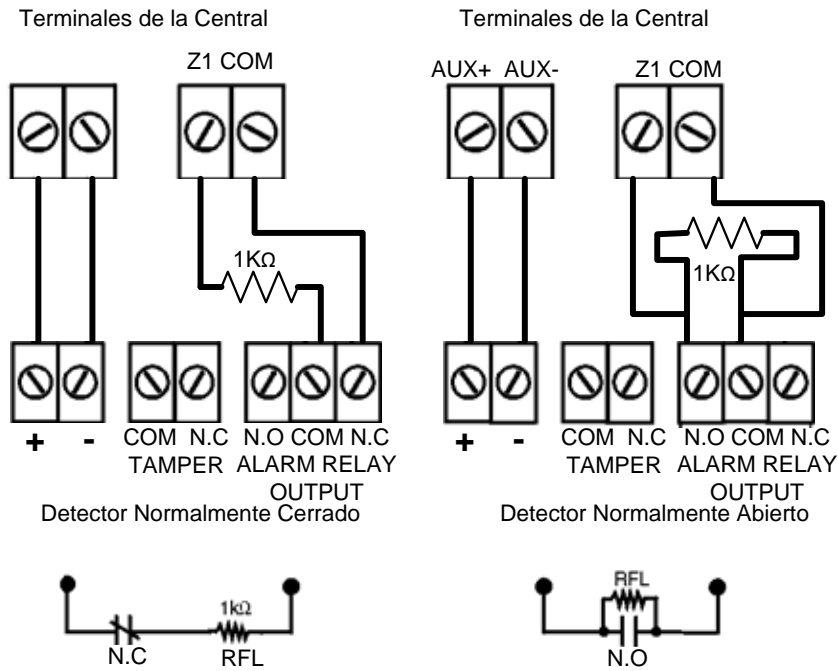
Si la instalación de seguridad no requiere detección antisabotaje o de fallo de cableado, se conecta los detectores como muestra el gráfico 6.30. Esta configuración comunicará una zona abierta o cerrada a la central y mostrará las zonas abiertas en el teclado, no se debe usar dispositivos con contactos normalmente abiertos (N.O.) en esta configuración ya que esto causaría que la central permanezca en alarma.



**Gráfico 6. 30 NC sin RFL**  
**Elaborado por: Franklin Baldospin**

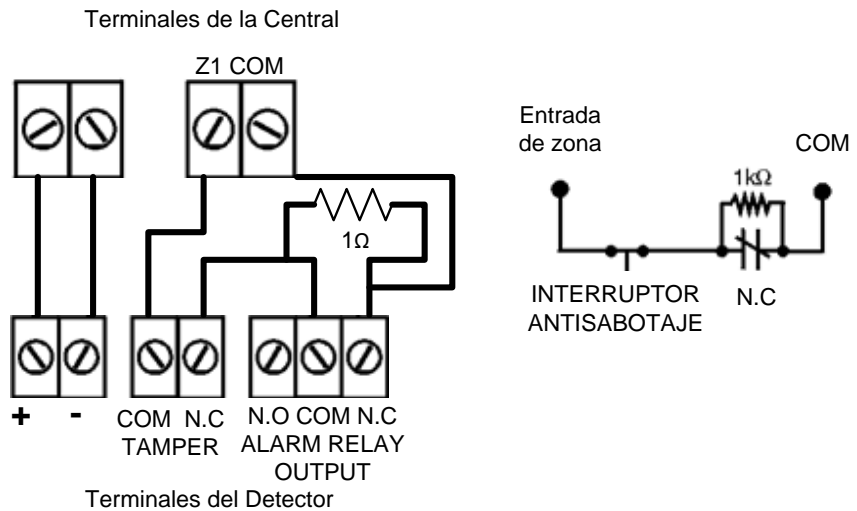
- **Contactos N.C. y N.O., Con Resistencia RFL**

Si la instalación de seguridad no necesita detección antisabotaje o de fallos de cableado, algunos detectores usan contactos normalmente abiertos, al conectar todos los detectores se usa una resistencia de fin de línea (RFL) de  $1k\Omega$  como muestra el gráfico 6.31:



**Gráfico 6. 31 Sensores NC y NO con resistencia RFL**  
**Elaborado por: Franklin Baldospin**

- Contactos N.C., Sin Resistencia RFL, Con Detección de Sabotaje**  
 Si se requiere detección de sabotaje, todos los detectores deben usar contactos normalmente cerrados, como la muestra el gráfico 6.32, comunicando a la central

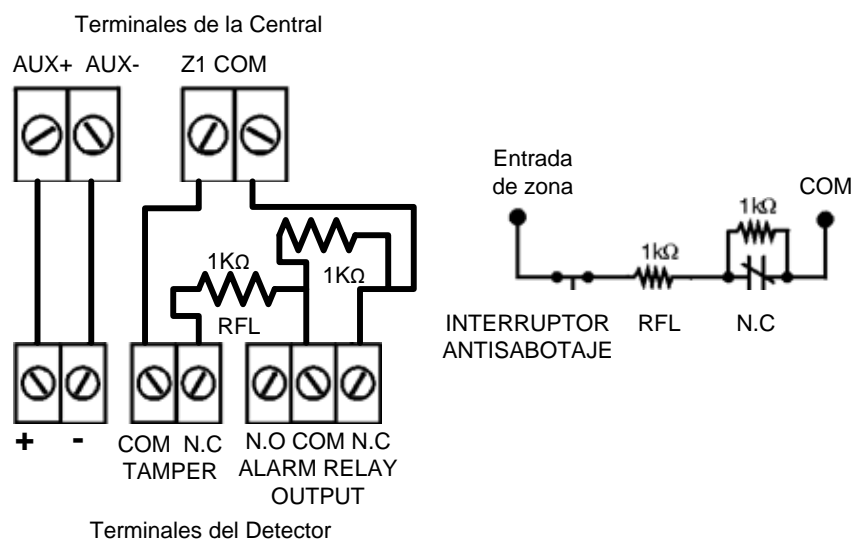


**Gráfico 6. 32 NC sin RFL con detección de Sabotaje**  
**Elaborado por: Franklin Baldospin**



- **Contactos N.C., Con Resistencia RFL, Con Detección de Sabotaje y Fallo de Cableado**

El reconocimiento de sabotaje y fallo de cableado (corto circuito) se lo realiza conectando los dispositivos de contactos normalmente cerrados como lo indica el gráfico 6.33. Esta configuración comunicará una zona abierta o cerrada a la central, mostrando en el teclado las zonas abiertas. La central también comunicará cualquier sabotaje (corte de cable) y/o fallo de cableado (corto circuito) detectado.



**Gráfico 6. 33 NC con Sabotaje y Corte**  
**Elaborado por: Franklin Baldospin**

Identificando el tipo de sensor a utilizar y la correcta conexión hacia la central se configura el equipo grabador de la siguiente manera:

3.- Se Ingresa en la pestaña Avanzando, Submenú Alarma en la cual por cada canal se activa la señal de movimiento, identificando que tipo de sensor utilizado (N.C, N.O), además de pérdida de video, pérdida del disco duro (HDD), como espacio en el mismo, la señal se maneja mediante una salida (borneras) a un buzzer (alarma) controlando tiempos tanto de zumbador y grabación todo independiente de la central PC1832

4.- Se cuenta con una alerta mediante Email como lo demuestra la gráfica 6.34 donde se configura los siguientes parámetros:

**Email: Encendido**

Ajustar la alarma en encendido

**SSL: ON**

SSL Secure Socket Layer (capa de conexión segura), es un protocolo de transporte, donde se puede cifrar la información de comunicación (incluyendo la dirección de correo electrónico), para prevenir un monitoreo al correo electrónico, la contraseña, o la información de comunicación.

Se ajusta el SSL a “encendido” y en el servidor Gmail.com, se configura en “apagado”, si la configuración no es la correcta se indaga en el sitio web personal para obtener el servidor SMTP y el casillero de correo de SSL.

**Puerto SMTP: 25**

Simple Mail Transfer Protocol (SMTP) (Protocolo para la transferencia simple de correo electrónico), es un protocolo de la capa de aplicación, basado en texto, utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA, teléfonos móviles, etc.), está definido en el RFC 2821 y es un estándar oficial de Internet.

