

**UNIVERSIDAD TÉCNICA DEL NORTE.**

**FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS.**

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE  
COMUNICACIÓN.**



**TEMA:**

**“DISEÑO DE UN SISTEMA DE VIDEO VIGILANCIA IP Y ALARMA BASADA EN  
MOVIMIENTO, UTILIZANDO SOFTWARE LIBRE SOBRE UN COMPUTADOR DE  
PLACA REDUCIDA, PARA LA EMPRESA COLOR 2000 DE LA CIUDAD DE  
IBARRA.”**

**TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN  
ELECTRÓNICA Y REDES DE COMUNICACIÓN.**

**AUTOR: CRISTIAN GERMAN CANACUAN IPIALES.**

**DIRECTOR: ING. OMAR OÑA**

**IBARRA 2018**

# AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

## 1.- IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto del repositorio digital institucional determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la universidad.

Por medio del presente documento dejo sentada mi voluntad de participaren este proyecto, para lo cual pongo a disposición la siguiente información.

Datos del contacto.	
Cedula de identidad.	100305984-5
Apellidos y nombres.	Cristian German Canacuan Ipiales.
Dirección.	Calle Principal SN – Barrio Olivo Alto.
Email.	<a href="mailto:crisfutnw3.a@gmail.com">crisfutnw3.a@gmail.com</a>
Teléfono.	0993699183 – 0991388775

Datos de la obra.	
Titulo.	“DISEÑO DE UN SISTEMA DE VIDEO VIGILANCIA IP Y ALARMA BASADA EN MOVIMIENTO, UTILIZANDO SOFTWARE LIBRE SOBRE UN COMPUTADOR DE PLACA REDUCIDA, PARA LA EMPRESA COLOR 2000 DE LA CIUDAD DE IBARRA.”
Autor.	Cristian German Canacuan Ipiales
Fecha.	Marzo 2018
Programa.	Pregrado
Titulo por el que opta.	Ingeniería en Electrónica y Redes de Comunicación
Director.	Ing. Omar Oña

## 2.- AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo Cristian German Canacuan Ipiales con C.I. 100305984-5 en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la biblioteca de la universidad con fines académicos. Para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión en concordancia con la Ley de Educación Superior, artículo 144.

## CONSTANCIA

Yo, CRISTIAN GERMAN CANACUAN IPIALES, manifiesto que la obra de la presente autorización es original y se desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que soy el titular de los derechos patrimoniales, por lo que asumo la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra. Abril 2018

EL AUTOR:



.....

Cristian Germán Canacúan Ipiales

CI: 100305984-5

# **CESIÓN DE DERECHO DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE**

Yo, Cristian Germán Canacúan Ipiales, con cedula de identidad Nro. 100305984-5, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículo 4,5 y 6 en calidad de autor del trabajo de grado denominado: “DISEÑO DE UN SISTEMA DE VIDEO VIGILANCIA IP Y ALARMA BASADA EN MOVIMIENTO, UTILIZANDO SOFTWARE LIBRE SOBRE UN COMPUTADOR DE PLACA REDUCIDA, PARA LA EMPRESA COLOR 2000 DE LA CIUDAD DE IBARRA.”, que ha sido desarrollado para optar por el título de: Ingeniería en Electrónica Y Redes de Comunicación, quedando la Universidad Técnica del norte facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi consideración de autor reservo los derechos morales de la obra antes citada.

En constancia suscribo este documento en el momento en que hago la entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.



Firma \_\_\_\_\_

Cristian Germán Canacúan Ipiales

CI: 100305984-5

Ibarra, abril 2018

## CERTIFICACIÓN

Certifico que el presente trabajo de titulación: “DISEÑO DE UN SISTEMA DE VIDEO VIGILANCIA IP Y ALARMA BASADA EN MOVIMIENTO, UTILIZANDO SOFTWARE LIBRE SOBRE UN COMPUTADOR DE PLACA REDUCIDA, PARA LA EMPRESA COLOR 2000 DE LA CIUDAD DE IBARRA.”, fue realizado en su totalidad por el Sr. Cristian German Canacuan Ipiales, bajo mi supervisión.



Ing. Omar Oña  
[oronia@utn.edu.ec](mailto:oronia@utn.edu.ec)

DIRECTOR DE TESIS.

## DECLARACIÓN DE AUTORÍA

Yo, Cristian Germán Canacúan Ipiales, con cedula de identidad Nro. 100305984-5, declaro bajo juramento que el trabajo aquí descrito es de mi autoría, y que este no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las Leyes de Propiedad Intelectual y normativa vigente de la Universidad Técnica del Norte.



Firma: \_\_\_\_\_

Cristian Germán Canacúan Ipiales

CI: 100305984-5

Autor.

## AGRADECIMIENTOS

*Agradezco a Dios por guiar mi camino de vida, a mi familia, sobre todo a mi padre y madre por enseñarme a seguir adelante aun cuando más difícil sea el camino, por brindarme su apoyo y confiar en mí, a mi esposa e hija por ser mi inspiración, a mis hermanos por sus consejos y compañía y a mis amigos que me apoyaron y fueron parte de mi desarrollo profesional.*

*Un agradecimiento especial al Ing. Omar Oña, por ser parte de este proyecto de titulación, por otro lado, agradezco sinceramente a todos mis maestros universitarios por brindarme las herramientas necesarias para desenvolverme en mi carrera profesional.*

*Cristian Germán Canacuan Ipiates.*



## DEDICATORIA

*El presente proyecto de titulación lo dedico a mi padre Germán Canacuán y a mi madre Mery Ipiales por su, esfuerzo y dedicación constante día a día, a mi amada esposa Wendy Lemos por su amor, cariño y apoyo incondicional y mi hija Abril Canacuán por ser el motivo de voluntad e inspiración en mi vida, a mis hermanos Jessica, Erick por su cariño y preocupación siendo ejemplo y guía en mi vida.*

*Cristian Germán Canacuan Ipiales.*

## RESUMEN

En el presente trabajo de grado se realizó el diseño de un sistema de video vigilancia IP y alarma basada en movimiento, utilizando software libre sobre un computador de placa reducida, para la empresa Almacén Color 2000 de la ciudad de Ibarra, con la finalidad de alertar sobre la presencia de intrusos en las áreas monitoreadas y mejorar la eficiencia del personal operativo, evitando exponer la integridad de las personas que acuden a esta empresa.

Se utilizó el método comparativo con sistemas propietarios similares para diseñar e identificar las principales características de este sistemas de video vigilancia IP y alarma, se determinó que requiere de aplicaciones como: captura de imágenes, detección de movimiento, alerta de la presencia de un intruso, la posibilidad de acceso local y remoto, adicionalmente se agregó características que los sistemas de video vigilancia convencionales no poseen como: control remoto de sistema de por medio de aplicaciones, notificación por medio de mensajes con Telegram.

Se seleccionó los dispositivos de hardware y herramientas de software libre para el computador de placa reducida Raspberry PI 3, las cuales permiten generar las características propias para cada aplicación tales como: cámara, dispositivo de almacenamiento, gestor de video, software Motion como gestor de cámaras, centralita de vos sobre IP Asterisk para el control por medio de un Softphone y vincular el Gateway de voz (teléfono celular) por medio de tecnología Bluetooth.

Se adaptó el sistema a las necesidades de la empresa las cuales fueron determinadas en una entrevista con el gerente de la empresa, posteriormente cubiertas mediante la creación de archivos intérpretes de comandos (scripts). El sistema es compatible con plataformas Windows y Linux y accesible desde la red local o remota.

## **ABSTRACT**

For this final degree work it was designed a system of video surveillance IP and alarm based on movement, using free software on a single board computer, for the company Warehouse Color 2000 of the city of Ibarra, with the purpose of alerting on the presence of intruders in the monitored areas and improve the efficiency of the operational personnel, avoiding exposing the integrity of the people who come to this company.

The comparison method with similar proprietary systems was used to design and identify the main characteristics of this IP video surveillance system and alarm, it was determined that it requires applications such as: image capture, motion detection, warning of the presence of an intruder, the possibility of local and remote access, additionally added features that conventional video surveillance systems do not possess such as: remote system control by means of applications, notification by means of Telegram messages.

For this degree work were chosen: hardware devices and free software tools for the single board computer Raspberry PI 3, which allow to generate the own characteristics for each application such as: camera, storage device, video software manager Motion as camera manager, Asterisk IP-based IP PBX for control by means of a Softphone and linking the voice gateway (cell phone) via Bluetooth technology.

The system was adapted to the needs of the company which were determined in an interview with the manager, later covered by the creation of command interpreter files (scripts). The system is compatible with Windows and Linux platforms and accessible from the local or remote network.

## **PRESENTACIÓN**

En este primer capítulo se realiza la explicación de la temática de este proyecto de titulación, los objetivos que se desea alcanzar, justificación y la debida delimitación del trabajo, en este capítulo se basa el desarrollo del proyecto.

En el segundo capítulo se presenta toda la investigación realizada acerca de los sistemas de video vigilancia, así como de la descripción de sus elementos, donde se detalla las diferentes tecnologías a usarse y alternativas basadas en optimización de recursos usando software libre.

En el tercer capítulo se desarrolla el diseño del sistema de video vigilancia y alarma basada en movimiento, para lo cual se ha considerado la infraestructura arquitectónica y tecnológica de la matriz de la empresa Color 2000, el diseño se contempla los requerimientos del gerente y normas correspondientes a los sistemas CCTV.

En el cuarto capítulo se realizó las pruebas de funcionamiento y corrección de errores a escala de laboratorio, para lograr funcionalidades óptimas en el diseño del sistema de video vigilancia y alarma basada en movimiento.

En el quinto capítulo se realizó un breve al Análisis Costo – Beneficio, que implica la realización de este proyecto.

En el sexto capítulo se exponen las conclusiones y recomendaciones obtenidas en el desarrollo del presente trabajo de titulación.

## ÍNDICE GENERAL

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE .....	ii
CONSTANCIA.....	iv
CESIÓN DE DERECHO DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE.....	v
CERTIFICACIÓN .....	vi
DECLARACIÓN DE AUTORÍA.....	vii
AGRADECIMIENTOS .....	viii
DEDICATORIA .....	ix
RESUMEN .....	x
ABSTRACT.....	xi
PRESENTACIÓN.....	xii
ÍNDICE GENERAL .....	xiii
ÍNDICE DE FIGURAS.....	xix
ÍNDICE DE TABLAS .....	xxiii
CAPÍTULO I .....	1
1. PRESENTACIÓN.....	1
Tema o título .....	1
Problema .....	1
Objetivos.....	2
1.3.1 Objetivo general.....	2
1.3.2 Objetivos específicos. ....	3
1.4 Alcance.....	3
1.5 Justificación.....	6
1.5.1 Justificación teórica.....	6
1.5.2 Justificación aplicativa. ....	7

CAPÍTULO II.....	9
2. MARCO TEÓRICO.....	9
2.1 Introducción general .....	9
2.2 Sistemas de video vigilancia.....	9
2.2.1 Sistemas de video vigilancia Analógicos.....	10
2.2.2 Sistemas de video vigilancia IP. ....	11
2.2.3 Sistemas de video vigilancia híbridos.....	12
2.2.4 Elementos y características de los sistemas de video vigilancia.....	13
2.2.4.1 Elementos de captación de Imagen (Cámaras). ....	13
2.2.4.2 Monitores. ....	20
2.2.4.3 Dispositivos de grabación. ....	21
2.2.4.4 Líneas de transmisión. ....	22
2.2.4.5 Accesibilidad remota. ....	23
2.2.4.6 Calidad de imagen.....	24
2.2.4.7 Gestión de eventos y videos inteligentes. ....	24
2.2.4.8 Escalabilidad y flexibilidad.....	25
2.2.5 Sistema de Alarma .....	25
2.2.5.1 Elementos de sistemas de alarma.....	26
2.3 Computadores de placa reducida .....	26
2.3.1 Raspberry Pi.....	27
2.3.2 Jaguarboard.....	27
2.3.3 ODroid. ....	27
2.3.4 CubieBoard. ....	28
2.3.5 Intel Galileo. ....	28
2.4 Software Libre .....	28
2.4.1 Características generales.....	29
2.4.2 Distribuciones de Linux.....	30

2.4.3 Administrador de procesos Cron. ....	32
2.4.4 Scripts en Linux. ....	32
2.4.5 Software libre para telefonía IP. ....	33
2.4.6 Software libre para gestión de cámaras. ....	36
2.5 Estándar IEEE 802.3 (Ethernet).....	37
2.5.1 Características de la tecnología Ethernet. ....	38
2.5.1.1 Ethernet elementos básicos. ....	38
2.6 Estándar IEEE 802.15 (Bluetooth) ....	39
2.7 Sistema Móvil Avanzado (SMA).....	40
2.7.1 Operadoras móviles en Ecuador. ....	40
2.7.2 Tecnologías del sistema móvil avanzado.....	41
2.8 Metodología .....	42
2.9 Modelo en V o de Cuatro Niveles.....	43
<b>CAPÍTULO III.....</b>	<b>45</b>
<b>3. DISEÑO DEL SISTEMA DE VIDEO VIGILANCIA Y ALARMA .....</b>	<b>45</b>
3.1 Situación actual.....	45
3.1.1 Análisis de Infraestructura en la empresa Color 2000. ....	48
3.1.2 Determinación de áreas a vigilar.....	48
3.1.3 Visualización y alertas del sistema. ....	50
3.1.4 Propósito del sistema. ....	50
3.1.5 Descripción general del sistema de seguridad. ....	50
3.1.5.1 Funciones del sistema. ....	52
3.1.5.2 Características del sistema. ....	52
3.2 Requerimientos .....	52
3.2.1 Requerimientos indirectos necesarios para el desarrollo del sistema. ....	53
3.2.2 Requerimientos iniciales del sistema. ....	54
3.2.3 Requerimientos iniciales de Arquitectura. ....	55

3.3 Selección de hardware y software para el sistema.....	57
3.3.1 Selección del computador de placa reducida .....	57
3.3.2 Selección de cámaras .....	59
3.3.3 Selección del HUB USB.....	61
3.3.4 Selección del Sistema Operativo. ....	62
3.3.5 Selección del software de gestión de cámaras. ....	64
3.3.6 Selección del software para telefonía IP.....	66
3.4 Diseño general del sistema.....	68
3.4.1 Diagrama de bloques.....	68
3.4.2 Diagrama de conexiones.....	70
3.4.3 Diagramas de flujo.....	71
3.4.4 Medios de transmisión .....	73
3.4.4.1 Cable USB .....	73
3.4.4.2 Cable de par trenzado.....	73
3.4.4.3 Transmisión inalámbrica.....	73
3.4.5 Dispositivo de almacenamiento del sistema .....	73
3.4.5.1 Dimensionamiento .....	73
3.4.5.2 Elección del dispositivo .....	75
3.4.6 Diseño de red para el sistema.....	75
3.4.6.1 Tabla de direccionamiento .....	75
3.5 Diseño del sistema de video vigilancia .....	76
3.5.1 Instalación del sistema operativo .....	76
3.5.1.1 Administración local .....	81
3.5.1.2 Administración remota.....	86
3.5.2 Instalación del software Motion.....	93
3.5.2.1 Configuración de ficheros individuales (Threads).....	99
3.5.2.2 Verificación de reconocimiento de cámaras web. ....	103



3.5.2.3 Montaje permanente del disco de almacenamiento externo. ....	105
3.5.3 Instalación del software Apache2 .....	107
3.5.3.1 Configuración de software .....	107
3.5.3.2 Programación de la interfaz web para el sistema.....	109
3.6 Diseño del sistema de alarma.....	110
3.6.1 Instalación de software Asterisk .....	110
3.6.1.1 Configuración de ficheros del software .....	114
3.6.2 Instalación del software Yowsup .....	118
3.6.3 Instalación del software Mutt.....	121
6.2.4 Instalación de Telegram con Python.....	123
3.6.5 Creación de Scripts para el control y alerta de eventos del sistema .....	126
3.6.5.1 Scripts para el control del sistema .....	127
3.6.5.2 scripts para alerta de eventos .....	129
3.7 Administración de tareas usando Cron .....	131
3.7.1 Herramienta Crontab.....	131
CAPÍTULO IV.....	133
4. PRUEBAS DE FUNCIONAMIENTO Y CORRECCIÓN DE ERRORES .....	133
4.1 Generalidades.....	133
4.2 Métodos de acceso para administración y configuración del sistema de video vigilancia. 134	
4.3 Comprobación del funcionamiento del software de gestión de cámaras. ....	135
4.4 Verificación de los modos de funcionamiento del sistema.....	137
4.4.1 Verificación del modo de Solo Monitoreo.....	137
4.4.2 Verificación del modo de Alarma y Monitoreo.....	139
4.4.3 Verificación de detección de movimiento y control de eventos. ....	140
4.4.3.1 Opciones de la llamada. ....	142
4.4.3.2 Recomendación de disponibilidad para la llamada telefónica. ....	143

4.5 Método de control local y remoto para el sistema de video vigilancia.....	145
CAPÍTULO V.....	147
5. ANÁLISIS COSTO-BENEFICIO .....	147
5.1 Introducción .....	147
5.2 Comparativa de elementos del sistema de video vigilancia.....	147
5.3 Determinación de los gastos a invertir .....	149
5.4 Determinación de los beneficios .....	150
5.4.1 Cálculo de beneficios.....	150
5.5 Periodo de recuperación.....	152
5.6 Beneficiarios del proyecto .....	153
5.6.1 Beneficiarios directos.....	153
5.6.2 Beneficiarios indirectos. ....	153
5.7 Impacto del proyecto.....	154
5.7.1 Impacto económico.....	154
5.7.2 Impacto social. ....	154
5.7.3 Impacto institucional.....	155
5.7.4 Impacto educativo.....	155
CAPÍTULO VI.....	156
6. CONCLUSIONES Y RECOMENDACIONES .....	156
6.1 Conclusiones .....	156
6.2 Recomendaciones .....	158
Bibliografía .....	160
Anexos .....	165
ANEXO 1.- Formulario de entrevista realizada a la Gerente Ing. Alicia Ramos.....	165
ANEXO 2.- GUÍA DE USO PARA EL SISTEMA .....	166
ANEXO 3.- GUÍA DE MANTENIMIENTO PARA EL SISTEMA .....	174
ANEXO 4.- GUÍA DE ADICIÓN DE DISPOSITIVOS (CÁMARAS) .....	177

ANEXO 5.- GUÍA DE USO Y REGISTRO DE USUARIO EN EL SOFTPHONE. ....	178
ANEXO 6.- CÓDIGO HTML DE LA PÁGINA WEB DE VISUALIZACIÓN. ....	180
ANEXO 7.- CARACTERÍSTICAS DE LAS CÁMARAS Y TELÉFONO MÓVIL USADOS EN EL SISTEMA. ....	187
ANEXO 8.- MANUAL DE PRUEBAS DE FUNCIONAMIENTO.....	189
ANEXO 9.- PLANOS DE INFRAESTRUCTURA Y DISEÑO DEL SISTEMA .....	194

## ÍNDICE DE FIGURAS.

Figura 1. Esquema de un sistema de CCTV analógico usando DVR de red. ....	11
Figura 2. Esquema básico de un sistema de video vigilancia IP. ....	11
Figura 3. Esquema básico de un sistema de video vigilancia Híbrido.....	12
Figura 4. Sensores CCD y sensores CMOS.....	14
Figura 5. Cámara web marca logitech. ....	17
Figura 6. Cámara IP Inalámbrica. ....	18
Figura 7. Cámara Analógica PTZ. ....	19
Figura 8. Monitor CCTV. ....	20
Figura 9. DVR.....	22
Figura 10. Esquema básico de un sistema de alarma. ....	25
Figura 11. Esquema básico de conexión Bluetooth. ....	39
Figura 12. Operadoras móviles en Ecuador. ....	40
Figura 13. Modelo en V para el desarrollo de Sistemas. ....	44
Figura 14. Entrada principal y salida del Almacén Color 2000.....	49
Figura 15. Área de atención al cliente y estanterías.....	49
Figura 16. Bodega del Almacén Color 2000. ....	50
Figura 17. Diagrama de bloques del sistema. ....	69

Figura 18. Diagrama de conexiones del sistema.....	70
Figura 19. Diagrama de flujo del sistema. ....	72
Figura 20. Página oficial de Raspberry Pi. ....	76
Figura 21. Descargas de Raspbian. ....	77
Figura 22. Selección de NOOBS OFFLINE.....	77
Figura 23. Interfaz de Win32 Disk Imager. ....	78
Figura 24. Interfaz de router huawei CNT.....	79
Figura 25. Interfaz de Putty. ....	79
Figura 26. Acceso SSH con Putty.....	80
Figura 27. Asistente de configuración Raspbian. ....	81
Figura 28. Instalacion de XRDP. ....	82
Figura 29. Interfaz de conexión a escritorio remoto en Windows. ....	83
Figura 30. Entorno grafico de Raspbian conexión desde Windows. ....	83
Figura 31. Instalacion de servidor VNC. ....	84
Figura 32. Interconexión desde Linux a Raspbian.....	85
Figura 33. Fichero rc.local. ....	85
Figura 34. Interfaz de registro en Weaved IoT. ....	87
Figura 35. Instalacion de kit Weaved IoT.....	88
Figura 36. Interfaz de Weaved en terminal.....	89
Figura 37. Registro de Nombre de dispositivo en Weaved. ....	89
Figura 38. Menú de activación de servicio en Weaved. ....	90
Figura 39. Menú de servicios por defecto en Weaved.....	90
Figura 40. Registro de un servicio en Weaved. ....	91
Figura 41. Servicios Activados en Weaved Iot.....	92
Figura 42. Vista de servicios desde la cuenta Weaved mediante navegador web. ....	92
Figura 43. Conexión mediante Weaved a escritorio remoto en Raspbian. ....	92
Figura 44. Interfaz gráfica de Raspbian mediante servicio de Weaved IoT.....	93

Figura 45. Configuración de interfaz wlan0 con IP estática. ....	94
Figura 46. Fichero motion.conf sección 1. ....	95
Figura 47. Fichero motion.conf sección 2. ....	96
Figura 48. Fichero motion.conf sección 3. ....	96
Figura 49. Fichero motion.conf sección 4-5-6. ....	97
Figura 50. Fichero motion.conf sección 7-8. ....	97
Figura 51. Fichero motion.conf sección 9-10. ....	98
Figura 52. Fichero motion.conf sección 11-12. ....	99
Figura 53. Fichero thread1.conf. ....	100
Figura 54. Fichero thread2.conf. ....	101
Figura 55. Fichero thread3.conf. ....	101
Figura 56. Fichero thread4.conf. ....	102
Figura 57. Fichero thread5.conf. ....	103
Figura 58. Detección de cámaras web y sus drivers. ....	104
Figura 59. Verificación de permisos de drivers. ....	104
Figura 60. Instalación de paquetes exfat. ....	105
Figura 61. Verificación de reconocimiento del disco externo. ....	105
Figura 62. Montaje permanente de disco externo en fichero fstab. ....	106
Figura 63. Acceso al fichero ports.conf. ....	107
Figura 64. Configuración del fichero ports.conf. ....	108
Figura 65. Configuración del fichero 000-default.conf. ....	108
Figura 66. Ficheros de página web en el directorio del servidor Apache2. ....	109
Figura 67. Interfaz de página web. ....	109
Figura 68. Descarga de software Asterisk 13. ....	111
Figura 69. Instalación de prerequisites para Asterisk 13. ....	111
Figura 70. Cargar ficheros de configuración de Asterisk 13. ....	112
Figura 71. Configurar menú de instalación de Asterisk 13. ....	112

Figura 72. Mensajes de Instalación completa de Asterisk 13.....	113
Figura 73. Asterisk 13 ejecutándose. ....	113
Figura 74. Fichero sip.conf. ....	114
Figura 75. Fichero users.conf.....	115
Figura 76. Fichero extensions.conf parte 1. ....	115
Figura 77. Fichero extensions.conf parte 2. ....	116
Figura 78. Fichero modules.conf. ....	116
Figura 79. Fichero chan_mobile.conf. ....	117
Figura 80. Direcciones MAC de dispositivos Bluetooth. ....	117
Figura 81. Modificación del fichero layer.py de Yowsup. ....	119
Figura 82. Actualización de versión WhatsApp en Yowsup. ....	120
Figura 83. Contraseña proporcionada por WhatsApp en Yowsup. ....	120
Figura 84. Fichero de configuración de cuenta Gmail en Mutt. ....	122
Figura 85. Clonación del repositorio para Telegram. ....	123
Figura 86. Registro en inicio en Telegram-cli. ....	124
Figura 87. Instalación de librería pexpect en Python.....	125
Figura 88. Guardado de Contactos en Telegram. ....	125
Figura 89. Envío de mensaje con Telegram.....	126
Figura 90. Script de control modoalarma.sh. ....	127
Figura 91. Scripts de activación y desactivación de la sirena.....	128
Figura 92. Script de recepción de mensajes WhatsApp.....	128
Figura 93. Script de control de alarma por WhatsApp. ....	129
Figura 94. Script disparo de evento. ....	130
Figura 95. Script generación de llamada.....	130
Figura 96. Script generación de sirena.....	130
Figura 97. Script de envío de correo y mensaje por Telegram. ....	131
Figura 98. Fichero crontan administración automática de procesos.....	132

Figura 99. Acceso al sistema desde red local. ....	134
Figura 100. Acceso al sistema desde Internet. ....	135
Figura 101. Estado de Motion y detección de cámaras. ....	136
Figura 102. Captura de video de cámaras. ....	137
Figura 103. Acceso a una cámara desde Internet. ....	138
Figura 104. Verificación del software de control Asterisk. ....	139
Figura 105. Verificación de esta del Gateway de voz en Asterisk. ....	140
Figura 106. Verificación de envío de correo. ....	141
Figura 107. Verificación de envío de Imágenes al correo. ....	141
Figura 108. Verificación de envío de mensaje por Telegram. ....	142
Figura 109. Ejecución de la llanada al gerente. ....	142
Figura 110. Plan CNT. ....	144
Figura 111. Plan Movistar. ....	144
Figura 112. Plan Tuenti. ....	145
Figura 112. Plan CLARO. ....	145
Figura 113. Verificación de control mediante Softphone Zoiper con cuenta SIP. ....	146
Figura 114. Verificación de control mediante Softphone Zoiper con cuenta IAX. ....	146

## ÍNDICE DE TABLAS

Tabla 1. Tabla de estándares de resolución de imagen. ....	15
Tabla 2. Características generales de un monitor. ....	20
Tabla 3. Características de los medios de transmisión usados en CCTV. ....	23
Tabla 4. Principales distribuciones de Linux. ....	30
Tabla 5. Método y formato para el levantamiento de información de la situación actual. ....	45
Tabla 6. Actores o Stakeholders que participan directamente en la investigación. ....	53

Tabla 7. Requerimientos de los usuarios. ....	53
Tabla 8. Requerimiento del sistema de videovigilancia. ....	54
Tabla 9. Requerimientos Funcionales de Hardware y Software a utilizarse .....	56
Tabla 10. Computadores de placa reducida. ....	57
Tabla 11. Elección del computador de placa reducida. ....	58
Tabla 12. Cámaras web.....	59
Tabla 13. Elección de cámara web. ....	60
Tabla 14. HUB USB. ....	61
Tabla 15. Elección del HUB USB. ....	62
Tabla 16. Sistemas operativos para Raspberry Pi.....	62
Tabla 17. Características de sistemas operativos para Raspberry.....	63
Tabla 18. Elección del Sistema operativo.....	64
Tabla 19. Características de softwares para gestión de cámaras. ....	65
Tabla 20. Elección del Software de gestión de cámaras. ....	66
Tabla 21. Características de software para telefonía IP.....	67
Tabla 22. Elección del Software para telefonía IP.....	68
Tabla 23. Consideraciones para el dimensionamiento del Disco Externo.....	74
Tabla 24. Almacenamiento por día.....	74
Tabla 25. Tabla de direccionamiento del sistema. ....	75
Tabla 26. Pasos para crear una cuenta en Weaved IoT.....	86
Tabla 27. Comparativa sistemas de video vigilancia analógicos vs prototipo del proyecto..	148
Tabla 28. Comparativa cámaras de sistemas de video vigilancia analógicos vs cámaras prototipo del proyecto. ....	149
Tabla 29. Análisis del costo. ....	150
Tabla 30. Análisis de beneficios. ....	151
Tabla 31. Periodo de recuperación del proyecto.....	152
Tabla 32. Indicadores de evaluación económica. ....	154



Tabla 33. Indicadores de evaluación en impacto social.....	154
Tabla 34. Indicadores de evaluación institucional. ....	155
Tabla 35. Indicadores de evaluación de impacto educativo. ....	155

# CAPÍTULO I

## 1. PRESENTACIÓN

### **Tema o título**

Diseño de un sistema de video vigilancia IP y alarma basada en movimiento, utilizando software libre sobre un computador de placa reducida, para la empresa Color 2000 de la ciudad de Ibarra.

### **Problema**

El Almacén Color 2000 dedica sus labores a la comercialización de pintura automotriz, arquitectónica y metalmecánica, preparación de colores y venta de complementarios, la fortaleza de este negocio es la experiencia de más de diez años en el mercado y su amplia línea automotriz, los cuales son elementos que diferencian a esta empresa frente a la competencia. Cuenta con su matriz ubicada en el la Av. Jaime Rivadeneira Frente al Coliseo Luis Leoro Franco y su sucursal en la Av. Teodoro Gómez 15-18 y Gral. Julio Enríquez.

El Almacén Color 2000 en su infraestructura de comunicaciones no cuenta con un sistema de video vigilancia y alarma en ninguna de sus dependencias, actualmente posee el servicio de internet residencial contratado con CNT EP tanto en su matriz como en la sucursal. La ausencia de un sistema de video vigilancia en el almacén ocasiona inseguridad hacia sus clientes, empleados y empresa como tal, el problema radica en la falta de monitoreo remoto y local de eventos ocurridos en sus instalaciones a tiempo real.

Las funciones que desempeña la gerencia del Almacén no permiten dirigir de forma interactiva y a tiempo completo las actividades que se desarrollan en la empresa tales como monitorear el cumplimiento de tareas asignadas a empleados, control de inventarios, monitoreo de ventas y otros elementos. Muchas veces existen pérdidas internas o el personal no cumple a cabalidad las tareas asignadas en el trabajo.

El Almacén Color 2000 es visitado diariamente cientos de clientes, la afluencia en la matriz de la empresa ocasiona que las actividades se centren en la atención al cliente. En estas circunstancias la gerencia indica que es donde se generan robos de productos y pérdidas de materiales por descuido de los trabajadores. La gerencia menciona además que muchas de las tareas asignadas a los empleados no se cumplen a tiempo generando retrasos y pérdidas.