Indica el puerto del remitente del servidor SMTP, generalmente el valor es 25 o 587 (Alternativo para clientes de correo), pero existen excepciones como el puerto SMTP del servidor de G-Mail el cual es 465.

**Servidor SMTP: smtp.gmail.com**

Indica la dirección de servidor que se utiliza de preferencia Gmail, ya que la capacidad es amplia para los datos a recibirse

**Correo electrónico remitente:** aaa@gmail.com (ejemplo)

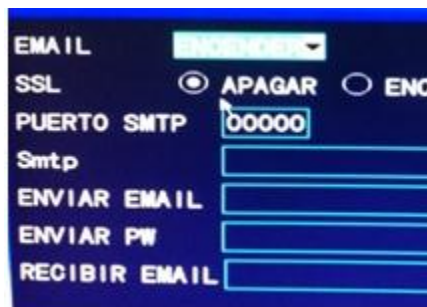
Indica la dirección de correo electrónico del remitente, esta debe ser consistente con el servidor se utiliza.

**Dirección del receptor:** fbrlpiruco@gmail.com (ejemplo)

Indica la dirección de correo electrónico del receptor para recibir imágenes transmitidas por la alarma de detección de movimiento del DVR, se debe eliminar tan pronto como sea posible las imágenes que se recibió para evitar sobrecargar la cuenta de correo electrónico.

**Enviar PW:**               \*\*\*\*\*

Contraseña configurada



**Gráfico 6. 34 Submenú Alarma**  
**Fuente: DVR TopBand TBO-9716E**

5.- El submenú **MOVIMIENTO** opera la activación para grabación de video en cada cámara al detectar movimiento, variando el nivel de sensibilidad deseado y área de cobertura, parámetros administrables vía local o remota hacia el equipo grabador así:

- Estado: Cerrar ( activa el modo movimiento de cada cámara)
- Sensibilidad: 1-4 ( valores de mínimo a máximo)
- Área MD: área de movimiento (selecciona la área más sensible)

6.- Para el funcionamiento de una cámara **PTZ** se ingresa al menú referente, donde se modifica parámetros de control indicado en el gráfico 6.35 así:

**Protocolo: PELCO P / PELCO D**

Pelco es la marca creadora de los protocolos más utilizados en cámaras PTZ siendo los más recomendados PELCO-P(8 bytesH) o PELCO-D(7bytes H).

**Velocidad: 4800 P-D o 2400 P-P**

Velocidad de transmisión (RATE) de los datos transmitidos en bits por segundo (bps)

**Bit de paridad o datos: 8**

Método de control de errores el cual se establece en 8 para cualquier caso

**Bit de Parada: 1**

Bits de transición de datos en el cual espera para la siguiente orden; están en el rango de los 500ms.

**Dirección: 1**

Dirección lógica de cada cámara por defecto están configuradas en 2 a la cual se la debe restar 1, por lo cual la dirección es siempre 1

**Crucero: Encendido**

Opción para activar posiciones de la cámara pre programadas al igual que la velocidad de cambio de cada imagen.



**Gráfico 6. 35 Configuración PTZ**  
**Fuente: DVR TopBand TBO-9716E**

La manipulación independientemente de la programación de la PTZ se la realiza mediante el control manual existente en el programa, como lo indica la gráfica 6.36 así:



**Gráfico 6. 36 Control PTZ**  
**Fuente: DVR TopBand TBO-9716E**

7.- La conexión en Red es importante para la comunicación de los datos sea esta en una red LAN o WEB; por lo cual se necesita de un switch o router el cual permite el acceso a dicha red a continuación se detalla la configuración del equipo así:

**Tipo. Static**

**Puerto Medios: 81**

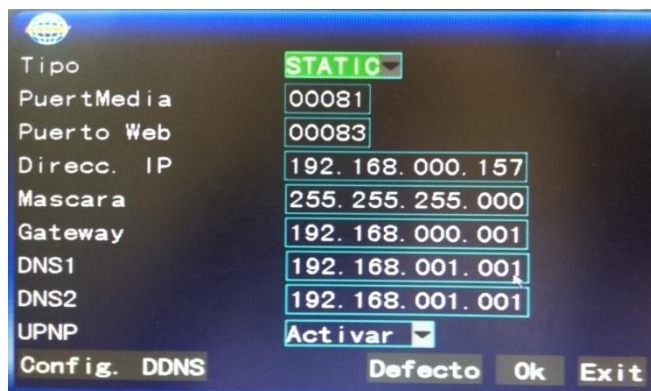
Puerto para una comunicación en red, verificando la IP asignada al DVR

**Puerto Web: 83, 5050, 8080,**

Puertos necesarios para una conexión a través del internet, estos puertos deben ser habilitados en el router.

### Dirección IP: 192.168.0.157

La dirección IP utilizada debe estar el rango disponible de la red interna (100-199), la IP pública asignada por el proveedor ISP es 186.47.84.11/248, con DNS 201.219.1.19 como lo indica el gráfico 6.37 así:



**Gráfico 6. 37 Submenú RED**  
**Fuente: DVR TopBand TBO-9716E**

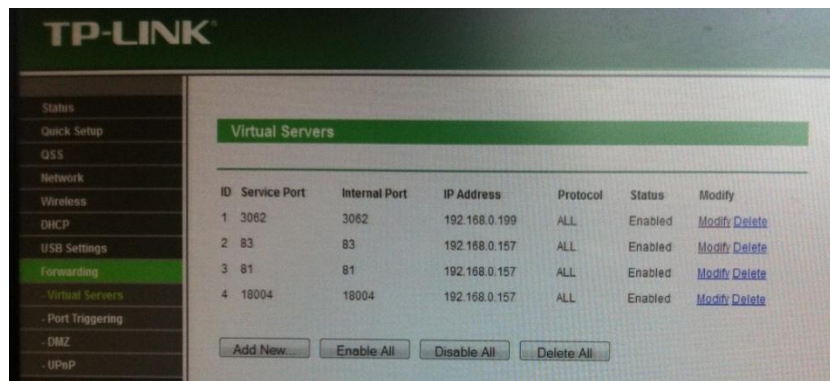
De acuerdo a la Red de la Fuerza de la Brigada Selva N°17 manipulada por personal de comunicación se informa que el acceso mediante WEB es restringido hacia la dirección IP 10.24.32.120/0 por razones de seguridad a la cual solo mediante una interconexión en un recinto militar se podrá acceder remotamente, es así que se habilita una red civil con la siguiente dirección IP 186.47.84.11/248 con apertura de los puertos para la comunicación, los cuales son 81, 83, 18004, 3062, 3064 para las pruebas de funcionamiento con un accesos local y remoto del sistema.

8.- La búsqueda de los archivos se realiza de varias maneras por tiempo de video, por evento de video, gestionando las imágenes, y por búsqueda de imágenes, en las cuales se ingresa la fecha y hora deseada, la copia de seguridad de los videos están en formato AVI, reproducido mediante programas de libre accesos como Real Player o Multimedia.

## Monitoreo Remoto

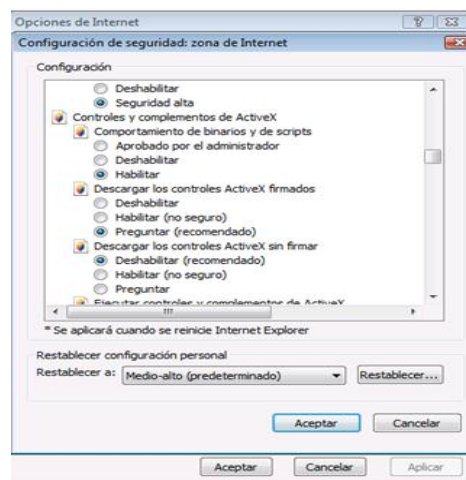
Para un acceso remoto desde una o varias dispositivos sean estas computadoras o dispositivos móviles, el grabador requiere configurar un protocolo de configuración dinámica de host o IP pública, con sus respectivos puertos.