El registrar eventos ocurridos en el Almacén Color 2000 y almacenarlos por medio de video e imágenes obtenidos con tecnología que utiliza software libre da origen a un sistema de video vigilancia escalable, flexible y robusto el cual permitirá el monitoreo remoto y local. El uso e implementación de estos sistemas de video vigilancia en la sociedad actual permiten salvaguardar la integridad de las personas y empresas manteniéndolas vigiladas y a su vez generando un ambiente de confort y seguridad, de manera sencilla, inmediata e inclusive con la posibilidad de tener al alcance de la pantalla de un teléfono móvil.

## **Objetivos**

### **1.3.1 Objetivo general.**

Diseñar un sistema de video vigilancia IP y alarma basada en movimiento, utilizando software libre sobre Raspberry PI, para la seguridad de la empresa Color 2000.

### **1.3.2 Objetivos específicos.**

- Estudiar los sistemas y tecnologías que se utilizan en video vigilancia y alarmas los cuales permitan: escalabilidad y accesibilidad para un diseño de sistema de video vigilancia basado en software libre.
- Analizar los dispositivos y softwares que intervienen en un sistema de video vigilancia IP y alarma, utilizando software libre y computadores de placa reducida.
- Diseñar el sistema de video vigilancia y alarma basándose en los requerimientos de la gerencia e infraestructura de la empresa Almacén Color 2000.
- Realizar pruebas de funcionamiento a escala de laboratorio para corregir errores del sistema.
- Elaborar una guía de uso y mantenimiento del sistema de video vigilancia y alarma.

## **1.4 Alcance**

Para el diseño del sistema de video vigilancia y alarma se tomará como base los requerimientos de la gerencia los cuales indiquen las áreas a vigilar en la infraestructura del Almacén Color 2000 la cual permitirá el diseño acorde a las necesidades específicas de esta empresa. Enfocándose en la matriz, se realizará el diseño del prototipo y de dimensionamiento del espacio necesario para almacenar el video e imágenes.

Se realizará un estudio de los componentes a utilizarse en el sistema de video vigilancia y alarma, tales como cámaras web, cámaras de video vigilancia cableadas e inalámbricas, computadores de placa reducida, dispositivos de almacenamiento y software de código abierto. Mediante estos elementos se realizará el proceso de diseño del prototipo de sistema.

Se instalará el sistema operativo Raspbian en el computador de placa reducida, se configurará una dirección de red estática y archivos para acceso hacia el escritorio remoto, posteriormente se instalarán el software Motion el cual controlará las cámaras y detectará el movimiento en horarios los cuales se programarán y Asterisk controlará las llamadas a la gerencia o autoridades frente a la detección de una irregularidad.

Se realizará un análisis para determinar la resolución y tipo de cámaras necesarias para este sistema, se considerará dos tipos; cámaras USB<sup>1</sup> y cámaras IP<sup>2</sup>. En el análisis se debe considerar el ambiente y espacio que cubrirá la cámara para determinar el tipo a usar. Se considerará factores como luminosidad, área e importancia del ambiente a cubrir.

El software Motion gestionará las cámaras haciendo que estas actúen como un sensor de movimiento además de cumplir con su función de captura de video, se configurará este software para actuar frente a la detección de un movimiento y considerarlo como un evento que estará sujeto a dos modos de funcionamiento del sistema, el modo de Solo monitoreo y modo Monitoreo y alarma.

El sistema de video vigilancia y alarma tendrá dos modos de funcionamiento, el primer modo de Solo monitoreo incluyen la función de video vigilancia y control del sistema dentro de los horarios de atención en la empresa, para lo cual se desarrollará una interfaz web que permitirá la visualización y gestión de las cámaras, el gerente también podrá visualizar la transmisión en video de las actividades en la empresa desde su teléfono móvil o tableta mediante una aplicación en donde podrá gestionar el sistema remotamente.

En el segundo modo de funcionamiento del sistema de Monitoreo y Alarma el cual actuará en los horarios de no atención de la empresa el sistema monitorizará mediante las

---

<sup>1</sup> USB: Bus de conexión Universal (Universal serial bus).

<sup>2</sup> IP: Protocolo de Internet (Internet Protocol).

cámaras activando la detección de movimiento. En este caso el gerente podrá visualizar mediante la interfaz web remotamente o por la aplicación instalada en su teléfono móvil o tableta lo que estará ocurriendo en las instalaciones de la empresa a tiempo real y controlar el sistema.

Los eventos a controlarse serán la detección de intrusos en las áreas de monitoreo, el cual si ocurre en el primer modo de funcionamiento no generará una alarma, pero guardará el video en el disco de almacenamiento masivo. Si el evento se detecta el segundo modo de funcionamiento este generará una alarma y se notificará al gerente de la intrusión a través de una llamada la cual será gestionada por el software Asterisk.

El software Asterisk realizará la llamada al usuario mediante el módulo chan\_mobile que permite conectar mediante Bluetooth un teléfono celular al sistema y usarlo como Gateway para acceder a la red de servicio móvil, se configurará en este software las opciones para actuar frente a la alerta, se considerará casos de falsos positivos y de acción inmediata como llamar al a las autoridades o disparar la sirena. En caso de que el usuario no conteste se realizarán las opciones programadas que se decidirá con el gerente.

El registro de los eventos detectados por las cámaras de seguridad se guardará en formato de imágenes y video en el disco de almacenamiento del sistema, adicionalmente se generará un respaldo el cual será enviado al espacio personal de almacenamiento en la nube del gerente. El gerente será capaz de visualizar este respaldo y manipular el espacio de almacenamiento del sistema para mantenerlo siempre disponible.

Se realizarán pruebas de funcionamiento a escala de laboratorio, con las cuales se pretende corregir posibles errores y calibrar el funcionamiento del sistema, se efectuarán pruebas de conexión, funcionalidad y monitoreo. Posteriormente se realizará un manual de uso y mantenimiento para la correcta dirección del sistema.

## **1.5 Justificación**

### **1.5.1 Justificación teórica.**

Un sistema de video vigilancia IP al igual que muchos tipos de sistemas de comunicación se realizan a través de internet y redes de acceso. Sean estas redes de acceso cableadas o inalámbricas dan origen a muchos beneficios sobre los sistemas de CCTV (Circuito Cerrado de Televisión) tradicionales, permitiendo la monitorización del sistema remotamente y a tiempo real, integrando funciones de almacenamiento y gestión.

El contar con un sistema para la vigilancia del delito y la atención de emergencias constituye un logro importante para el país. En el 2013, el Sistema Integrado de Seguridad ECU 911 atendió a nivel nacional 1.573.876 emergencias, 634. 511 fueron claves rojas, de las cuales se salvaron 4.858 vidas. Los incidentes atendidos durante el año crecieron en todo el territorio ecuatoriano, pues pasaron de 125.589 en enero a 157.913 en noviembre. (Plan Nacional de Seguridad Integral, 2014)

El crecimiento de las de sectores comerciales en donde funcionan micro, pequeñas y medianas empresas, involucra la utilización de tecnologías enfocándose a la seguridad y vigilancia. El desarrollo de nuevos sistemas que cumplan con características únicas involucra la investigación y uso de software libre dirigidos al diseño de una solución.

Este proyecto pretende cubrir las necesidades de seguridad de la empresa Almacén Color 2000 con un sistema de bajo costo, utilizando software libre, plataformas de telefonía móvil e internet las cuales harán al sistema amigable, eficiente y seguro de esta forma el sistema responderá a los distintos eventos y necesidades en casos de emergencia, mediante la integración de video vigilancia y alarma.

### **1.5.2 Justificación aplicativa.**

El sistema de video vigilancia y alarma con funcionalidades IP, utilizando software libre sobre un computador de placa reducida, es una alternativa al sistema tradicional, que permitirá optimizar recursos de hardware y software, al utilizar redes existentes como internet y la red de servicio móvil avanzado (SMA<sup>3</sup>).

Este proyecto se pretende disminuir las debilidades existentes por la ausencia de un sistema de video vigilancia y alarma, ya sea por el alto costo de los equipos, por la complejidad de su funcionamiento, o porque en gran parte este tipo de soluciones se distribuyen bajo licencias propietarias y de manera individual.

Este sistema a diferencia de los sistemas de video vigilancia convencionales permite el funcionamiento de alarma en mismo hardware, ahorrando recursos y optimizando funciones. Podrá controlar y registrar los eventos de forma remota. Simplificando el uso del sistema y con costes económicos más bajos a los sistemas convencionales.

La seguridad es tarea de todos y los sistemas integrados de video vigilancia como el ECU 911 ayudan a disminuir índices delictivos en porcentajes aproximados a 20%. A esto, se suman los esfuerzos de implementar nuevas tecnologías e impulsar la investigación, de modo tal que los procesos internos y servicios sean constantemente actualizados para cumplir de forma eficiente sus funciones. (Plan de Nacional Seguridad integral, 2014) El diseño de este sistema pretende brindar ventajas y optimizar las funciones de las actividades que se realizan en la empresa.

El sistema de video vigilancia IP constará de un gestor de vídeo, cámaras y sistema de almacenamiento, cuyo contenido puede observarse desde un monitor, televisor y dispositivos

---

<sup>3</sup> SMA: Servicio Móvil Avanzado (Service Mobile Advanced).



que se encuentren dentro y fuera de la red. Mientras que un sistema de alarma consta de una unidad de control de alarma, sirena y un sensor.

El proyecto utilizará software libre para integrar varios dispositivos tales como cámaras web y una Raspberry Pi para construir un sistema integrado de video vigilancia y alarma IP, mediante la unificación con un gestor de video, la unidad de control de alarma, y las cámaras como los sensores de movimiento, adicionalmente la red celular permitirá alertar la detección de un intruso al gerente, mientras que internet permitirá la administración, almacenamiento y notificación del funcionamiento del sistema, además un teléfono móvil podrá activar y desactivar el sistema de alarma.

## **CAPÍTULO II**

### **2. MARCO TEÓRICO**

#### **2.1 Introducción general**

Los sistemas de video vigilancia con en pasar del tiempo se han convertido en una herramienta esencial para la seguridad del hogar y de las empresas, debido a la necesidad de las personas en mantener monitoreados espacios como tiendas, locales comerciales, supermercados, empresas, bancos y otros sitios para esto se han desarrollado una variedad de soluciones específicas de acuerdo a los requerimientos de cada entidad. A esto se suma el uso de nuevas tecnologías basadas en software libre para desarrollar sistemas de video vigilancia alternativos con funcionalidades dedicadas a entidades que requieren de estos sistemas, cada uno con infraestructuras y necesidades diferentes.

Los sistemas de video vigilancia en la actualidad permiten salvaguardar la integridad de las personas y bienes de la empresa además de obtener una transmisión de video a tiempo real de lo que ocurre en en el espacio monitoreado, son beneficios que proporcionan estos sistemas para crear ambientes de confort y seguridad

#### **2.2 Sistemas de video vigilancia**

Los sistemas de video vigilancia son un conjunto de dispositivos que brindan al usuario numerosas posibilidades que le permiten solventar sus necesidades de una forma eficiente y eficaz, gestionando las cámaras para la monitorización de un sitio sea de manera local o remota.

Los sistemas de video vigilancia conocidos como sistemas CCTV en donde las siglas vienen del inglés “Closed Circuit Television” que traducido conocemos como “Circuito Cerrado de Televisión”. El objetivo de este sistema es la supervisión, el control y el eventual registro de la actividad física dentro de un local, espacio o ambiente en general. Se denomina circuito cerrado porque, a diferencia de la televisión tradicional, este solo permite un acceso limitado y restringido del contenido de las imágenes a algunos usuarios. (Mata, 2011)

Estos sistemas por la tecnología que usan se pueden clasificar de la forma siguiente:

### **2.2.1 Sistemas de video vigilancia Analógicos.**

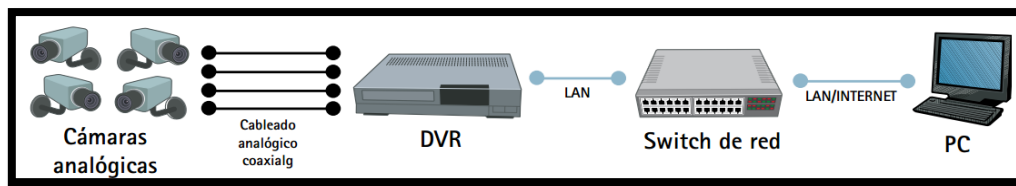
Los sistemas de video vigilancia analógicos son una solución estándar la cual consta de grabación de video en un circuito cerrado, estos sistemas se componen de dispositivos tales como monitores, grabadores, cámaras analógicas y otros dispositivos analógicos.

Estos sistemas han sido los más usados durante las décadas pasadas a medida que los DVR<sup>4</sup> evolucionaron, contando finalmente con un puerto Ethernet para su conexión a redes IP. Esto, con el tiempo, es lo que se denominó DVR de red y permitió la monitorización remota a través de PC's. Algunos sistemas DVR que se usan todavía actualmente permiten la monitorización simultánea de video en tiempo real y vídeo grabado, mediante que otros sistemas sólo permiten la monitorización de vídeo grabado. Algunos sistemas necesitan aplicaciones especiales en el cliente para poder monitorizar la imagen, mientras a otros les basta con un navegador web estándar. (Mata, 2011)

El esquema presentado en la figura 1 muestra un ejemplo de un sistema de video vigilancia analógico y sus elementos básicos.

---

<sup>4</sup> DVR: Grabador de vídeo digital (Digital Video Recorder).



**Figura 1. Esquema de un sistema de CCTV analógico usando DVR de red.**

*Fuente: Mata, (2012).*

### 2.2.2 Sistemas de video vigilancia IP.

En los últimos años la tecnología de video vigilancia ha sufrido una revolución como consecuencia de la aplicación de la tecnología IP en el sector. El video IP o video vigilancia IP, al igual que muchos otros tipos de comunicaciones como son el correo electrónico, los servidores Web o la telefonía IP, se realizan a través de redes, ya sean cableadas o inalámbricas. Todo el flujo de audio/video se efectúa a través de la misma infraestructura de red común, lo cual conlleva multitud de ventajas sobre los sistemas de CCTV tradicionales. Adicionalmente, la red IP se usa para ofrecer alimentación eléctrica a determinados dispositivos (por ejemplo, cámaras de red) mediante el uso de la tecnología PoE<sup>5</sup> (Power over Ethernet). (Mata, 2011)

En la figura 2 se muestra un ejemplo de la arquitectura básica de un sistema de video vigilancia IP.



**Figura 2. Esquema básico de un sistema de video vigilancia IP.**

*Fuente: Scurity central services. (2008). Recuperado de: [http://securitycentralservices.com/Imagenes/cctv%20\(1\).jpg](http://securitycentralservices.com/Imagenes/cctv%20(1).jpg) (Grafico)*

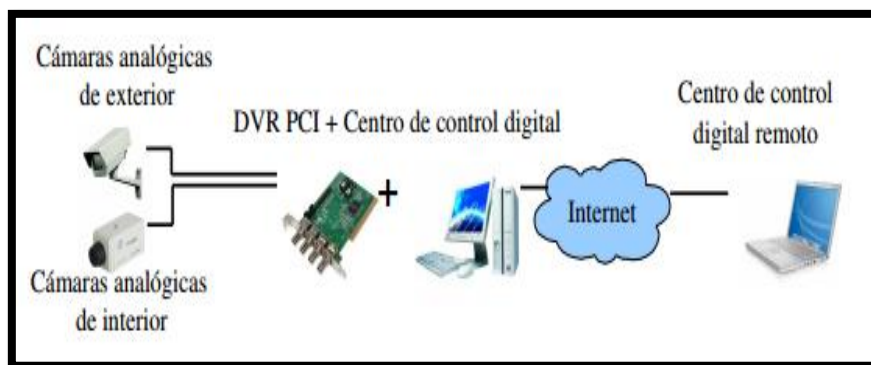
<sup>5</sup> PoE: Alimentación a través de Ethernet (Power over Ethernet).

Un sistema de video IP permite supervisar vídeo y grabarlo desde cualquier lugar de la red, tanto si se trata por ejemplo de una red de área local (LAN) o de una red de área extensa (WAN) como Internet. Esto permite una monitorización remota en tiempo real, centralizado las labores de monitorización, almacenamiento diferente al del espacio monitorizado. (Mata, 2011)

### 2.2.3 Sistemas de video vigilancia híbridos.

Un sistema de video vigilancia híbrido contiene la mayoría de elementos que caracterizan a los sistemas de video vigilancia analógicos excepto el centro de control, que será un computador, obteniendo como resultado la posibilidad de acceder a las imágenes mediante un gestor web, a este computador se le puede instalar tarjetas PCI<sup>6</sup> comúnmente llamadas tarjetas DVR que actúa como un servidor de vídeo. Estas tarjetas cuentan con un número determinado de puertos BNC<sup>7</sup> a los que se conectan las cámaras analógicas. Las cámaras de vigilancia de red se integran a sistema mediante la conexión al cableado de la red área local.

El esquema básico de este sistema se muestra en la figura 3:



**Figura 3. Esquema básico de un sistema de video vigilancia Híbrido.**

*Fuente: Muñoz, H. (2007). Sistema de Video vigilancia Híbrido. p 7.*

<sup>6</sup> PCI: Interconexión de Componentes Periféricos (Peripheral Component Interconnect).

<sup>7</sup> BNC: Conector de cable coaxial tipo C (Bayonet Neill-Concelman)

## **2.2.4 Elementos y características de los sistemas de video vigilancia**

Entre los elementos principales de los sistemas de video vigilancia están los captadores de imagen a estos se les denomina cámaras de vigilancia, los elementos reproductores de imagen que son los monitores, elementos de grabación de imagen, elementos transmisores de la señal de video y otros elementos que se detallan a continuación.

### **2.2.4.1 Elementos de captación de Imagen (Cámaras).**

Una cámara es un dispositivo encargado de capturar las imágenes de una zona hacia la que ha sido orientada, convirtiéndolas en una señal eléctrica de video que transmite al resto de componentes de la instalación. Se trata, sin lugar a dudas, del equipo electrónico más importante y determinante de los sistemas de Circuito Cerrado de Televisión. (Fernández, 2013)

Los elementos que conforman este equipo y hacen notable sus propiedades y funcionamiento son:

- Dimensiones y peso.

Las cámaras ofertadas en el mercado actual tienen una variedad considerablemente alta y múltiples opciones en cuanto a tamaño se refiere, cabe destacar que las dimensiones de la cámara van acorde al fin de su uso en la implementación de un sistema de video vigilancia.

- Tipo y tamaño del sensor.

Gracias a los sensores los cuales son dispositivos compuestos por celdas microscópicas que mediante sus propiedades fotosensibles y conductoras son capaces de distinguir los colores de la imagen y mediante filtros dividen los colores de la imagen permitiendo reproducirlos posteriormente.

El sensor de tipo CCD<sup>8</sup> es el más estandarizado y utilizado en la actualidad. En sistemas de seguridad y video vigilancia con cámaras analógicas en donde se emplean sensores CCD de 1/3" (Con un ángulo de visión muy elevado) y CCD de 1/4" (más económico y con menor ángulo de visión).

El sensor CMOS<sup>9</sup> se utiliza generalmente en web-cams y cámaras IP. Una ventaja de los sensores CMOS frente a los sensores CCD es su bajo consumo energético y su tamaño más reducido. (Fernández, 2013)



**Figura 4. Sensores CCD y sensores CMOS.**

*Fuente: Blog Tecnosinergia. (2011). Recuperado de:*

*<https://tecnosinergiamx.files.wordpress.com/2011/07/ccd-vs-cmos-fact-and-fiction1.jpg> (Grafico)*

- Tipo de objetivo y lente.

Un objetivo está formado por uno o varios grupos de lentes, cuya finalidad es reproducir sobre el dispositivo de captación la imagen situada frente a la cámara. Es elemento ´por tanto está situado en la parte frontal de la cámara permitiendo variar el formato y las dimensiones del área de cobertura de la imagen. (Fernández, 2013)

<sup>8</sup> CCD: Dispositivo de carga acoplada (Charge-coupled device).

<sup>9</sup> CMOS: Semiconductor complementario de óxido metálico (Complementary metal-oxide-semiconductor).

- Resolución.

La resolución de imágenes se presenta en dos formas digital y analógica, estas tienen una gran similitud, pero diferencias muy importantes en su definición. En el video analógico, una imagen consta de líneas o líneas TV. En un sistema digital una imagen está formada por píxeles cuadrados. (Vargas, 2015, pág. 22)

Existen muchos estándares para la resolución de imágenes, de los cuales los más notables se detallan en la tabla 1 a continuación:

**Tabla 1. Tabla de estándares de resolución de imagen.**

<b>Analógicos</b>	<b>Digitales</b>
<b>NTSC</b>	<b>VGA</b>
<b>PAL</b>	<b>MEGAPIXEL</b>

**Fuente:** (Vargas, 2015, pág. 22)

- Sensibilidad.

Proporciona la capacidad de reproducción de imágenes de video en condiciones de baja iluminación. Es la cantidad de iluminación mínima de una escena para obtener la señal de video. La sensibilidad se mide en LUX<sup>10</sup>. Las cámaras a blanco y negro tienen en general una sensibilidad de 0,01 LUX. En cambio, las cámaras color tienen una sensibilidad aproximada de 0,1 a 1 LUX. (Junghanss, 2012)

<sup>10</sup> LUX: Unidad de intensidad de iluminación del Sistema Internacional.



Debemos considerar en el área a ser vigilada, factores de incidencia como la luz en el área tanto en día como en la noche, esto debemos tomarlo en cuenta en el momento de realizar un diseño de sistema de video vigilancia y realizar la selección de la cámara según las condiciones del área a vigilar. Este tema de la luz a veces no es tomado tan una cuenta como debería por los instaladores de sistemas y sin embargo es una de las primeras cosas que hay que evaluar, no hay que olvidarse la similitud de la cámara al ojo humano, ya que sin luz el ser humano no ve nada. En un lugar pobremente iluminado, y con una cámara con sensibilidad convencional se obtendrá una imagen oscura y turbia que seguramente impedirá el correcto monitoreo y bajará la calidad de imágenes adquiridas por el sistema, detalle que disgustará al cliente. (Ganchala, 2011)

- Cámaras de uso en video vigilancia.

La selección de una cámara depende de cual se acople mejor a la necesidad que se tenga. Algunas de las más útiles y de mayor aplicación son: cámaras analógicas (conexión BNC), cámaras IP y las conocidas webcams. A continuación, se describen estos tres tipos, sus principales características y usos.

#### Webcams

Las cámaras web “webcams”, como son conocidas en inglés, son dispositivos conectados a un ordenador mediante una interfaz USB u otra semejante. El funcionamiento de estos equipos se basa en la codificación de los videos, o imágenes digitales, para su posterior envío mediante Internet. Sus principales funciones se dan en la visualización en tiempo real de video, en aplicaciones de mensajería instantánea, así como en actividades de vigilancia últimamente. El funcionamiento de estas cámaras es sencillo. La luz de la imagen que será procesada, pasa por una lente y se refleja en un filtro RGB (rojo-verde-azul por sus siglas en ingles), dando así lugar a una descomposición de los tres colores básicos antes mencionados.

Esta división de colores se concentra en un sensor de luz, ya sea del tipo CCD o CMOS, que asignan valores binarios (1-0) a los píxeles que serán enviados para su respectiva codificación de video. Finalmente son comprimidos, para luego compartirlos por Internet. (Betancourt, 2013)

Podemos observar en la figura 5 la ilustración de una cámara web de alta resolución normalmente ofertada en el mercado.



**Figura 5. Cámara web marca logitech.**

**Fuente:** Logitech. (2016). HD PRO WEBCAM C920. Recuperado de: <http://www.logitech.com/es-es/product/hd-pro-webcam-c920?crd=34>. (Grafico)

## Cámaras IP

Las cámaras IP o también conocidas como cámaras de red, son dispositivos diseñados para el envío de información mediante internet. Las señales enviadas corresponden a video y audio que, desde un explorador o un módulo concentrador (como hubs o switches), son insertadas en una red para su utilización. Este tipo de cámaras suelen integrar sistemas embebidos con funciones como: detección de movimiento, identificación de rostros, notificaciones mediante email o SMS, entre otras. Las anteriores características vuelven a estos dispositivos la principal competencia de las aplicaciones de video vigilancia de bajo costo.

Algunas de las ventajas de estos dispositivos son: capacidad de acceso a sus capturas mediante una conexión a internet, posibilidad de múltiples usuarios accediendo a dichas capturas simultáneamente, capacidad de visión nocturna (en la mayoría de casos), transmisión de audio, posibilidad de PT<sup>11</sup> (pan/tilt) o PTZ<sup>12</sup> (pan/tilt/zoom) y control del sistema de manera remota. Entre las principales desventajas están: los altos precios (en busca de productos de gran calidad y buen respaldo), así como la dependencia de dos elementos propensos a fallos en un sistema de seguridad, como lo son: el suministro eléctrico y la estabilidad de conexión. (Betancourt, 2013)

La Figura 6 muestra una cámara IP con algunas características señaladas.



**Figura 6. Cámara IP Inalámbrica.**

*Fuente: ForoCoches. (2016). Recuperado de:*

*[http://img.auctiva.com/imgdata/1/4/2/9/7/0/2/webimg/480596802\\_o.jpg?nc=80](http://img.auctiva.com/imgdata/1/4/2/9/7/0/2/webimg/480596802_o.jpg?nc=80). (Grafico)*

### Cámara analógica

Estas cámaras son las más comunes para aplicaciones de video vigilancia y su funcionamiento es básico. Por otra parte, la asociación de la imagen capturada, ya sea imagen

<sup>11</sup> PT: Función de cámara de seguridad de rotación en plano vertical y horizontal. (pan - tilt).

<sup>12</sup> PTZ: Función de cámara de seguridad de rotación en plano vertical y horizontal con zoom. (pan -tilt-zoom).

a color o escala de grises, a una señal eléctrica continua en el tiempo, es la razón de que se les catalogue como analógicas. La calidad en la señal en este tipo de sistemas, se limita principalmente por las distancias de trabajo debido al medio físico por el cual se transmite. El cable coaxial, por ejemplo, cuenta con un nivel de resistencia que es de suma importancia en las aplicaciones analógicas. Con base en lo anterior, se deben seleccionar adecuadamente los tipos de cables para permitir aumentar la distancia de transmisión.

Las cámaras analógicas como la que se muestra en la figura 7, a diferencia de las digitales, basan su resolución en líneas de televisión. A continuación, se muestra la escala que caracteriza la calidad de la resolución, según la cantidad de líneas de televisión (TVL<sup>13</sup>). (Betancourt, 2013)

- Calidad de imagen estándar: 380 TVL a 420 TVL.
- Alta calidad de imagen: 480 TVL.
- Muy alta calidad de imagen: 540 TVL a 700 TVL



**Figura 7. Cámara Analógica PTZ.**

*Fuente: Techresources. (2016). Recuperado de:  
<http://recursos-tecnologicos.com/hd-turbo-1080p/172-camara-turbo-hd-1080p-tubo-ir-40m-hikvision.html>.  
(Grafico)*

---

<sup>13</sup> TVL: Medida de resolución en cámaras analógicas líneas de televisión. (TV-Line).

### 2.2.4.2 Monitores.

Las imágenes captadas por la cámara y transformadas en señales eléctricas de vídeo necesitan ser reproducidas en un dispositivo que tenga la capacidad de visualización, para lograr el monitoreo y supervisión estas deben ser interpretadas y controladas por personal competente. Un monitor como el que se muestra en la figura 8 tiene la capacidad de traducir las señales eléctricas de vídeo y volverlas a convertir a imagen.



**Figura 8. Monitor CCTV.**

*Fuente: Equipos y redes. (2016). Monitor. Recuperado de: [http://www.equiposyredes.com/uploads/1/2/9/1/12913156/4327266\\_orig.jpeg?390](http://www.equiposyredes.com/uploads/1/2/9/1/12913156/4327266_orig.jpeg?390). (Grafico)*

Entre las características más importantes de un monitor de vídeo tenemos las presentadas en la tabla 2.

**Tabla 2. Características generales de un monitor.**

<b>Características de un Monitor</b>	<b>Descripción</b>
<b>Tamaño</b>	Indica la longitud en pulgadas de la pantalla.
<b>Resolución y Brillo</b>	Indica el número de píxeles que puede representarse de forma horizontal y vertical en la pantalla y el brillo indica el nivel de iluminación.

---

<b>E/S</b>	Indica el número de entradas y salidas de la señal de video que posee.
<b>Frecuencia de refresco</b>	Indica el número de fotogramas que puedes reproducir por segundo.
<b>Tipo de conexión de las entradas</b>	Indica si provee de conexión directa con las cámaras (BNC) o tiene conexión para ordenador o grabador (VGA-HDMI).
<b>Capacidad de reproducción de audio</b>	Indica si puede reproducir audio en los posibles formatos compatibles.
<b>Tensión e intensidad de funcionamiento</b>	Valores de funcionamiento del equipo expresado en voltios (V) y amperios (A) respectivamente.
<b>Potencia de consumo</b>	Relacionado con la energía eléctrica que demandara. Se expresa en vatios (W).

---

Fuente: (Fernández, 2013, págs. 166-167)

#### **2.2.4.3 Dispositivos de grabación.**

Estos dispositivos permiten almacenar digitalmente las imágenes de video generadas por las cámaras para su posterior revisión, de esta forma se respalda y controla eventos y

sucesos producidos durante la ausencia del responsable del monitoreo. En la figura 9 se muestra un DVR (Grabador de disco digital) como ejemplo de los dispositivos de grabación digitales.

Los Grabadores de vídeo digital en red conocidos NVR <sup>14</sup> y los DVR tienen características similares, como lo son dimensiones y peso, capacidad del disco de almacenamiento, número de canales, formato de codificación de la información de vídeo, formato de compresión de la información de vídeo, niveles de calidad de grabación de video, formato de compresión de audio, velocidad de la actualización de grabación, resolución de grabación admitida, posibilidades de en red TCP/IP, modos de grabación y posibilidad de conexión con otros componentes como micrófono, altavoces, ratón, dispositivos de control PTZ<sup>15</sup>, alarmas, etcétera.



**Figura 9. DVR**

*Fuente: Equipos y redes. (2016). DVR. Recuperado de:  
<http://www.equipoysredes.com/uploads/1/2/9/1/12913156/3077199.jpeg?213>*

#### **2.2.4.4 Líneas de transmisión.**

Es el medio físico por el cual se transmite la señal eléctrica de vídeo, este medio puede constar de componentes que ayuden a la transmisión de la señal como amplificadores y

---

<sup>14</sup> NVR: Grabador de Video de Red (Network Video Recorder).