De antemano verificamos si la direcciones IP esta correctamente subida al router TP-Link 300 utilizado en la red interna como lo muestra el gráfico 6.38 así:



**Gráfico 6. 38 Ingreso CMD**  
**Fuente: DVRQ-see QT428**

A continuación se habilita los controles ActiveX, en la pestaña Herramientas, opciones de internet, seguridad, nivel personalizado, como lo indica el gráfico 6.39 así:



**Gráfico 6. 39 Habilitación ActiVex**  
**Fuente: Servidor PC**

Una vez realizado estas operaciones, se instala el programa NetView para acceder; al ingresar al sistema de vigilancia, es necesario dirección IP, puerto a conectarse y contraseña el cual previamente está configurado como lo indica el gráfico 6.40:



**Gráfico 6. 40 Programa NetView**

**Fuente: Servidor PC**

La administración es idéntica a una configuración local del DVR cumpliendo con todas las funciones a las cuales tiene accesos el usuario, como la muestra el gráfico 6.41:



**Gráfico 6. 41 Visualización del Sistema de Vigilancia**

**Fuente: Programa NetView**

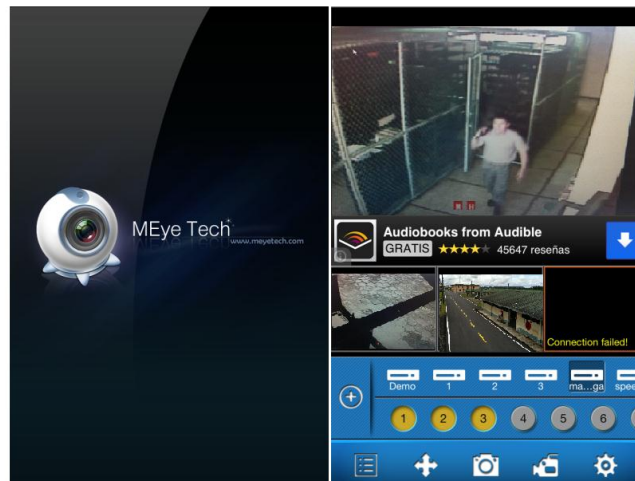
## **Vigilancia Móvil**

El DVR permite un monitoreo móvil desde teléfonos inteligentes y otros dispositivos que utilizan los sistemas operativos Android, Blackberry, Symbian y Windows Mobile Pro, además del iPad y iPhone en redes 3G o Wi-Fi



Se analizó la configuración en un iPhone o iPad por ser las tecnologías más actuales sin embargo se puede optar por otros equipos del mercado.

Para acceder se configura el equipo grabador digital con el puerto 18004, y en el dispositivo móvil se instala el programa Asee o KMeye free (software libre), obtenido mediante iTunes; aplicación que se conecta como lo muestra el gráfico 6.42 así:



**Gráfico 6. 42 Aplicación iTunes**  
**Fuente: Tienda iTunes**

#### **6.8.10 Control de Accesos**

##### **Configuración del Teclado DSC LCD 5511**

La configuración del teclado, se lo realiza con los siguientes códigos de programación así:

<b>5555</b>	Código de Instalador
<b>1234</b>	Código de Usuario
<b>#</b>	Borrar
<b>##</b>	Guarda y salir (final de cada línea de programación)

La programación del teclado es similar al sistema central, cada programación realizada se visualizara con alertas en la parte superior del panel led, habilitando y deshabilitando opciones presionando el número correspondiente.



Se recomienda activar las opciones 1,4,6,7 las siguientes son reservadas para una futura configuración.

Las teclas de emergencia, incendio, auxilio y pánico, por recomendación del fabricante están activas sin embargo se puede configurar personalmente sus parámetros así:

(*) (8) (5555)	Código del instalador
(000)	Acceso a programación de teclado
(7)	opciones de las teclas de emergencia
«1.2.3»	activas
«4-7»	para uso futuro
«8»	aviso de temperatura baja
##	

En caso de falla en el ingreso de los datos se intenta nuevamente, o se presiona el siguiente código el cual restaura el sistema al de fábrica así:

**(\*) (8) (5555) (999) (5555) (999)** Restaura al sistema original todos los valores

### **Configuración de Alarma DCS 1832**

Antes de configurar la alarma 1832 se recomienda un estudio del manual a fin de evitar fallos y satisfacer la necesidad requerida.

Los comandos de usuario permiten una configuración tanto en:

- Armado en modo ausente

La luz **ready**, encendida para todos los dispositivos cuando están activados o excluidos a continuación se marca el código de usuario valido y se procede a salir por la puerta programada con retardo, tras el armado la luz **armed** se encenderá

- Armado en modo presente

La luz **ready**, encendida, se ingresa el código valido, se permanece en el lugar, no se puede abrir una zona programada con retardo y tras el armado la luz **armed** se enciende y queda todo el ambiente protegido.

- Desarmado

El usuario debe ingresar por una puerta programada como retardo, tras la entrada el teclado emitirá un tono fijo para alertar al usuario que debe desarmar el sistema, y marcar el código valido.

Si ha ocurrido algún disparo de alarma mientras el sistema estaba armado, la luz de la memoria y las zonas que estuvieron en alarma titilaran o se mostraran en el visor LCD se marca # para que el teclado regrese al estado ready.

### Comandos ( \* )

Los comando más utilizados se detallan a continuación sin embargo de acuerdo a las necesidades del ambiente a instalarse se puede configurar más opciones apoyados del manual de operaciones.

- (\*)(1) Exclusión (sistema desarmado) / reactivar zonas en modo presente/ausente cuando sistema armado
- (\*)(2) menú de condiciones de falla
- (\*)(3) memoria de alarma
- (\*)(4) habilitar/deshabilitar el sonido de la puerta
- (\*)(5) programación de códigos de usuario
- (\*)(6) comandos de usuario
- (\*)(7)(x) funciones de comando 1 - 4
- (\*)(8) programación de instalador
- (\*)(9)(Código)armado presente sin retardo de entrada
- (\*)(0) armado rápido (sistema desarmado)/Salida rápida (sistema armado)

En caso de registrarse fallo en el sistema tanto en modo armado como ausente, se procede a la identificación del mismo ingresando el siguiente código:

**(\*)(2) Visualización de fallas**

De acuerdo la Tabla 6.7 se detallan los problemas que se puedan suscitar:

<b>Número</b>	<b>Problema</b>
<b>(1)</b>	Batería baja
<b>(2)</b>	Circuito de la sirena
<b>(3)</b>	Problema general en el sistema
<b>(4)</b>	Sabotaje general en el sistema
<b>(5)</b>	Supervisión del modulo
<b>(6)</b>	Bloqueo de RF detectado
<b>(7)</b>	Batería baja en el pc1832
<b>(8)</b>	Falla CA en el pc 1832
<b>Luz (1)(*)</b>	Mantenimiento necesario
<b>Luz (2)(*)</b>	Problema de CA
<b>Luz (3)(*)</b>	Problema en la línea telefónica
<b>Luz (4)(*)</b>	Falla en la comunicación
<b>Luz (5)(*)</b>	Falla en la zona
<b>Luz (6)(*)</b>	Sabotear en la zona
<b>Luz (7)(*)</b>	Batería baja en el dispositivo inalámbrico
<b>Luz (8)(*)</b>	Perdida de hora y fecha

**Tabla 6. 7 Fallas**  
**Elaborado por: Franklin Baldospin**

La programación de la unidad de control PC1832 se realiza mediante el teclado 5511 en el cual se ingresa el código de instalador; inmediatamente se visualizara un icono de espera en el LCD lo cual indica petición de datos, un tono continuo indica error, dos tonos indican que se puede continuar con el siguiente paso.

Las luces de armado y listo muestran el estado de la programación:

*Luz Armado encendida*; panel esperando por el número de la sección (3 dígitos)

*Luz listo encendida*; panel esperando por la entrada de datos

*Luz listo intermitente*; panel esperando por la entrada de datos HEX

No es posible entrar en modo de programación del instalador mientras el sistema está armado o en alarma

### **Definiciones de Zonas**

Existen 4 secciones o particiones, de las cuales cada una cuenta con 8 zonas programables, con un total de 32 zonas cableadas.

La configuración para, un contacto magnético, un sensor de movimiento, y un botón de pánico, se detalla a continuación:

(*) (8) (5555)	Ingreso a la configuración como instalador
(001)	Definición de las zonas en la sección 1
(01)	<b>Retardo1</b> (cuando está armado da un retardo de entrada cuando es activada, sensor de movimiento)
(03)	<b>Instantánea</b> (cuando está armado alarma instantánea cuando es activada, contacto magnético)
(08)	<b>Incendio Estándar 24h</b> , alarma instantánea cuando es activada, sensor de humo
(00)	<b>Zona nula</b> , para las restantes zonas no utilizadas
# #	Guardar y salir

### **Tiempos del Sistema**

Se ingresa en la sección (005), donde se indica con un número de dos dígitos la partición a configurar (01, 02, 03, 04), y a continuación se programa los retardos o demora en el tiempo de respuesta de la alarma.

Las particiones permiten trabajar independientemente cada una de ellas como 4 sistemas independientes cada uno con su teclado, o como 1 unidad de control central, manejando diferentes sectores, es por esta razón que se debe apuntar a la correcta partición a trabajar así:

(*) (8) (5555)	Ingreso
(005)	Tiempos del sistema
(01)	Partición 1
(020)	Retardo de entrada 1 (tiempo en segundos, 20s)
(020)	Retardo de entrada 2 (tiempo en segundos, 20s)
(010)	Retardo de salida (tiempo en segundos, 10s)
##	Guardar y Salir

### **Salidas PGM**

La Unidad PC1832 tiene dos salidas PGM en la tarjeta, con capacidad de crecer hasta 14 salidas de baja y alta corriente según la RFL utilizada.

Esta salida es necesaria para cualquier sensor de humo; el cual ayuda al reseteo correcto del sensor en caso de activación.

(*) (8) (5555)	Ingreso
(009)	Salida PGM
(03)	Restauración del sensor
##	Guardar y salir

La salida permanecerá normalmente activa y se desactivara por cinco segundos cuando un comando de restauración de incendio (\*) (7) (2) sea ejecutado o cuando se detecte una alarma de incendio con verificación automática.

### **Bloqueo de Teclado**

El sistema bloquea el teclado cuando una serie de códigos erróneos son digitados, emite un tono de error fijo de dos segundos y se envía alertas a la central; para la configuración de número de intentos y tiempos se lo detalla a continuación:

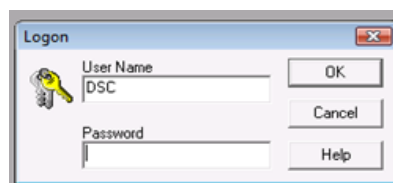
(*) (8) (5555)	Ingreso
(012)	bloqueo de teclado
(010)	intentos de códigos erróneos
(020)	tiempo de bloqueo
##	Guardar y salir
(000)	desactivar la función

## DLS 5

La transmisión de los datos mediante una red hacia un servidor se realiza utilizando una tarjeta TL-250 adicional conectada a la unidad de control PC1832 la cual funciona de transmisor y como receptor el programa DLS 5, el mismo que reconoce y almacena información necesaria para el control de accesos.

El programa DLS 5 es una herramienta útil para el registro de cualquier evento ocasionado en la alarma, siendo capaz de almacenar un máximo de 150, sean estos cierre, apertura, disparos de alarma, manipulación de códigos, identificación de usuarios, cortes de energía, fallas a nivel operativo del sistema, etc. con lo cual se lleva un informe con fecha, hora y tipo de eventualidad.

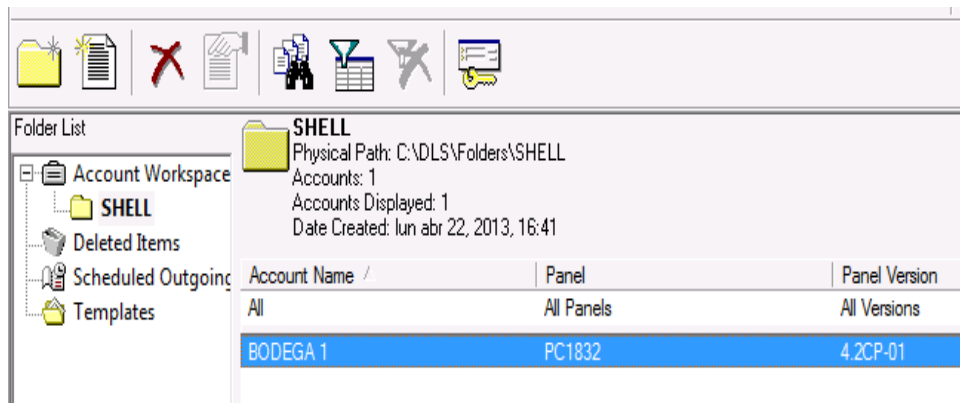
Para el ingreso al software se llena los parámetros, nombre DSC y contraseña 1234 valores por defecto como lo indica el gráfico 6.43 así:



**Gráfico 6. 43 Ingreso DLS**  
**Fuente: DLS 5**

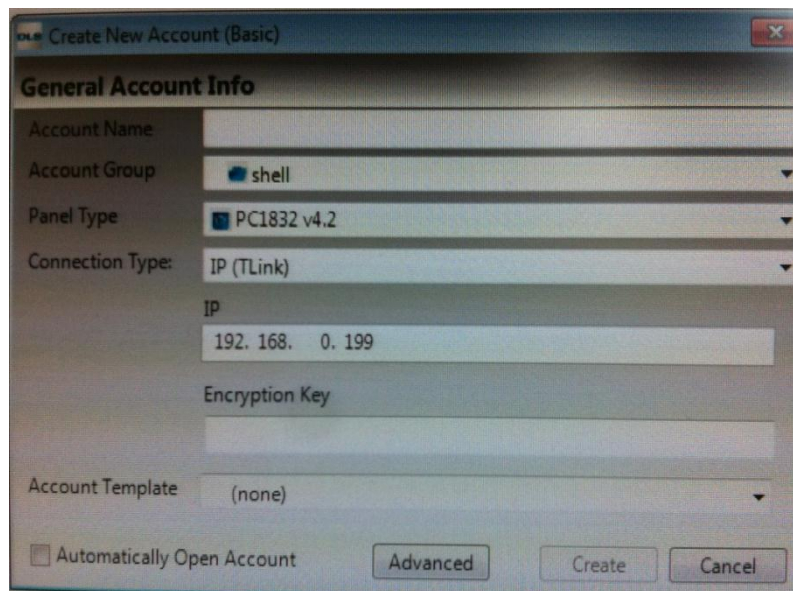
A continuación se crea un archivo en la base de datos del software con el nombre de la localización (**SHELL**), necesario para la identificación del sistema como lo ilustra el gráfico 6.44 así:





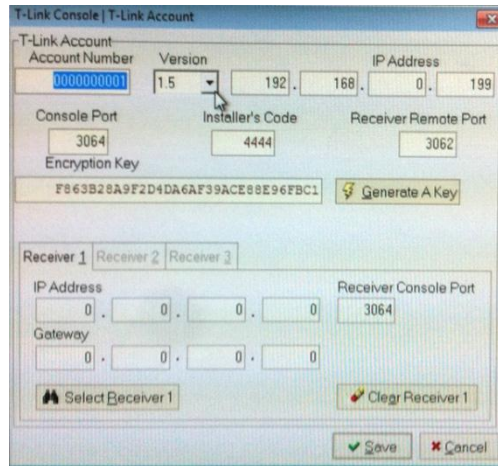
**Gráfico 6. 44 Nueva Carpeta Shell**  
**Fuente: DLS 5**

En la pestaña **Create New Account** ubicada en la barra de herramientas general, se ingresa los datos de la cuenta, como el nombre de cada unidad de control, numero telefonico si la conexión es por DLS, tipo de alarma (PC 1832) y la version actualizada de la misma como se visualiza en el gráfico 6.45 así:



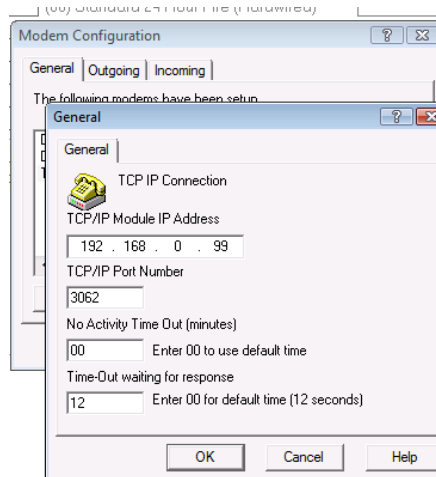
**Gráfico 6. 45 PC 1832**  
**Fuente: DLS 2012**

Si la transmision es por TCP/IP se ingresa la direccion IP de la tarjeta T-Link 250, con la unidad de control PC 1832, los puertos 3062 y 3064 como lo indica el gráfico 6.46:



**Gráfico 6. 46 IP PC 1832**  
**Fuente: DLS 5**

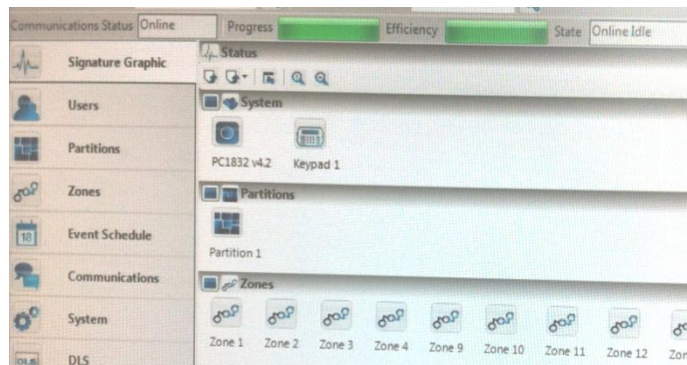
La configuración del modem por el cual se direcciona la información se lo realiza a través de la herramienta **Tools** en la subsección **Modem Configuración** como lo muestra la gráfica 6.47 así:



**Gráfico 6. 47 Modem Configuración**  
**Fuente: DLS 5**

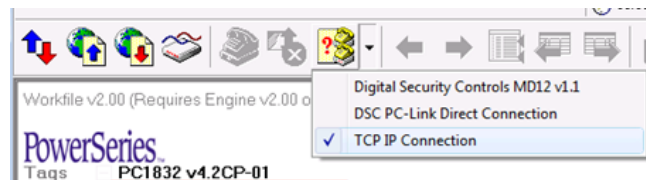
- TCP/IP: Dirección IP conectada
- TCP/IP Port: Puerto de Conexión 3062
- Time Out: Tiempo de No actividad
- Time Out Waiting: Tiempo de espera para la respuesta

Finalmente la ventana por la cual se visualiza la Unidad de Control PC1832 monitoreada es como lo indica la gráfica 6.48 siguiente:



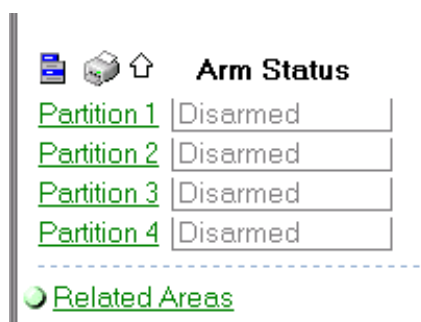
**Gráfico 6. 48 Dispositivos en Línea**  
**Fuente: DLS 5**

La conexión mediante el protocolo TCP/IP se lo indica a través de la siguiente pestaña del gráfico 6.49 así:



**Gráfico 6. 49 Tipo de Conexión**  
**Fuente: DLS 5**

Al iniciar una petición de datos a la central de antemano se verifica el estado de la misma; la opción **PC1832 Status**, confirma si el sistema está armado o desarmado, a continuación se descargan los datos a una velocidad de 318Mbps, visualizándose el estado de las 4 particiones como lo indica el gráfico 6.50:



**Gráfico 6. 50 Estado del sistema**  
**Fuente: DLS 5**

## Autenticación y Base de Datos

La Unidad PC1832 para el control de acceso a la Bodega N°3 cuenta con una base de datos y autenticación de personal mediante el uso del contraseñas proporcionadas al personal autorizado, detallado a continuación en la tabla 6.8:

Cargo	Clave	Locación
Cap. Franklin Oña	2468	Comandante U.C 17BS
Bodeguero CAL	0102	B. CAL Armamento Asalto
Bodeguero BOES	0304	B. BOES Armamento Entrenamiento
Auxiliar CAL	0506	B. CAL Armamento Asalto
Auxiliar BOES	0708	B. BOES Armamento Entrenamiento

**Tabla 6. 8 Base de datos**  
**Elaborado por: Franklin Baldospin**

La información es ingresada a la base de datos creada en la unidad de control como lo muestra el gráfico 6.51 así:

User Code	Partition 1	Supervis...	Duress	Bypass	Remote Access	Bell Squawk	One Time Use	Opening Reporting Code	Closing Reporting Code	
User 1	0102	Yes	No	No	No	Yes	No	FF	FF	BODEGUERO CAL1
User 2	0304	Yes	No	No	No	Yes	No	FF	FF	BODEGUERO CAL2
User 3	0506	Yes	No	No	No	Yes	No	FF	FF	BODEGUERO BOES1
User 4	0708	Yes	No	No	No	Yes	No	FF	FF	BODEGUERO BOES2
User 5	AAAA	No	No	No	No	No	No	FF	FF	
User 6	AAAA	No	No	No	No	No	No	FF	FF	
User 7	AAAA	No	No	No	No	No	No	FF	FF	
User 8	AAAA	No	No	No	No	No	No	FF	FF	
User 9	AAAA	No	No	No	No	No	No	FF	FF	
User 10	AAAA	No	No	No	No	No	No	FF	FF	
User 11	AAAA	No	No	No	No	No	No	FF	FF	
User 12	AAAA	No	No	No	No	No	No	FF	FF	
User 13	AAAA	No	No	No	No	No	No	FF	FF	
User 14	AAAA	No	No	No	No	No	No	FF	FF	
User 15	AAAA	No	No	No	No	No	No	FF	FF	
User 16	AAAA	No	No	No	No	No	No	FF	FF	
User 17	AAAA	No	No	No	No	No	No	cc	cc	

**Gráfico 6. 51 Base de Datos y Claves**  
**Fuente: DLS 5**

En primer lugar se debe verificar el estado del sistema, a continuación la base de datos almacena hasta 72 usuarios con claves desde 4 a 6 dígitos, cada uno de los

usuarios tiene un nivel de acceso permitido según las atribuciones configuradas, y existe un acceso universal o código máster #40 el cual accede a todo el sistema, si restricciones proporcionado al comandante en turno encargado de la Bodega

#### Atribuciones

- Superv: Supervisión de la alarma
- Durre: Código de asalto a nivel operativo
- Bypass: Exclusión de zonas
- Escort: Modulo de Accesos Remoto
- FFU: Activación de PGM
- Bell: Acceso a disparos de alarma
- One: Cantidad de veces a utilizar el código ingresado
- Part1: Acceso a que partición

La información se la visualiza en una lista con fecha, hora y tipo de evento registrado en la alarma, como lo indica el gráfico 6.52 , todos estos datos se puede almacenar para un reporte en caso de necesitarlo, ademas con una conexión a internet se puede operar atraves de cualquier dispositivo movil.