<sup>15</sup> PTZ: Paneo, inclinación y ampliación (Pan, Tilt and Zoom).

distribuidores. Estos medios de transmisión pueden ser cableados (mediante par trenzado, cable coaxial o fibra óptica) o inalámbricos utilizando ondas electromagnéticas de radiofrecuencia o tecnología Wi-Fi. (Fernández, 2013, pág. 159)

**Tabla 3. Características de los medios de transmisión usados en CCTV.**

<b>Medios de transmisión</b>	<b>Tipos</b>	<b>Características</b>
<b>Cableados</b>	Cable coaxial	Composición interna muy resistente, resistente a las interferencias.
	Cables de pares trenzados	El cable UTP Transporta de grandes cantidades de información, en distancias mayores al cable coaxial sin usar amplificadores.
	Fibra óptica	Inmune a las interferencias, pero poco utilizado en CCTV por su coste relativamente mayor.
<b>Inalámbricos</b>	Señales de radio frecuencia	Se limita a componentes (fundamentalmente cámaras) en donde realizar la instalación cableada resulta muy complicada y costosa.
	Señales infrarrojas	En las instalaciones CCTV queda reservada para las pequeñas aplicaciones como los mandos a distancia.

Fuente: (Fernández, 2013)

#### **2.2.4.5 Accesibilidad remota.**

Las cámaras de red se conectan fácilmente a las redes IP existentes y permiten actualizaciones en tiempo real de video de alta calidad para que resulte accesible de cada uno



de los ordenadores de una red. Las áreas sensibles como son la sala de servidores, la recepción o cualquier lugar remoto pueden ser monitorizado detalladamente de una forma económica, a través de la red de área local o de Internet. (Mesias, 2011)

Es importante notar la disponibilidad de acceso que brindan estos sistemas, brindándonos opciones de conexión a varios usuarios a la vez, manteniendo el monitoreo de forma rápida y a tiempo real.

#### **2.2.4.6 Calidad de imagen.**

Para poder obtener imagen y video de calidad y con claridad de una persona u objeto debemos seleccionar los elementos que nos proporcionen estas bondades, estos elementos deben estar implicados dentro del diseño del sistema de video vigilancia. Se proporciona las tecnologías que permite a una cámara de red producir una mejor calidad del video. En cuanto a resolución y nitidez de la imagen siempre se busca obtener el mejor resultado dependiendo del área a ser vigilada y los componentes que caracterizan la cámara para la zona particularmente seleccionada.

#### **2.2.4.7 Gestión de eventos y videos inteligentes.**

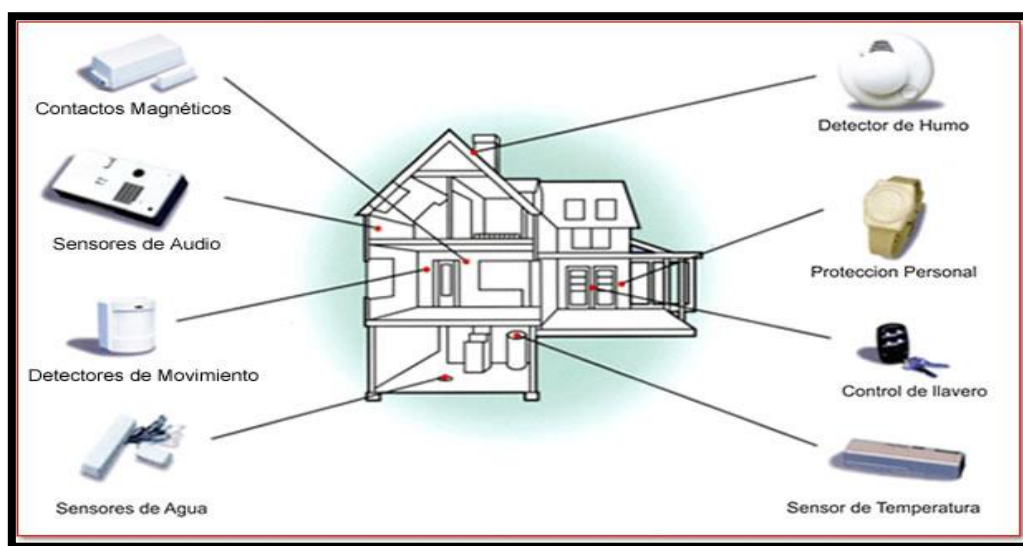
Las cámaras de red avanzadas, dispositivos de grabación y servidores con tecnologías que nos permiten reducir la cantidad de peso del video y que a través de los modos de grabación inteligente que permite tener tareas programadas en donde se puedan optimizar el recurso de almacenamiento basándose en eventos además realizar el respaldo de los mismo.

### 2.2.4.8 Escalabilidad y flexibilidad.

Estos sistemas pueden aumentar de acuerdo a las necesidades del usuario, las misma que nos ofrecen un sin número de cámaras IP y no se necesita de mucha inversión para la implementación de las misma.

### 2.2.5 Sistema de Alarma

Sistema de seguridad electrónico instalado al interior de una propiedad, compuesto por una central o panel de alarmas (dispositivo esencial en el sistema), un teclado que permite programar todas las funciones del sistema, avisadores acústicos (sirenas, luces etc.) y por último un determinado sistema de detectores o sensores denominados de acción perimetral, tales como contactos magnéticos para puertas y ventanas, sensores de humo y de temperatura, que serán los encargados de informar a una central de monitoreo ante la ocurrencia de situaciones anómalas como robos, incendios y emergencias médicas en el hogar. (Gacitúa, 2007, págs. 8-10)



**Figura 10. Esquema básico de un sistema de alarma.**

**Fuente:** *Actiweb.es. (2013). Recuperado de:*

*<http://www.directoriolocal.com/dl/media/Promocionales/24429MaximaSeguridad4.jpg>. (Grafico)*

### 2.2.5.1 Elementos de sistemas de alarma.

Este sistema consta de los siguientes dispositivos:

- **Panel o central de alarmas:** Recibe los eventos detectados por los dispositivos que forman parte del sistema.
- **Teclado:** Permite al usuario autorizado la activación y desactivación del sistema
- **Sensores Magnéticos:** Detectan si alguna puerta o ventana son abiertas.
- **Sensor Infrarrojo de movimiento:** Detectan la presencia de un intruso en el interior de la empresa.
- **Sirena interior y/o exterior:** Alerta audible ante una emergencia.
- **Pulsadores para emergencias** fijos o inalámbricos (botón de pánico): Activación manual del sistema de alarma.
- **7. Placa disuasiva:** Se ubica fuera de la propiedad, advierte a los delincuentes que los bienes están siendo protegidos.

## 2.3 Computadores de placa reducida

Un computador de placa reducida o también conocido como dispositivo SBC (Single Board Computer), es un computador completo en un sólo circuito, el cual dispone de todas las características de una computadora funcional en una sola tarjeta de tamaño reducido. En definitiva, alberga todo lo que necesita para su correcto funcionamiento en la placa base. A lo largo del presente trabajo, se mencionarán algunos de estos dispositivos y sus características. Actualmente, estos dispositivos se encuentran en auge debido principalmente a la buena relación de prestaciones y a su reducido precio. En los últimos años, los SBC o mini PCs han

sufrido una gran evolución y desarrollo, aumentando su rendimiento y características, hasta el punto de ser utilizados como un computador de uso común. (García, 2016)

Hoy en día, los computadores de placa reducida se orientan hacia una multitud de aplicaciones y se usan dispositivos de uso industrial y domésticos. Principalmente los computadores de placa reducida tienen más acogida en aplicaciones para el hogar y para las pequeñas empresas, entre los computadores de placa reducida más conocidos están los siguientes:

### **2.3.1 Raspberry Pi.**

Raspberry Pi es un computador SBC (Single Board Computer) de bajo costo de tamaño muy reducido se puede comparar al tamaño de una tarjeta de crédito, fue creado principalmente con el propósito de enseñar a los niños a programar los computadores. Este dispositivo fue desarrollado por la fundación Raspberry Pi en la Universidad de Cambridge, el cual tiene como objetivo la enseñanza de la informática en las escuelas. (Raspberry, 2017)

### **2.3.2 Jaguarboard.**

Este computador de placa reducida conocido como JaguarBoard nació recientemente de un proyecto de Kickstarter y ya en su primer modelo, la Jaguar One cuyo mayor atractivo es la compatibilidad con X86 y la posibilidad de instalar Windows 8 o 10 en su versión completa. (Jaguarboard, 2015)

### **2.3.3 ODroid.**

Este computador es la principal competencia de la Raspberry Pi 3 tanto en características como al precio comercial del dispositivo, pero sobre todo por prestaciones están al mismo nivel. Con una diferencia que este computador en su placa base no cuenta con tarjeta

inalámbrica de que sea de serie, esto se soluciona con un adaptador inalámbrico WiFi. El último modelo ODroid-XU4 es más potente, tiene más memoria RAM, puerto de infrarrojos y su salida HDMI permite sacar vídeo 4K a 60 Hz con soporte H.265. (Hardkernel, 2013)

### **2.3.4 CubieBoard.**

Un computador de placa reducida versátil y de gran potencia, este el ordenador en sus más recientes modelos CubieAOI-A20 y el Cubieboard5 y dispone de mucha característica y prestaciones que lo hacen un SBC muy potente. La recién lanzada placa cuenta con procesador Allwinner H8 de ocho núcleos, la posibilidad de integrar una batería para nuestro proyecto y conectividad máxima para este tipo de productos: HDMI, DisplayPort, Wifi, BT 4.2, SATA 2.0, IR y salida de audio S/PDIF. (CubieBoard, 2016)

### **2.3.5 Intel Galileo.**

Este computador de placa reducida posee características que garantizan la compatibilidad con el software de Arduino Uno R3, incluyendo también la capacidad de conectar los mismos accesorios. Este es un proyecto completamente libre que actualmente se encuentra en su segunda generación Galileo Gen 2 y toda la documentación está publicada para que la comunidad la tenga a su disposición y puedan estudiarla con detenimiento. (Intel, 2017)

## **2.4 Software Libre**

Al hablar de software libre nos referimos a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. Nos referimos especialmente a cuatro clases de libertad para los usuarios de software:

- Libertad 0: la libertad para ejecutar el programa sea cual sea nuestro propósito.

- Libertad 1: la libertad para estudiar el funcionamiento del programa y adaptarlo a tus necesidades, el acceso al código fuente es condición indispensable para esto.
- Libertad 2: la libertad para redistribuir copias y ayudar así a tu vecino.
- Libertad 3: la libertad para mejorar el programa y luego publicarlo para el bien de toda la comunidad, el acceso al código fuente es condición indispensable para esto.

El software libre no significa que sea “No comercial”. Cualquier programa libre estará disponible para su uso, desarrollo y distribución comercial. El desarrollo comercial del software libre ha dejado de ser excepcional y de hecho ese software libre comercial es muy importante. (Stallman, 2004)

#### **2.4.1 Características generales.**

Algunas de las características del software libre han sido enfocadas a una gama amplia de usuarios brindando ventajas para desarrollar aplicaciones que resuelvan sus necesidades, entre las que más se destacan están las siguientes:

Multiusuario. - Permite a usuarios diferentes con permisos diferentes, compartir el procesador y demás recursos del ordenador al mismo tiempo.

Multitarea. – A través de esta característica se realizan varias actividades a la vez, las cuales están controladas por el sistema operativo y no por las aplicaciones que se están ejecutando en ese instante.

Compatibilidad. – Se refiere a la compatibilidad de archivos desarrollados en otro sistema operativo y que se puedan usar, tales como libreoffice, openoffice, entre otras que son compatibles con Windows, existen también algunos programas que se pueden ejecutar en Windows.

Estabilidad. – Si algún programa falla no significa que afectará al resto de programas o aplicaciones que se estén ejecutando en ese instante en el sistema operativo.

Soporte. – Está respaldada por una gran comunidad de personas que se dedican al desarrollo, actualización y mejoras para proveer soluciones, esto lo realizan mediante blogs, foros o comunidades.


Adaptación. - Linux permite adaptarse al mercado y a las necesidades debido a que se tiene libertad de modificación del código y puede modificarse de acuerdo al problema y sus necesidades.

#### 2.4.2 Distribuciones de Linux.

Las distribuciones de Linux se logran gracias a las comunidades de personas y también a empresas que dedican sus labores a unir el núcleo Linux con aplicaciones y determinados paquetes de software para satisfacer las necesidades de un grupo específico de usuarios, dando así origen a ediciones domésticas, empresariales y para servidores.

Entre las principales distribuciones de Linux se encuentran las siguientes:

**Tabla 4. Principales distribuciones de Linux.**

Distribución	Descripción
 <p>UBUNTU</p>	<p>Distribución basada en Debian, con lo que esto conlleva y centrada en el usuario final y facilidad de uso. Muy popular y con mucho soporte en la comunidad. El entorno de escritorio por defecto es GNOME.</p>

---

**REDHAT ENTERPRISE**

Esta es una distribución que tiene muy buena calidad, contenidos y soporte a los usuarios por parte de la empresa que la distribuye. Es necesario el pago de una licencia de soporte. Enfocada a empresas.

---

**FEDORA**

Esta es una distribución patrocinada por RedHat y soportada por la comunidad. Fácil de instalar y buena calidad.

---

**DEBIAN**

Otra distribución con muy buena calidad. El proceso de instalación es quizás un poco más complicado, pero sin mayores problemas. Gran estabilidad antes que últimos avances.

---

**OpenSuSE**

Otra de las grandes. Fácil de instalar. Versión libre de la distribución comercial SuSE.

---

**GENTOO**

Esta distribución es una de las únicas que incorporaron un concepto totalmente nuevo en Linux. Es un sistema inspirado en BSD-ports. Puedes compilar/optimar el sistema completamente desde cero. No es recomendable adentrarse en esta distribución sin una buena conexión a internet, un

---



---

ordenador medianamente potente y cierta experiencia en sistemas Unix.

---



Esta distribución fue creada en 1998 con el objetivo de acercar el uso de Linux a todos los usuarios, en un principio se llamó Mandrake Linux. Facilidad de uso para todos los usuarios.

---

Fuente: (Martinez, 2014)

### **2.4.3 Administrador de procesos Cron.**

Cron es un administrador de procesos en segundo plano que ejecuta procesos o scripts en intervalos regulares de tiempo los cuales pueden ser programador por el usuario. Puede compararse a Cron con el equivalente al programador de tareas de Windows. Cron recurre al archivo de configuración Crontab el cual contiene los procesos o scripts que deben ejecutarse detallado con la hora y el día, por lo tanto, Crontab es un archivo de GNU Linux donde se guardan las distintas tareas programadas de los usuarios.

### **2.4.4 Scripts en Linux.**

Un script es un archivo que contiene un conjunto de comandos que son ejecutados secuencialmente, desde el primero hasta el último. El objetivo es automatizar la tarea de introducir los comandos uno por uno en la consola de comandos, y ejecutar las ordenes que queremos realizar de forma ágil y automática.

En todos los scripts se encuentra una primera línea, textualmente es `#!/bin/bash` se puede separar esta línea en dos partes, la primera es `#!`. A esta secuencia de dos caracteres se le denomina como sha bang. El sha bang indica al sistema que lo que viene a continuación son instrucciones de comando, para que este las procese como tal. La segunda parte `/bin/bash` indica el shell que va a utilizar el script para ejecutar los comandos. (Ovtoaster, 2014)

#### 2.4.5 Software libre para telefonía IP.

La telefonía IP está conformada por un conjunto de aplicaciones y protocolos que permiten servicios, entre los más comunes hacer y recibir llamadas telefónicas a través de redes informáticas, están presentes en redes LAN, se utilizan con frecuencia en Intranets corporativas y educativas, hasta en Internet. La telefonía IP hace uso de la tecnología VoIP<sup>16</sup> que permite digitalizar, empaquetar y transportar la voz sobre redes de datos, así también la telefonía IP trae consigo innumerables ventajas a la par de ciertas desventajas, pero, sobre todo, representa grandes oportunidades para proyectos de pequeña, mediana y gran escala, para este proyecto y por los retos que se plantea representa una parte fundamental el diseño de sistemas de video vigilancia y sistemas de alarma con funciones de alerta con llamadas.

El papel del software libre respecto a la telefonía IP ha sido y es importante en cuanto a las propuestas que la comunidad Open Source ha expuesto y continúa desarrollando. Algunas de estas propuestas y alternativas son:

**Bicom PBXware.** - Es una distribución basada en Gentoo y disponible únicamente en arquitectura i386, es una distribución con el único fin de ofrecer un sistema que facilite el uso de una plataforma de telefonía y que soporta un amplio abanico de tecnologías VoIP y PSTN<sup>17</sup>,

---

<sup>16</sup> VoIP: Voz sobre Protocolo de Internet o Telefonía IP. (Voice over Internet Protocol).

<sup>17</sup> PSTN: Red telefónica pública conmutada. (Public Switched Telephone Network).

donde podremos crear operadores automáticos IVR<sup>18</sup>, hilos musicales de espera, redes de voz tanto nacionales como a nivel global, correos de voz ampliamente mejorados, conferencias puente y otras tantas funcionalidades más. Ciertamente, la interfaz de configuración de esta distribución es de lo más amigable, y ofrece que tendremos en minutos un sistema de comunicaciones PBX<sup>19</sup> funcionando. (Bicom, 2018)

**Alpine Linux.** - Diseñado con el objetivo de lograr un sistema de comunicaciones seguro en esta distribución podremos encontrar singulares características que nos ayudarán a prevenir brechas de seguridad por las que nuestro sistema pueda ser vulnerado. Ofrece también firewalls, aplicaciones VPN<sup>20</sup>, así como cajas y servidores VoIP, es un sistema bastante ligero gracias a las librerías y herramientas base que más comúnmente podemos encontrar en sistemas embebidos. (Alpine, 2018)

**DigAnTel.** - Destinada a ofrecer al usuario un sistema de telefonía VoIP gratuito y de gran estabilidad y seguridad, ya que está basado en una muy lograda combinación entre CentOS, Asterisk y FreePBX. Ofrece funcionalidades como VoicePulse, Openfire, vtigerCRM, OpenVPN o Postfix, así como un módulo para soporte automatizado Polycom. La simpleza y eficiencia de su instalación la hacen la más recomendada para los que se inician en este campo, ya que no requiere conocimiento alguno de cómo funcionan Asterisk o Linux, la podemos encontrar únicamente disponible para arquitecturas i386. (Pimentel, 2018)

**AsteriskNOW.** - Es una distribución sobre la que se puede desplegar una plataforma de comunicaciones VoIP. En ella podemos encontrar los paquetes preinstalados de Asterisk, la interfaz gráfica AsteriskGUI, el framework DAHDI, así como los componentes necesarios para que ejecutemos correctamente toda la instalación y configuración de nuestra plataforma. Como

---

<sup>18</sup> IVR: Respuesta de voz interactiva. (Interactive Voice Response).

<sup>19</sup> PBX: Central telefónica Privada conectada a la red pública de telefonía. (Private Branch Exchange).

<sup>20</sup> VPN: Red privada virtual. (Virtual Private Network).

paquete opcional nos ofrece la interfaz gráfica de FreePBX. Basado en Fedora y CentOS, nos ofrece una estabilidad y compatibilidad de paquetería para que nos sea más fácil el desarrollo o instalación de software. (Digium, 2018)

**FreePBX.** - Bajo el compendio de Linux, Apache, MySQL y LAMP encontramos esta distribución que integra Asterisk, junto con una interfaz gráfica orientada al usuario estándar y muy intuitiva que ellos mismos han desarrollado. Se ofrece de forma gratuita y lista para poner en producción. Posee una adaptación modular, podemos ir completándola a medida que vayamos necesitando según qué recursos, pudiendo añadir módulos de BlackLists, de enrutamiento entrante/saliente, colas de llamadas, buzones de voz VoIP, de respuesta de voz interactiva, está disponible en 32 y 64 bits. (Technologies, 2018)

**Elastix.** - Desde que en 2006 apareciese como una interfaz para gestionar tareas de Asterisk, Elastix ha evolucionado gratamente hasta llegar a ofrecernos una solución "todo en uno", siendo posible durante la instalación, además de los paquetes base para el despliegue de la plataforma VoIP, otros complementos que mejoran o amplían las funcionalidades, sistema de mensajería instantánea y demás funcionalidades. Es la segunda solución más extendida (tras AsteriskNOW) para la implementación de estos sistemas de comunicación. Podemos encontrarla disponible para arquitecturas de 32 y 64 bits. (Elastix, 2018)

**TrixBox.** - La versión free que se ofrecía a los usuarios ya no está activa, por lo que únicamente se puede encontrar de pago o bien buscar una versión obsoleta de dicho sistema. Podremos encontrar en sus sistemas, donde años de experiencia han dado lugar a un sistema muy estable grandes funcionalidades. Aunque actualmente deja de llamarse Trixbox, ya que su nombre actual es Fonality. (Fonality, 2018)

#### 2.4.6 Software libre para gestión de cámaras.

Los softwares de gestión de video cumplen la función de optimizar las características de las cámaras y brindar al sistema funcionalidades para la video vigilancia, compresión del video, administración de almacenamiento, detección de movimiento, monitoreo remoto y respuestas ante intrusiones. Existen una variedad de este tipo de software de código abierto a continuación se menciona algunos de los más destacables.

**ZoneMinder** es un conjunto de aplicaciones gratuitas para cámaras de vídeo, diseñado para la seguridad de vídeo de bajo coste como circuito cerrado de televisión comercial o para el hogar, detección de movimiento para la prevención de robo, monitoreo del niño con aplicación de niñera o familia. Es compatible con la captura, análisis, registro y seguimiento de los datos de vídeo procedentes de cámaras conectadas a un sistema Linux. En la detección de movimiento, también se admiten las alertas por correo electrónico y visualización remota. (ZoneMinder, 2018)

**Motion** es un programa que supervisa la señal de vídeo desde una o más cámaras y es capaz de detectar si una parte significativa de la imagen ha cambiado; en otras palabras, se puede detectar el movimiento.

El programa está escrito en C y está hecho para el sistema operativo Linux. Motion es una herramienta basada en la línea de comandos cuya salida puede ser en formato jpeg, fies ppm o secuencias de vídeo MPEG. Motion es impulsado por línea de comandos estrictamente y puede ejecutarse como un demonio. Es la herramienta perfecta para monitorear su propiedad, enfocándose sólo en aquellas imágenes que son interesantes. (Dave, 2018)

**Shinobi** es un software de circuito cerrado de televisión de código abierto escrito en node.js. Diseñado con un sistema de múltiples cuentas, corrientes por WebSocket, y guardar a WebM. Xeoma es el software más vendido para la vigilancia de vídeo flexible. (Alam, 2018)

**Xeoma** inspirado en juegos y aplicaciones para niños, Xeoma permite construir su sistema de vigilancia de vídeo mediante la funcionalidad de combinación de bloques. Su interfaz innovadora y de uso sencillo creado para los usuarios, es perfecta para hogares y negocios. Todas las funciones habituales y actualmente está siendo elaborado para Cámaras IP. (Felenasoft, 2018)

## 2.5 Estándar IEEE 802.3 (Ethernet)

Ethernet es la tecnología de red de área local más usada en la actualidad, es la tecnología LAN más popular, IEEE<sup>21</sup> 802.3 define las reglas para la configuración de una red Ethernet la cual maneja dos aspectos físico y lógico correspondientes a la capa física y la capa de enlace de datos respectivamente.

Utiliza el esquema de acceso CSMA/CD<sup>22</sup> es decir comparte el mismo canal de comunicación y además todos los equipos reciben todas las transmisiones. El esquema de acceso CSMA/CD, accede a la red utilizando el acceso múltiple de percepción de portadora con detección de colisión es decir que el componente de la red escucha antes de transmitir, si dos componentes transmiten se genera una colisión. Por lo que el uso de conmutadores reduce en gran medida las colisiones y aumenta el rendimiento de la red. (Ortiz, Francisco, Jorge, Pablo, & Luis, 2012, págs. 28-29)

---

<sup>21</sup> IEEE: Instituto de Ingeniería Eléctrica y Electrónica. (Institute of Electrical and Electronics Engineers).

<sup>22</sup> CSMA/CD: Acceso múltiple con escucha de portadora y detección de colisiones.

### 2.5.1 Características de la tecnología Ethernet.

El nombre correcto para esta tecnología es IEEE 802.3 CSMA/CD, pero casi siempre es referido como Ethernet. IEEE 802.3 Ethernet fue adoptado por la organización internacional de estandarización (ISO), haciéndolo un estándar de redes internacional. Ethernet continuó evolucionando en respuesta a los cambios en tecnología y necesidades de los usuarios. Desde 1985, el estándar IEEE 802.3 se actualizó para incluir nuevas tecnologías.

La arquitectura Ethernet provee detección de errores, pero no corrección de los mismos. Tampoco posee una unidad de control central, todos los mensajes son transmitidos a través de la red a cada dispositivo conectado. Cada dispositivo es responsable de reconocer su propia dirección y aceptar los mensajes dirigidos a ella. El acceso al canal de comunicación es controlado individualmente por cada dispositivo utilizando un método de acceso probabilístico conocido como contención. (Edwards, 2012)

#### 2.5.1.1 Ethernet elementos básicos.

Ethernet consta de cuatro elementos básicos para su funcionamiento lógico y físico:

- **El medio físico:** compuesto por los cables y otros elementos de hardware, como conectores, utilizados para transportar la señal dos utilizan entre los computadores conectados a la red.
- **Los componentes de señalización:** dispositivos electrónicos estandarizados (transceivers) que envían y reciben señales sobre un canal Ethernet.
- **El conjunto de reglas para acceder el medio:** protocolo utilizado por la interfaz (tarjeta de red) que controla el acceso al medio y que les permite a los computadores

acceder (utilizar) de forma compartida el canal Ethernet. Existen dos modos: half y full dúplex

- **El frame Ethernet:** conjunto de bits organizados de frame es utilizado para llevar los datos dentro del sistema Ethernet. También recibe el nombre de marco o trama. (Barbieri, 2012)

## 2.6 Estándar IEEE 802.15 (Bluetooth)

IEEE 802.15 es el estándar para Bluetooth, tecnología de comunicaciones inalámbricas que fue establecida para corto alcance, admitiendo transmisión de voz y datos creando una red de área personal (PAN). Éste es un sistema que ensancha el espectro por saltos de frecuencia, trabajando en las bandas ISM de disponibilidad internacional a 2,4 GHz. La especificación 2.0 de Bluetooth aplicó una velocidad de transmisión mejorada de hasta 3 Mbits/s; además, ésta tecnología sigue la tendencia a la reducción del consumo energético. (Rohde & Schwarz, 2016)



**Figura 11. Esquema básico de conexión Bluetooth.**

*Fuente: Grupo Tecma Red S.L. (2012). Recuperado de:*

*<https://www.casadomo.com/images/casadomo/articles/content/20120723-russound-audio-bluetooth.jpg>  
(Grafico)*

En la figura 11 observamos que en la tecnología Bluetooth se encuentra incorporada en la mayoría de dispositivos móviles, permitiendo la conectividad de auriculares inalámbricos o entre teléfonos móviles u otros dispositivos para su sincronización. También, la mayoría de automóviles nuevos cuentan con el sistema de manos libres basado en Bluetooth®, como un



equipamiento estándar u opcional. Debido al bajo valor de consumo de esta tecnología de baja energía está dirigida al mercado de sensores de uso deportivo, sanitario y de condición física. Además, la posibilidad de conectar dispositivos de baja energía a los terminales móviles permite el diseño de nuevas aplicaciones. (Rohde & Schwarz, 2016)

## 2.7 Sistema Móvil Avanzado (SMA)

Es el servicio que permite a los abonados realizar y recibir llamadas de voz, SMS y acceder conexiones de datos mediante alguna aplicación como redes sociales. Este servicio final transmite, emite y recepta señales, imágenes, sonidos, datos, voz o información de cualquier naturaleza.

### 2.7.1 Operadoras móviles en Ecuador.

En el Ecuador existen tres operadoras que brindan este servicio móvil avanzado con sus tecnologías y aplicaciones.



**Figura 12. Operadoras móviles en Ecuador.**  
*Fuente: Claro, Cnt, Movistar, Tuenti. (2016). (Grafico)*

**CNT EP (Corporación Nacional de Telecomunicaciones)**, es la empresa pública de telecomunicaciones del Ecuador creada el 30 de octubre de 2008, opera brindando servicios de telefonía fija local, regional e internacional, servicio de acceso a internet estándar y de alta velocidad a través de redes de cobre y de fibra óptica, Internet móvil 3g y 4g LTE, televisión satelital y telefonía móvil en el territorio nacional ecuatoriano.

**CONECEL S.A. (Claro)**, empresa que impulsa el desarrollo mediante la conectividad, buscando crear un servicio universal, oferta servicios triple play, internet fijo, TV por cable, Internet móvil 3g y 4g y telefonía móvil. La Responsabilidad Corporativa de CLARO Ecuador está principalmente en contribuir a la disminución de la brecha digital, al lograr que la población tenga acceso a productos y servicios de telecomunicaciones en todos los rincones del país. La red de CLARO brinda acceso a servicio móvil al 96% de la población en el territorio ecuatoriano.

**OTECEL S.A. (Movistar y Tuenti)**, es una empresa proveedora de servicios de telefonía móvil de Ecuador, subsidiaria del Grupo Telefónica. Movistar, inició sus operaciones en abril de 2005. Movistar es la segunda mayor operadora de telefonía móvil del Ecuador con más de 3,8 millones de clientes, con muchos puntos de atención al cliente y con redes CDMA y GSM. Tuenti es la nueva marca de la concesionaria Otecel, busca consolidarse en el mercado de los servicios móviles ofreciendo navegación y acceso a redes sociales al público juvenil.

### **2.7.2 Tecnologías del sistema móvil avanzado.**

**WCDMA:** Ofrece flexibilidad en servicios combinando conmutación de paquetes y circuitos sobre el mismo canal, con una velocidad entre los 8 Kbps hasta 2 Mbps. Esta forma de transmitir datos es muy efectiva, especialmente si se dispone de un medio muy limitado, por ejemplo, el aire (ya que en ella no se puede ocupar cualquier frecuencia ya que algunas ya tienen otros usos específicos), además con ella se puede transmitir datos mucho más rápido y poder tener conexiones simultaneas, por ejemplo, hoy en día es posible en los celulares hablar y navegar a la vez. (Olguín & José, 2010)

**GSM:** Permiten que varios usuarios compartan un mismo canal, mediante la técnica TDMA (Acceso múltiple por división de tiempo) a cada llamada se le asigna una ranura de tiempo permitiendo que múltiples llamadas compartan un mismo canal sin interferencias,

también utiliza la técnica Frequency Hopping la cual minimiza las interferencias de las fuentes externas. Posee una velocidad de hasta 9.6 Kbps.

**HSPA:** Se basa en la red 3G y una mejora de 3G. Por lo tanto, tiene una carga y descarga más rápida velocidad. Es la velocidad máxima puede escalar tan alto como 14 Mbps. HSPA es a veces llamada sistema de comunicaciones móviles 3.5 G.