Event	Date/Time	Event
Event Buffer Appended	15/07/2013 21:20	
Partition 1	15/07/2013 21:14	System Test
Partition 1	15/07/2013 21:12	Special Opening
Partition 1	15/07/2013 21:12	Opening by Downloading
Partition 1	15/07/2013 21:08	Armed in Away Mode
Partition 1	15/07/2013 21:08	Special Closing
Partition 1	15/07/2013 21:08	Closing by Downloading
System	15/07/2013 20:31	DLS Lead Out
Partition 1	15/07/2013 20:21	System Test
Partition 1	15/07/2013 20:20	Special Opening
Partition 1	15/07/2013 20:20	Opening by Downloading
Partition 1	15/07/2013 20:19	Armed in Away Mode
Partition 1	15/07/2013 20:19	Special Closing
Partition 1	15/07/2013 20:19	Closing by Downloading
System	15/07/2013 20:17	DLS Lead Out

**Gráfico 6. 52 Datos Recolectados**  
**Fuente: DLS 2012**

## FASE IV

### COMUNICACIÓN DE RESULTADOS

#### 6.8.11 Pruebas y Fallas del Sistema de Video–Vigilancia

Se verifica con material fotográfico la incidencia del prototipo instalado en el Batallón Selva N°17, tanto para el sistema de vigilancia como el monitoreo de la bodega CAL Y BOES de material bélico visualizado en el gráfico 6.53 y 6.54 así:

Monitoreo:



**Gráfico 6. 53 Visualización en la Central de Monitoreo**  
Elaborado por: Franklin Baldospin

Cámara PTZ: Ubicación




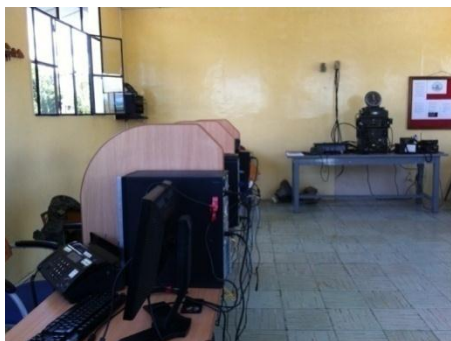


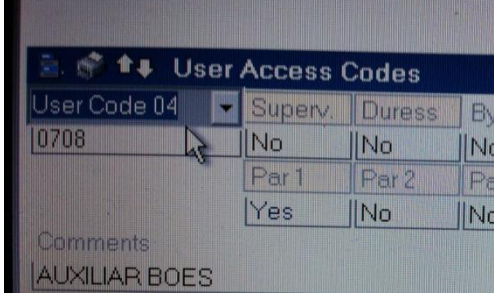
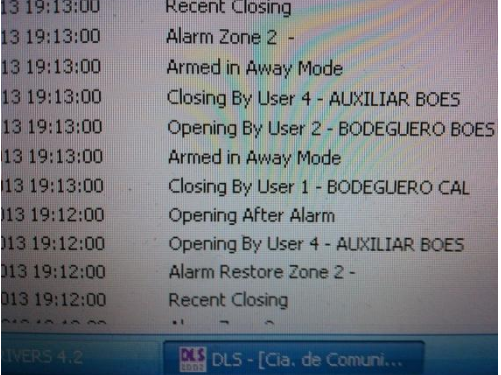
**Gráfico 6. 54 Ubicación PTZ**  
Elaborado por: Franklin Baldospin

Posiciones programadas de cobertura



**Gráfico 6. 55 Vistas PTZ**  
Elaborado por: Franklin Baldospin

Central de Monitoreo y Control: Infraestructura y Equipo

<p><i>Unidad de Comunicaciones</i></p>	<p><i>Equipos Existentes</i></p>																																								
																																									
<p><i>Equipo y Servidor</i></p>	<p><i>Ping a la conexión DLS</i></p>																																								
	 <table border="1"> <thead> <tr> <th>Count</th> <th>IP Address</th> <th>Response Time</th> </tr> </thead> <tbody> <tr> <td>13</td> <td>192.168.0.57</td> <td>33.4 ms</td> </tr> <tr> <td>12</td> <td>192.168.0.57</td> <td>17.0 ms</td> </tr> <tr> <td>11</td> <td>192.168.0.57</td> <td>5.6 ms</td> </tr> <tr> <td>10</td> <td>192.168.0.57</td> <td>14.5 ms</td> </tr> </tbody> </table>	Count	IP Address	Response Time	13	192.168.0.57	33.4 ms	12	192.168.0.57	17.0 ms	11	192.168.0.57	5.6 ms	10	192.168.0.57	14.5 ms																									
Count	IP Address	Response Time																																							
13	192.168.0.57	33.4 ms																																							
12	192.168.0.57	17.0 ms																																							
11	192.168.0.57	5.6 ms																																							
10	192.168.0.57	14.5 ms																																							
<p><i>Base de Datos</i></p>	<p><i>Registro de Eventos</i></p>																																								
 <table border="1"> <thead> <tr> <th>User Code</th> <th>Superv.</th> <th>Duress</th> <th>By</th> </tr> </thead> <tbody> <tr> <td>04</td> <td>No</td> <td>No</td> <td>No</td> </tr> <tr> <td>0708</td> <td>Par 1</td> <td>Par 2</td> <td>Pa</td> </tr> <tr> <td></td> <td>Yes</td> <td>No</td> <td>No</td> </tr> </tbody> </table> <p>Comments AUXILIAR BOES</p>	User Code	Superv.	Duress	By	04	No	No	No	0708	Par 1	Par 2	Pa		Yes	No	No	 <table border="1"> <thead> <tr> <th>Timestamp</th> <th>Event Description</th> </tr> </thead> <tbody> <tr> <td>13 19:13:00</td> <td>Recent Closing</td> </tr> <tr> <td>13 19:13:00</td> <td>Alarm Zone 2 -</td> </tr> <tr> <td>13 19:13:00</td> <td>Armed in Away Mode</td> </tr> <tr> <td>13 19:13:00</td> <td>Closing By User 4 - AUXILIAR BOES</td> </tr> <tr> <td>13 19:13:00</td> <td>Opening By User 2 - BODEGUERO BOES</td> </tr> <tr> <td>13 19:13:00</td> <td>Armed in Away Mode</td> </tr> <tr> <td>13 19:13:00</td> <td>Closing By User 1 - BODEGUERO CAL</td> </tr> <tr> <td>13 19:12:00</td> <td>Opening After Alarm</td> </tr> <tr> <td>13 19:12:00</td> <td>Opening By User 4 - AUXILIAR BOES</td> </tr> <tr> <td>13 19:12:00</td> <td>Alarm Restore Zone 2 -</td> </tr> <tr> <td>13 19:12:00</td> <td>Recent Closing</td> </tr> </tbody> </table>	Timestamp	Event Description	13 19:13:00	Recent Closing	13 19:13:00	Alarm Zone 2 -	13 19:13:00	Armed in Away Mode	13 19:13:00	Closing By User 4 - AUXILIAR BOES	13 19:13:00	Opening By User 2 - BODEGUERO BOES	13 19:13:00	Armed in Away Mode	13 19:13:00	Closing By User 1 - BODEGUERO CAL	13 19:12:00	Opening After Alarm	13 19:12:00	Opening By User 4 - AUXILIAR BOES	13 19:12:00	Alarm Restore Zone 2 -	13 19:12:00	Recent Closing
User Code	Superv.	Duress	By																																						
04	No	No	No																																						
0708	Par 1	Par 2	Pa																																						
	Yes	No	No																																						
Timestamp	Event Description																																								
13 19:13:00	Recent Closing																																								
13 19:13:00	Alarm Zone 2 -																																								
13 19:13:00	Armed in Away Mode																																								
13 19:13:00	Closing By User 4 - AUXILIAR BOES																																								
13 19:13:00	Opening By User 2 - BODEGUERO BOES																																								
13 19:13:00	Armed in Away Mode																																								
13 19:13:00	Closing By User 1 - BODEGUERO CAL																																								
13 19:12:00	Opening After Alarm																																								
13 19:12:00	Opening By User 4 - AUXILIAR BOES																																								
13 19:12:00	Alarm Restore Zone 2 -																																								
13 19:12:00	Recent Closing																																								

**Gráfico 6. 56 Infraestructura Existente**  
**Elaborado por: Franklin Baldospin**



Unidad de Control PC 1832 y dispositivos



**Gráfico 6. 57 Control de Accesos**  
**Elaborado por: Franklin Baldospin**

### 6.8.12 Presupuesto

El valor que tiene la ejecución del prototipo de red de video- vigilancia para el monitoreo y control de accesos al 17-BS en el tiempo establecido, asume a la cantidad de \$ **2724,00** para lo que se toma en cuenta los siguientes recursos descritos en las Tablas 6.9 - 6.10 y 6.11 así:

#### Costos Materiales

<b>MATERIALES</b>	<b>VALOR \$</b>
Uso de Internet	50,00
Memory 8 gb	35,00
Resmas de hojas	8,00
Impresiones	35,00
Cable UTP Cat 6	125,00
Amarras 25U	5,00
Taípe	1,00
Estilete	1,00
<b>TOTAL</b>	<b>260,00</b>

**Tabla 6. 9 Costos Materiales**  
**Elaborado por: Franklin Baldospin**

## Costos Equipos

<b>EQUIPOS</b>	<b>CANTIDAD</b>	<b>VALOR \$</b>
Cámaras TopBand (3,6mm) domo	1	120,00
Cámara TopBand (3,6mm) tubular	1	120,00
Cámara Zmodo PTZ	1	750,00
DVR TopBand (4 CH)	1	350,00
Baluns (pares)	4	30,00
Fuentes de Alimentación (12V-5 A)	3	20,00
Conectores Pulpo	2	4,00
Alarma DCS 1832	1	300,00
Tarjeta de red DCS 1832	1	450,00
Sensor de Movimiento DCS	1	20,00
<b>TOTAL</b>		<b>2164,00</b>

**Tabla 6. 10 Costos Equipos**  
**Elaborado por: Franklin Baldospin**

## Presupuesto General

<b>CONCEPTO</b>	<b>VALOR</b>
MATERIALES	260,00
EQUIPOS	2164,00
TRANSPORTE	150,00
VARIOS	150,00
<b>TOTAL</b>	<b>2724,00</b>

**Tabla 6. 11 Presupuesto General**  
**Elaborado por: Franklin Baldospin**

## 6.9 Conclusiones y Recomendaciones

### Conclusiones

- La implementación de cámaras con sensores CCD (fijas, domo, PTZ) en el sistema de seguridad de la Bodega N°3 Unidades CAL y BOES, facilita la calidad de la imagen en todo espectro de condiciones de iluminación, con una resolución de 640x480 pixeles, esta se monitorea con una dirección IP pública 186.47.84.11, habilitando los puertos 83 HTTP, 81 LAN y 18004 para un dispositivo móvil, este contenido multimedia es comprimido mediante el protocolo H.264 a una velocidad de 28,8 Kbps a 1.5Mbps, así el stream de video para vigilancia y seguimiento registra una calidad excelente de imagen en formato AVI o MPGE4 según el equipo.
- El control de acceso mediante el teclado LCD 5511 que controla la unidad central PC1832 proporciona un registro de eventos con fecha, hora, y tipo de los dispositivos activados, con lo cual se mejora el método de control y autenticación del personal, a través de una base de datos interna con 1 código máster y 4 códigos auxiliares los cuales arman y desarman el sistema; estos reportes son transmitidos en red hacia una PC a velocidad promedio de LAN=120 f/s conectada a una IP Pública 186.47.84.11 la cual permite un monitoreo remoto por medio del puerto 3062, 3064.
- La transmisión de datos es mediante una red LAN con dirección IP 192.168.0.157/0, puerto 81 a una velocidad típica de 10/100Mbps hacia el equipo grabador de video digital DVR con capacidad de almacenamiento de 2Tbytes, la cual al ser totalmente independiente, brinda calidad y seguridad de los datos, necesarios para un monitoreo continuo mediante el

software NetView de 24horas|7días; optimizando tiempo y personal; de igual manera el control de accesos, está en red a un PC con dirección IP 192.168.0.60/0 el cual transmite los datos mediante la tarjeta T-Link250 a un mínimo de ancho de banda con cifrado de 128-bits y velocidad de 512Kbps, permitiendo así una comunicación estable y rápida de acceso inmediato al sistema a través del internet.

- Las comunicaciones avanzadas IP y GSM/GPRS ha permitido la utilización de teléfonos inteligentes como iPhone, Tablets de Apple, Blackberry de Windows y Android de Google los cuales permiten la conexión a internet, mediante WIFI o una red móvil necesaria para un monitoreo, administración, configuración y actualización; ventajas que brinda el software libre Asee y Habit DSC que gracias al menú adaptativo el cual maneja opciones relevantes permite una conexión estable y segura de información en vivo y a cualquier momento.

### **Recomendaciones**

- El uso de nuevas equipos para la transmisión de videos bajo demanda en el sistema Pentaplex como FURY Serie de Digital Watchdog el cual permite grabación, visualización, reproducción, transmisión sobre red y almacenamiento; marcando así una nueva tendencia hacia sistemas más seguros con mejoras al algoritmo de compresión MPEG4 reduciendo la capacidad de almacenamiento; además cuenta con una compatibilidad entre dispositivos IP y analógicos integrándose fácilmente.

- La utilización de equipos de control de accesos con mayores ventajas de marcas reconocidas como SOYAL y ENFORCER Security con módulos de control de asistencia y acceso al mismo tiempo, capacidad para 1024 usuarios y niveles de acceso como PIN, tarjeta o ambos métodos, la información es transmitida mediante un conector RS-485 conectado a módulos de interfaz TCP/IP a una velocidad de 100Mbps proporcionando reportes de entrada, salida, tardanzas, horas trabajadas, etc, la inversión es baja en contraparte con las ventajas y garantía que se ofrece con este equipo.
- La construcción de una infraestructura y ductería adecuada para cableado subterráneo por cual permita una conexión de la red LAN mediante un Transceiver Avtech de fibra a cobre disponibles de acuerdo a los canales necesarios hacia la fibra óptica(F.O.) Monomodo de 8hilos; así se puede obtener un stream de video y transmisión de datos sin perdidas y latencias ocasionadas por la conexión ADLS .
- La soluciones completas de GSM/GPRS de Risco Group son ideales para proteger ambientes de manera remota, esta cuenta con módulos bidireccionales AGM los cual proporciona una comunicación móvil primaria y una de respaldo a través de encriptación de datos con autenticación mediante PIN mejoras en la interfaz utilizada para un acceso mediante WEB o smarphoners.

## 6.10 Bibliografía

- **ADELL JORDI.** Nuevas Tecnologías de Comunicación. Barcelona España. Ediciones Edutec, 2001
- **VEGA, J.M.** Nuevas tecnologías de la información y comunicación. Madrid España. Editorial Dykinson, 2004
- **CRUZ PIÑOL M.** Contextos culturales en las nuevas tecnologías de la Información. Madrid España. Ediciones pirámide, 1999
- **SANTILLANA,** Los Sistemas de Comunicación, Primera Edición. Grupo Prisa, España, Marzo
- **DELGADO,** Antonio. Comunicaciones M2M, Grupo EROSKY, Bizkaia. Febrero 2010
- **JAIRO Amaya,** SISTEMAS GSM-GPRS , Salamanga, Tercera Edición, Marzo 2009
- **ING.CONSENTINO** Luis, Control de Accesos, Editorial RNDS, México, Abril 2000.
- **ZACKER CRAIG.** Redes. Manual de Referencia. Mc Graw Hill.
- **GROTH, DAVID; SKANDIER, TOBY** (2005). Guía del estudio de redes, (4ª edición). Sybex, Inc.. ISBN 0-7821-4406-3.
- **TANENBAUM, ANDREW S.** (2003) (Google Books). Redes de computadoras (4ª edición). Pearson Educación. ISBN 9789702601623
- **JUAN C. SANMIGUEL, JOSÉ M. MARTÍNEZ,** ‘Use of feedback strategies in the detection of events for vídeo surveillance’, IET Computer Vision, 5(5):309-319, Sept. 2011

- **TORRES, ÁLVARO.** Telecomunicaciones y telemática. Tercera edición: 2007, Colombia, Colección Telecomunicaciones.
- **HUIDOBRO MOYA, JOSÉ MANUEL.** Redes y servicios de telecomunicaciones. Madrid : Thomson, 2006.
- **HUIDOBRO MOYA, JOSÉ MANUEL.** Tecnologías de telecomunicaciones. México, D. F. : Alfaomega, c2006.
- **HERRERA PÉREZ, ENRIQUE.** Introducción a las telecomunicaciones modernas. México : Limusa, 2004.
- **AXIIS Communications,** *Guía técnica IP*, Canadá Julio 2005, Cap.1, p.8

#### **Fuentes de Internet**

- **Dispositivos TopBand** <http://www.topbandcctv.com/>
- **AVITECH DVR** <http://www.avtech.com.tw/index.php>
- **Sistemas Paradox** <http://www.paradox.com/>
- **Aplicaciones Zmodo** <http://www.zmodo.com/network-video>
- **Manual DSC PC1832** [http://cms.dsc.com/media/documents/all/PC1616-PC1832-PC1864\\_V4-2\\_NA\\_UM\\_SP\\_29007353R001.pdf](http://cms.dsc.com/media/documents/all/PC1616-PC1832-PC1864_V4-2_NA_UM_SP_29007353R001.pdf)
- **Convergencia tecnológica** [http://Convergencia\\_tecnologica.blogspot.com/](http://Convergencia_tecnologica.blogspot.com/)
- **Ejercito del Ecuador,** <http://www.ejercitodelecuador.mil.ec/>
- **DSC Products,** <http://www.dsc.com/index.php>
- **Sistemas de Seguridad,** <http://blogdeseguridad.com>

**6.11 Anexos**

**Anexo 1**

<i><b>Edificio central</b></i>	<i><b>Bodega 4. Hangar 1</b></i>	<i><b>Bodega 4 Hangar 2</b></i>
		
<i><b>Bodega 4 Hangar 3</b></i>	<i><b>Bodega 4 Caseta</b></i>	<i><b>Bodega 2</b></i>
		
<i><b>Bodega 1</b></i>	<i><b>Bodega 1 Caseta</b></i>	<i><b>Bodega 3</b></i>
		

**Gráfico 6. 58 Bodegas 1,2,3,4**  
**Elaborado por: Franklin Baldospin**



## Anexo 2

Product Image



### 8 Channel DVR | Real-time | CIF/D1 Resolution | H.264

QT428

#### Features:

- 8 Channel H.264 CIF/D1 DVR
- Remote Internet monitoring (up to 10 users at the same time)
- Mobile Phone Surveillance
- Compatible with MAC and PC
- Customize up to 8 additional cameras when you need
- Zoom In on live or playback footage with 2X digital zoom!
- Receive instant email alerts and snapshot images when motion is detected
- Send email alerts up to 3 different email addresses
- Backup and retain important footage on a PC, Flash Drive or USB Hard Drive
- Manage and monitor multiple QT-series DVRs with Central Management Software (CMS).

---

#### What's Included:

- (1) 8 Channel H.264 real-time DVR
- (1) Power supply for DVR 12V /3A
- RJ-45 Ethernet network cable
- BNC to RCA Video cable
- Remote control
- USB Mouse
- CD with manuals and software
- Quick Start Guide

---

#### Remote Monitoring Compatibility:



---

#### System Compatibility:



Windows XP, Vista, 7



Mac OS X 10.6 & 10.7

### Specification:

#### DVR

DVR Model	QT428
Video Compression	Advanced H.264
Max Hard Drive Storage	Supports 1 SATA HDD up to 2 TB
Backup Via	PC, Flash Drive, USB Hard Drive
Power	DC 12V / 3A (Adapter Included)
Operating Temperature	50°F-104°F / 10°C-40°C
CIF Recording Option	Real Time: 240 FPS (30 FPS Per Channel)
CIF Playback Resolution	352x240
D1 Recording Option	60 FPS (7.5 FPS Per Channel)
D1 Playback Resolution	704x480
Recording Mode	Motion Detection, Time Schedule, Alarm Trigger, Manual
USB Interface	USB Mouse, USB Backup
Video Inputs/Outputs	8 BNC Input(s)/1 VGA Output(s)/1 BNC Output(s)
Audio Inputs/Outputs	4 RCA Input(s) /1 RCA Output(s)
Alarm Sensor Inputs/Outputs	8 Input(s)/1 Output(s)
Network Interface	RJ-45 for Router Connection Enabling Remote Monitoring
Pan/Tilt/Zoom Control	1 RS-485 Connection (PTZ Camera Not Included)
DVR Dimensions/Weight	11.75"x 11"x 2.5" / 3.1lbs

#### Viewing

Live Display Resolution	704x480
Display Modes	Single Camera, Split Screen Multi-Camera, Auto-Sequence
Video Search	Time, Motion Detection, Alarm Trigger, Manual
Computer System Support	Windows XP, Vista, 7, Mac OS X 10.6 & 10.7
Compatible Browsers	Chrome, Internet Explorer, Mozilla Firefox, Safari
Mobile Phone Support	Android, BlackBerry 5, 6 & 7, iPhone/iPad, Windows Mobile Pro 5, 6 & Phone 7, Symbian
Simultaneous Remote Viewers	Up to 10 Users
Stream	Dual Stream

[www.Q-See.com](http://www.Q-See.com)

## Anexo3



Product Image

### Weatherproof | 540TV Line of Resolution | 100ft Night Vision

QD5401B

#### Features:

- 540TV Lines of Resolution
- Weatherproof cameras for Indoor or outdoor use
- 100 feet of night vision
- Operating Temperature = 14°F to 122°F (-10°C to 50°C)

#### What's Included:

- (1) Camera kit with QD5401B
- (1) Power adapter for camera.
- (1) 60 Ft. Stamese RG-59 shielded cable

#### Specification:

Cameras	
Camera Model	QD5401B
Weatherproof	Weatherproof Indoor & Outdoor
Horizontal Resolution	540 TV Lines
Image Sensor	1/3, CCD, Color, Sony
Infrared LEDs	48
Night Vision Range	Up to 100 ft
Lens	4.3 mm Lens (55° to 60° Field of View)
Mount	3-Axis Stands
Camera Cables	60 Feet of Cable with Each Camera
Camera Dimensions/Weight	5.75" x 3.25" x 3" / 1.4lbs

## Anexo 4



### **TBO-305\*\*\*\*IR**

#### **Features:**

- ◆ SONY / SHARP Color CCD
- ◆ IR LED:  $\phi$  5X 36PCS, IR Distance: 30m
- ◆ Board Lens 3.6mm/6mm
- ◆ Dimension: 140(L) X 73(W) X 66(H) mm
- ◆ Weight: 360g

#### **Specifications:**

Models: TBO-3052/TBO-3053/TBO-3054

1/4" SHARP / 1/3" SONY / 1/3" SONY CCD Super HAD

Definition 420TVL/420TVL/480TVL

Effective pixels PAL: 752 (H) \* 582 (V) NTSC: 768 (H) \* 494 (V) / PAL:

500 (H) \* 582 (V) NTSC: 510 (H)\*492 (V) TV System PAL / NTSC

Minimum illumination 0LUX (infrared leds to on) Gamma Correction

0.45 SNR  $\geq$  48dB (AGC OFF)

Electronic shutter Auto: PAL: 1 / 50 ~ 1 / 100, 000; NTSC 1 / 60 ~ 1 / 100, 000 sec;

Automatic Gain Control

Auto Backlight Compensation

Auto white balance

Video Output 1.0Vp-p

Operating temperature -10 °C ~ +50 °C

## Anexo 5



### **TBO-506\*\*\*\*IR**

#### **Features:**

- ◆ Board Lens 3.6mm/6mm
- ◆ IR LED:  $\Phi 5 \times 24$  pcs IR distance: 20m
- ◆ Dimension:  $\Phi 94 \times 65$  mm
- ◆ Weight (g): 165g

#### **Specification:**

Model: TBO-5062IR/ TBO-5063IR/ TBO-5064IR

1/4" SHARP/ 1/3" SONY CCD/ 1/3" SONY Super HAD CCD

Resolution 420 TVL /420 TVL /480TVL

Effective pixels; PAL: 500 (H) \* 582 (V) NTSC: 510 (H) \* 492 (V)

PAL: 752 (H) \* 582 (V) NTSC: 768 (H) \* 494 (V)

Minimum illumination: 0Lux (IR Leds On)

Gamma Correction: 0.45

SNR:  $\geq 48$  dB (AGC OFF)

Electronic shutter Auto: PAL: 1 / 50 ~ 1 / 100,000; NTSC 1 / 60 ~ 1 / 100,000 sec;

Automatic Gain Control

Auto Backlight Compensation

Auto White Balance

Video Output: 1.0Vp-p composite video, 75 $\Omega$

Power: DC12V