**HSPA+:** actualización de la tecnología HSPA con mejoras en la calidad de navegación, acceso a servicios multimedia, mejor calidad y definición. Es una tecnología 4G que permite la descarga a una velocidad de hasta 168Mbps.

**LTE:** reduce costos estructurales y la potencia consumida dando más capacidad a más usuarios por célula. Es un estándar de comunicación 4G que es compatible con la transmisión de vídeo de alta definición, la velocidad de descarga de hasta 299.6Mbps. (Techies, 2016)

## 2.8 Metodología

Con el seguimiento adecuado y una metodología para el desarrollo de este prototipo electrónico se podrá obtener resultados que satisfagan las necesidades de la empresa y usuarios de este sistema. Por cual es establece que “Para el diseño y desarrollo de proyectos de software se aplican metodologías, modelos y técnicas que permiten resolver los problemas” (Valdéz, s.f.)

Mediante una metodología se organizará el procedimiento de desarrollo del sistema de video vigilancia basado en movimiento en una secuencia de pasos en donde se pueda supervisar de forma ordenada y sistemática, verificando el cumplimiento de los objetivos propuestos, que además brindará la posibilidad de corrección a cada paso del desarrollo del sistema.

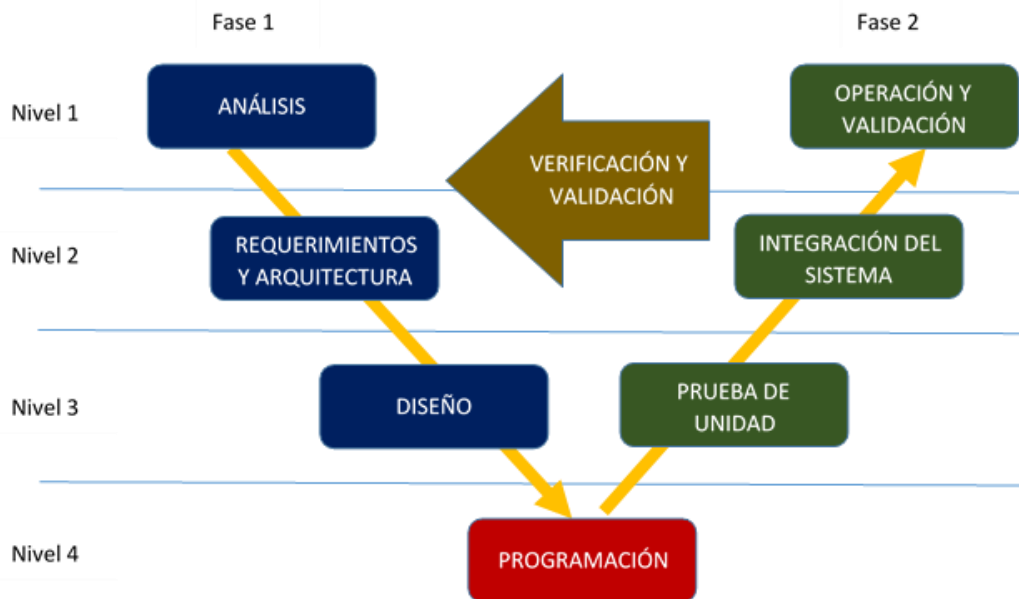
## 2.9 Modelo en V o de Cuatro Niveles

El modelo en V es un tipo de metodología utilizada para la gestión de proyectos, el cual utiliza técnicas de evaluación en donde describe métodos para la gestión y la elaboración de sistemas. Consiste en un proceso tipo cascada, donde se realiza validaciones y verificaciones en paralelo al proceso de desarrollo.

La “V” en este modelo es una representación gráfica del ciclo de vida para el desarrollo de sistemas está compuesta por dos fases, la primera fase correspondiente al lado izquierdo representa el desarrollo del proyecto, la cual se encarga en descomponer las necesidades y las especificaciones necesarias para crear el sistema; la segunda fase correspondiente a lado derecho está encargada de realizar la verificación de cada nivel del sistema.

Se puede adoptar el modelo en V y volverlo tan complejo como uno lo necesite, sin embargo, el fundamento es el mismo, ya que los objetivos de este modelo son minimizar los riesgos del proyecto y a la vez mejorar y garantizar la calidad de este.

En la Figura 13 se observa los componentes de este método, las dos fases correspondientes al lado izquierdo y derecho que presenta este modelo, además se indica que ambas fases están divididas por niveles que tienen relación directa entre su fase opuesta, esto indica que cada proceso cuenta con su método de verificación al momento de realizar su validación. La descripción de cada uno de los niveles del modelo en V o de cuatro niveles se detalla a continuación:



**Figura 13. Modelo en V para el desarrollo de Sistemas.**

*Fuente: (Rodríguez, 2008)*

El nivel 1 está orientado al “usuario”. El inicio del proyecto y el fin del proyecto conforman los dos extremos del ciclo de desarrollo en el modelo en “V”. En este nivel se definen los requisitos y especificaciones, estos se traducen en documentación que permitirá alcanzar el resultado final que se desea para el sistema.

El nivel 2 determina los requerimientos funcionales necesarios para la elaboración del sistema propuesto. Una vez realizado la integración del sistema se compara y se evalúa con los requerimientos iniciales planteados.

El nivel 3 se encarga de la arquitectura del sistema, abarca todo lo relacionado al software y hardware necesario para el desarrollo del sistema final, además define todos los estados que poseerá cada parte del sistema. En la fase de verificación se comprueba la funcionalidad individual de cada una de las partes del sistema.

En el nivel 4 se conoce como implementación en este se unen ambas fases, y en base a la documentación del diseño, se desarrolla una codificación para cada parte del sistema.

## CAPÍTULO III

### 3. DISEÑO DEL SISTEMA DE VIDEO VIGILANCIA Y ALARMA

En este capítulo se realiza un análisis a los factores que intervienen en el desarrollo de este sistema como lo son sus componentes, requerimientos, funciones, limitaciones y arquitectura de diseño. Se trató el tema con los actores involucrados, en este caso el gerente propietario del Almacén Color 2000, de esta manera se obtuvo la idea clara de la perspectiva del usuario. Mediante este análisis se pudo realizar la elección del software y hardware, para esto se empleó el estándar ISO/IEC/IEEE 29148 utilizando la metodología del modelo en V.

#### 3.1 Situación actual

Para el análisis de la situación actual fue necesario recopilar información sobre las algunas preguntas referentes al diseño del sistema y de esta forma obtener una visión clara para el desarrollo del proyecto. Esta información se obtuvo del gerente propietario de la empresa Almacén Color 2000 “Ing. Alicia Ramos”, que se encuentra a cargo de la administración. En la siguiente tabla se detalla el método que se utilizó para la obtención de la información

**Tabla 5. Método y formato para el levantamiento de información de la situación actual.**

<b>SITUACIÓN ACTUAL</b>	
<b>Método:</b>	Para realizar el levantamiento de información de la situación actual se empleó una entrevista con el gerente. Este método de investigación fue seleccionado debido a que la información se recopila de manera uniforme, es decir, permite descartar aquellos datos que no son de

---

utilidad a los objetivos de la entrevista permitiendo una fácil interpretación y análisis de la información.

La entrevista se realizó a la gerente propietaria Ing. Alicia Ramos, quien se encuentra de la administración, lo que se busca es identificar las áreas más importantes a monitorear, la forma de visualización y que métodos de alerta frente a un evento.

---

**Formato:**

Esta entrevista según es de tipo no estructurada, este tipo de entrevistas son muy útiles en los estudios descriptivos, ya que se busca los motivos para que se requiera este sistema y además obtener información específica sobre las áreas a monitorear.

El formulario de esta entrevista contiene preguntas abiertas, porque estas permiten captar más información y se espera una respuesta amplia y profunda.

El formulario de esta entrevista se puede observar en el Anexo 1 de este trabajo.

---

Fuente: Autoría.

Una vez realiza la entrevista a la Ing. Alicia Ramos, se logró recolectar información para sustentar el desarrollo de este sistema, a continuación, se detallan los resultados obtenidos con esta entrevista.

Mediante una entrevista con el gerente se determinó que existe la necesidad de un sistema de video vigilancia que permita la monitorización en la matriz de la empresa, debido a casos en los que la empresa presenta pérdidas ocasionadas por el robo de productos. La gerencia menciona también que el acceso a la bodega en donde se almacenan los productos debe ser vigilada, esto con el motivo de evitar pérdida de productos y monitorear las actividades de los empleados de la empresa.

La empresa con el fin de proteger los bienes materiales ha instalado un sistema de alarma convencional, el cual dispara una sirena cuando se activan los sensores de contacto en

la entrada principal y su salida de emergencia, cabe destacar que la empresa solo ha protegido accesos principales, La infraestructura arquitectónica de la empresa consta de ventanales tanto en la primera planta como en la segunda planta, esto podría ser usado por delincuentes para acceder a las instalaciones y sustraer los bienes.

En la primera planta debido a la afluencia de clientes y desarrollo de actividades del personal operativo, se precisa de un enfoque de monitoreo mediante video vigilancia con el objetivo de registrar en video los eventos ocurridos durante el día de laborable. En la segunda planta se debe vigilar el almacenamiento de los productos y el acceso a ellos, debe tener un respaldo en forma de video e imágenes.

Para complementar el sistema de alarma ya instalado en la empresa debe incorporarse un sistema de alarma basado en la detección de movimiento y que alerte al gerente propietario de la intrusión en las instalaciones de la empresa mediante una llamada a su teléfono móvil, envíe de un correo con imágenes del evento y envíe de un mensaje vía WhatsApp o Telegram hacia el número del gerente ya que la respuesta de atención a redes sociales es más rápida en la actualidad.

El objetivo de salvaguardar la integridad de clientes y empleados de la empresa Almacén Color 2000 y ofrecer un servicio de calidad tanto en atención como en seguridad, monitoreo y vigilancia forman parte de la misión de esta empresa por lo tanto es importante mantener un registro de las actividades que se realizan y respaldarlas en forma de video e imágenes.

El diseño de este sistema de videovigilancia se enfoca en la infraestructura de la matriz en donde funciona la empresa Almacén Color 2000, esta infraestructura consta de dos plantas en las cuales se basa este diseño. En la primera planta de esta institución están ubicadas las áreas de acceso principal, atención al cliente, salida auxiliar y la sección de estantería,



mostradores y vitrinas de los productos que oferta esta empresa. En la segunda planta se ubica la bodega con el fin de almacenamiento de productos, esta área es un espacio único sin divisiones.

Con los antecedentes mencionados anteriormente se propone a la gerencia realizar un diseño de un sistema de video vigilancia y alarma basada en la detección de movimiento para la matriz de empresa con el fin de dar una solución alternativa a las necesidades de esta institución, este diseño será presentado como trabajo de grado para la carrera de Ingeniería Electrónica y Redes de Comunicación en la universidad Técnica del Norte.

### **3.1.1 Análisis de Infraestructura en la empresa Color 2000.**

La infraestructura de la empresa Almacén Color 2000 como se muestra en los planos del anexo 9 se basa en cuatro áreas específicas a ser monitoreadas, las cuales están distribuidas entre la planta primera y la segunda. La primera planta se destaca la entrada principal como acceso a la empresa, la salida trasera o de emergencia, el área de atención al cliente y el espacio de estanterías, mostradores y vitrinas.

La segunda planta es un espacio amplio y sin obstáculos de visión en donde está ubicada la bodega de la empresa.

### **3.1.2 Determinación de áreas a vigilar.**

Las principales áreas que vigilar para el diseño de este sistema son:

Entrada principal y puerta trasera del edificio, es necesario una cámara por cada acceso a la empresa.



**Figura 14. Entrada principal y salida del Almacén Color 2000.**

*Fuente: Fotografía captura por el autor.*

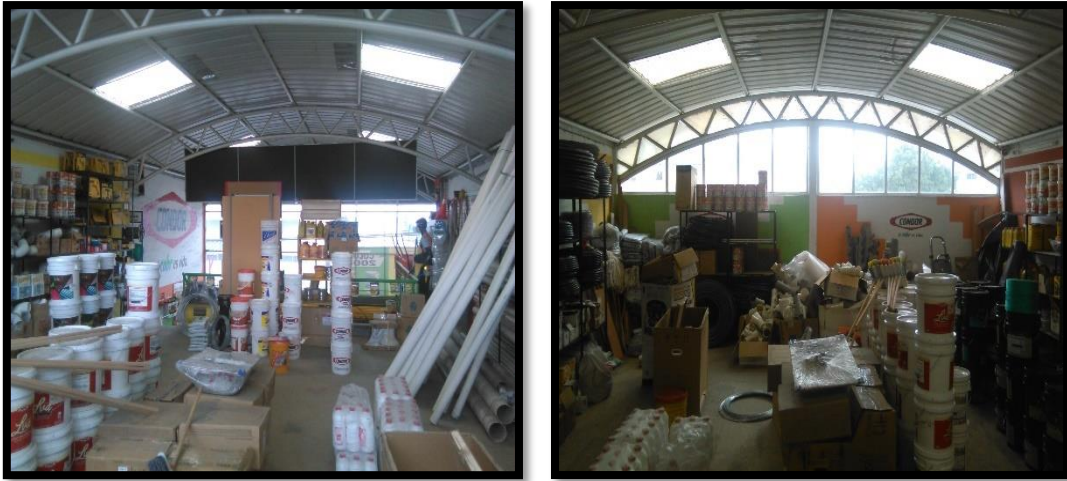
Se destina una cámara a la estantería, mostradores y otra para la zona de atención al cliente.



**Figura 15. Área de atención al cliente y estanterías.**

*Fuente: Fotografía capturada por el autor.*

La zona de almacenamiento de productos ubicada en la planta superior debe contar con una cámara para el monitoreo. Esta zona es de gran importancia para la gerencia de la empresa por ser un área extensa se dedica una cámara.



**Figura 16. Bodega del Almacén Color 2000.**  
*Fuente: Fotografía captura por el autor.*

### **3.1.3 Visualización y alertas del sistema.**

La visualización de la captura de imágenes y video se desea obtener mediante un monitor, Smartphone o tableta y a través de internet, las alertas frente a una intrusión se dirigirán al correo del sistema y por llamada al móvil del gerente, añadiendo también un mensaje de alerta a través de la aplicación Telegram.

### **3.1.4 Propósito del sistema.**

El propósito de este sistema es cubrir las necesidades de videovigilancia en la empresa Almacén Color 2000 con un sistema alternativo basado en software libre y la detección de movimiento mediante el empleo de cámaras web y softwares de gestión tanto de imagen como de control de llamadas.

### **3.1.5 Descripción general del sistema de seguridad.**

El sistema consta de dos partes, la primera enfocada a la video vigilancia y monitorización en las zonas acceso y de mayor importancia de la empresa descritas anteriormente, se lo realiza mediante la instalación de un sistema operativo y configuración del

computador de placa reducida en donde se instala el sistema operativo Raspbian que permite la gestión de cámaras utilizando el software Motion en donde se configura la detección de movimiento y el almacenamiento de la captura de video e imágenes generadas por las cámaras.

Esto permite la visualización de la transmisión de las cámaras ya sea en un monitor o en un computador de escritorio y el almacenamiento del video e imágenes en un disco a forma de respaldo.

La segunda parte dirigida al control del sistema y alarma basada en movimiento, la cual se logra gracias a la interacción de software Asterisk con el software Motion, en donde Asterisk toma control del sistema localmente mediante la configuración de un plan de marcado específico para este sistema, este plan de marcado está enfocado a la ejecución de scripts elaborados para el control y la detección de eventos mediante la función System del software Asterisk. Mediante un Softphone podemos controlar la activación y desactivación del sistema de alarma basada en detección de movimiento.

Asterisk permite conectarse a la red de Servicio Móvil Avanzado (SMA), haciendo uso del módulo cha\_mobile.so el cual permite generar un canal de comunicación FXS con un teléfono móvil haciendo uso de la tecnología Bluetooth y convertir el teléfono móvil en un Gateway de voz hacia la red de telefonía móvil.

Este modo de funcionamiento permiten responder frente a una intrusión en la empresa en donde se genera una llamada hacia el gerente propietario con las opciones programadas en el plan de marcado, se envía un correo y una alerta mediante redes sociales como WhatsApp o Telegram.

### **3.1.5.1 Funciones del sistema.**

La función principal del sistema consiste en el monitoreo y captura de video e imágenes obtenidas por las cámaras, las cuales serán transmitidas en un monitor, mediante un servidor web en la red local o internet. La función secundaria en conjunto con el monitoreo brinda un sistema complementario de alarma basada en la detección de movimiento, si se detecta movimiento generara una llamada telefónica, él envió de mensajes de alertas por correo electrónico y mensajería instantánea.

### **3.1.5.2 Características del sistema.**

El sistema se utilizará para la seguridad y monitoreo del Almacén Color 2000. El sistema de videovigilancia estará basado en un computador de placa de un tamaño reducido, cámaras web, un teléfono móvil con Bluetooth para la comunicación hacia la red de telefonía móvil y un disco de almacenamiento masivo con la finalidad de respaldar los video e imágenes obtenidos por las cámaras. El sistemas obtendrá las imágenes y video de las áreas a monitorearse, a estas se puede acceder mediante un Monitor o mediante un dispositivo como Tableta, Smartphone, Computador portátil o de escritorio mediante en navegador web en donde se trasmitirá el video obtenido de las cámaras mediante un servidor web. El sistema frente a la detección de movimiento realizara una llamada al gerente indicando esta alerta, paralelamente se envía un mensaje por correo electrónico con imágenes del evento captado y una alerta por mensajería instantánea por Telegram o Whassaap.

## **3.2 Requerimientos**

Este Sistema de videovigilancia pretende monitorear las áreas anteriormente definidas mediante la entrevista con el gerente de la empresa Almacén color 2000. Los requerimientos son el punto de partida para el desarrollo de este proyecto, de relacionan directamente las

necesidades del usuario con las soluciones que brindara el cumplimiento de los objetivos de este proyecto, para comprender esto de una forma más clara se identifica y lista los actores que intervienen de forma directa en este sistema como se muestra en la tabla 6.

**Tabla 6. Actores o Stakeholders que participan directamente en la investigación.**

<b>ACTORES INVOLUCRADOS</b>		
<b>Nº</b>	<b>Actor</b>	<b>Función</b>
<b>1</b>	Ing. Alicia Ramos	Gerente propietario.
<b>2</b>	Personal Operativo Almacén color 2000	Empleados a quienes es destinado este proyecto.
<b>3</b>	Ing. Omar Oña	Director del Presente Trabajo de Titulación.
<b>4</b>	Cristian Canacuan	Desarrollador del proyecto.
<b>5</b>	Universidad Técnica del Norte	Entidad de respaldo.

Fuente: Autoría.

### 3.2.1 Requerimientos indirectos necesarios para el desarrollo del sistema.

Una vez realizada la entrevista al Gerente y analizada la información obtenida, se puede describir algunos de los requerimientos que se identificaron para este proyecto. En la Tabla7 se detallan los requerimientos de los actores que intervienen en el proyecto. Se emplea la nomenclatura StSR, (Stakeholder Requirements Specification) que hace referencia a la especificación de requisitos de los interesados y se hace uso de su nomenclatura para la numeración de los requerimientos de esta tabla.

**Tabla 7. Requerimientos de los usuarios.**

<b>StSR</b>				
<b>REQUERIMIENTOS DE LOS ACTORES</b>				
<b>#</b>	<b>REQUERIMIENTO</b>	<b>PRIORIDAD</b>		
		<b>ALTA</b>	<b>MEDIA</b>	<b>BAJA</b>
<b>REQUERIMIENTOS DE USUARIOS</b>				
<b>StSR 1</b>	Monitoreo desde un Smartphone.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>StSR 2</b>	Control remoto del sistema.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>StSR 3</b>	Fácil activación y desactivación del sistema.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>StSR 4</b>	Video e imágenes deben ser guardados en un disco duro.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

<b>REQUERIMIENTOS OPERACIONALES</b>				
<b>StSR 5</b>	Conexión a Internet para el monitoreo remoto.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>StSR 6</b>	Conexión Bluetooth y WiFi.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>StSR 7</b>	Capacidad para funcionar por largos periodos de tiempo.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>StSR 8</b>	Tiempo para cargar la configuración del modo de funcionamiento Monitoreo y Alarma.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Fuente: Autoría.

### 3.2.2 Requerimientos iniciales del sistema.

Para lograr los objetivos propuestos en este sistema de videovigilancia, se debe plantear cuáles serán los requerimientos funcionales, A continuación, se presenta la Tabla 8 que corresponde a los requerimientos iniciales del sistema, aquí se definen los límites funcionales del sistema, se describen detalladamente los requerimientos de uso, interfaces, modos y estados, además de los requerimientos físicos. Esta tabla emplea la nomenclatura SySR, (System Requirements Specification).

**Tabla 8. Requerimiento del sistema de videovigilancia.**

<b>SySR</b>					
<b>REQUERIMIENTO DE FUNCIONES</b>					
#	Requerimiento	Prioridad			Relación
		Alta	Media	Baja	
<b>SySR 1</b>	Monitoreo de áreas por medio de video.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SySR 2</b>	Alarma por detección de movimiento.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>REQUERIMIENTO DE USO</b>					
<b>SySR 3</b>	Softphone para controlar los modos de funcionamiento del sistema.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>StSR 2</b>
<b>SySR 4</b>	Cargador de 5v -dc 2,5A para alimentar el computador de placa reducida	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SySR 5</b>	Hub USB con alimentación propia para conectar las cámaras	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SySR 6</b>	Disco duro externo para almacenar el video e imágenes.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>StSR 4</b>
<b>SySR 7</b>	Teléfono móvil con Bluetooth	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

<b>REQUERIMIENTO DE PERFORMANCE</b>					
<b>SySR 8</b>	Cámaras con resolución buena de imagen.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<b>SySR 9</b>	Rapidez en el procesamiento de los datos	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SySR 10</b>	Los componentes del sistema deben estar protegidos contra actos vandálicos.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SySR 11</b>	Ubicación estratégica del sistema en la infraestructura de la empresa.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<b>REQUERIMIENTO DE INTERFACES</b>					
<b>SySR 12</b>	La conexión Bluetooth debe ser automática.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<b>REQUERIMIENTO DE MODOS/ESTADOS</b>					
<b>SySR 13</b>	La activación del modo Monitoreo y Alarma se realiza con una contraseña ingresada en el Softphone instalado en el Smartphone.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<b>StSR 3</b>
<b>SySR 14</b>	El modo Solo Monitoreo debe estar en continuo funcionamiento.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>REQUERIMIENTO FÍSICOS</b>					
<b>SySR 15</b>	Integración del sistema en la infraestructura de la empresa.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SySR 16</b>	Computador de tamaño reducido.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Fuente: Autoría.

### 3.2.3 Requerimientos iniciales de Arquitectura.

En este análisis se presenta los requerimientos de arquitectura del sistema, en donde se definen los requerimientos lógicos, de diseño, hardware, software y eléctricos. Esta Tabla 9 se emplea la nomenclatura SRSR y así se obtiene la numeración de los requerimientos, se debe considerar que por la importancia de estos requerimientos esta tabla se la más importante ya que servirá para la elección de los componentes electrónicos que forman parte de este sistema de videovigilancia.



Tabla 9. Requerimientos Funcionales de Hardware y Software a utilizarse

<b>REQUERIMIENTOS DE FUNCIONES</b>					
#	Requerimiento	Prioridad			Relación
		Alta	Medi a	Baja	
<b>REQUERIMIENTOS LÓGICOS</b>					
<b>SRSH 1</b>	El sistema debe ubicarse dentro de un Rack pequeño.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<b>SySR 10</b>
<b>SRSH 2</b>	Debe contar con un UPS en caso de corte de energía eléctrica.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>SySR 15</b>
<b>SRSH 3</b>	En distancias superiores a 5m se debe usar cable USB activo.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<b>SySR 15</b>
<b>REQUERIMIENTOS DE DISEÑO</b>					
<b>SRSH 4</b>	Ubicar las cámaras y enfocarlas en el área a monitorear y que no sean manipuladas.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<b>SySR 15</b>
<b>SRSH 5</b>	El teléfono móvil debe contar con tarjeta sim activa de alguna operadora local.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<b>SRSH 6</b>	El número de teléfono móvil debe tener crédito para realizar llamadas.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SRSH 7</b>	El cableado debe estar canalizado por estética y protección.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<b>REQUERIMIENTOS DE SOFTWARE</b>					
<b>SRSH 8</b>	Soporta sistemas operativos Linux.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SRSH 9</b>	Capacidad de soportar gestión múltiple de cámaras.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SRSH 10</b>	Capacidad de gestionar llamadas VoIp.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SRSH 11</b>	Capacidad de ejecutar comandos del sistema (Modulo System.so).	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SRSH 12</b>	Poseer licencia gratuita para la utilización del software.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>REQUERIMIENTOS DE HARDWARE</b>					
<b>SRSH 13</b>	Buena velocidad de procesamiento y bajo costo.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<b>SySR 9</b>
<b>SRSH 14</b>	Mayor número de puertos USB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SRSH 15</b>	Conexión inalámbrica WiFi y Bluetooth.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>SRSH 16</b>	Salida de audio y video HDMI para interfaz gráfica del Sistema Operativo.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<b>SRSH 17</b>	Soporta discos externos.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<b>SySR 6</b>

## *REQUERIMIENTOS ELÉCTRICOS*

<b>SRSH 18</b>	Tomas eléctricas de pared, cargadores para alimentar los dispositivos.	☒	☐	☐	<b>SySR 4</b>
--------------------	--	---	---	---	---------------






Fuente: Autoría.

### 3.3 Selección de hardware y software para el sistema

Para el funcionamiento del sistema se debe tener los siguientes componentes básicos los cuales son: un computador de placa reducida, dispositivos de captura de video e imágenes (cámaras), HUB USB.

#### 3.3.1 Selección del computador de placa reducida

Tabla 10. Computadores de placa reducida.

Tipos de Ordenadores						
Características	Raspberry Pi 3	JaguarBoard	ODroid	CubieBoard	Intel Galileo	
<b>Descripción Grafica</b>						
<b>Procesador</b>	4 × ARM Cortex-A53, 1.2GHz	Intel Atom Z3735G	Samsung Exynos5422 Cortex™-A15 2Ghz and Cortex™-A7	ARM A7 8 núcleos	Pentium 400 MHz. con 16 Kb de memoria caché	
<b>Memoria</b>	1GB LPDDR2 (900 MHz)	1GB DDR3L	2GB LPDDR3	2 GB DDR3	DDR3 256 MB NOR Flash de 8MB	
<b>GPU</b>	Broadcom VideoCore-IV	No	ARM Mali-T628	PowerVR SGX544	No	
<b>Almacenamiento</b>	micro SD 8-32 GB soporta disco externo	On Board 16 GB eMMC	micro SD 8-32 GB	8 GB + SATA	micro SD 8-32 GB	
<b>Consumo de energía</b>	5V- 2.5A	5V- 2A	5V / 4A	5V- 2A Soporta batería de litio (como	5V- 1A	

					3.7 V a 5300 mAh)	
<b>Dimensiones</b>	85mm x 56 mm x 20mm	101.9mm x 65.5 mm x 1.6mm	x	83mm x 20 mm	x	91mm x 20 mm x 123mm x 72mm x 20mm
<b>Precio</b>	\$ 68	\$ 89		\$ 95		\$ 99 \$ 79
<b>Red</b>	Ethernet 10/100 Mbps 802.11n Wireless LAN	Ethernet 10/100 Mbps		Ethernet 10/100 Mbps		Ethernet 10/100 Mbps 802.11n Wireless LAN
<b>Velocidad</b>	1.2 GHz	1.83 GHz		2GHz		2GHz 400 MHz
<b>Bluetooth</b>	Bluetooth Classic, Bluetooth Low Energy.	4.1 No		No		Bluetooth 4.1 No
<b>Puertos</b>	HDMI, toma de audio y video analógico de 3,5 mm, 4 × USB 2.0, Ethernet, interfaz serie de la cámara (CSI), interfaz serie de pantalla (DSI).	HDMI, toma de audio y video analógico de 3,5 mm, 3 × USB 2.0, Ethernet.		HDMI, toma de audio y video analógico de 3,5 mm, 3 × USB 2.0, Ethernet.		HDMI, toma de audio y video analógico de 3,5 mm, 3 × USB 2.0, Ethernet. HDMI, toma de audio y video analógico de 3,5 mm, 3 × USB 2.0, Ethernet.

Fuente: Elaborado por Cristian Canacuan, fuente (CubieBoard, 2016), (Intel, 2017), (Jaguarboard, 2015), (Raspberry, 2017), (Hardkernel, 2013).

Con la información obtenida de la Tabla 10 sobre computadores de placa reducida y de las tablas de requerimientos del sistema se procede a realizar la elección del computador de placa reducida a usar en la tabla siguiente.

**Tabla 11. Elección del computador de placa reducida.**

HARDWARE	REQUERIMIENTOS						VALORACIÓN TOTAL
	SRSH 8	SRSH 13	SRSH 14	SRSH 15	SRSH 16	SRSH 17	
<b>Raspberry Pi 3</b>	●	●	●	●	●	●	6
<b>JaguarBoard</b>	●	○	○	○	●	○	2
<b>ODroid</b>	●	○	○	○	●	●	3
<b>Cubieboard</b>	●	○	○	●	●	○	3
<b>Intel Galileo</b>	●	○	○	○	●	○	2

●Cumple

---

○ No cumple

Elección: **Raspberry Pi 3**

---




Fuente: Autoría.

**Elección:** De acuerdo a los resultados que se obtuvieron en la Tabla 11 se determinó que el computador de placa reducida Raspberry Pi 3 es el más adecuado para el desarrollo de este sistema debido a sus características, las cuales cumplen con los requerimientos establecidos anteriormente, soporta la instalación de sistemas operativos Linux, su velocidad de procesamiento es alta, cuenta con 4 puertos USB para conexión de periféricos, cuenta con conexión vía WiFi y Bluetooth, cuenta con salida de Audio y video HDMI, soporta discos duros externos y su coste es relativamente bajo.

### 3.3.2 Selección de cámaras

Las cámaras web son pequeñas cámaras digitales que se conectan a una computadora con funciones de capturar imágenes y transmitir las a través del internet por medio de una página web u otras computadoras.

**Tabla 12. Cámaras web.**

<b>Webcams</b>			
<b>Características</b>	Cámara Logitech Pro C920	Cámara Imexx IME-41674	Cámara MINTON MWC 7105
<b>Descripción grafica</b>			
<b>Sensor de captura</b>	CMOS	CMOS	CMOS
<b>Resolución</b>	8MP	5 MP	1 MP
<b>Resolución de video MAX</b>	1920 x 1080	1280 x 720	640 x 480
<b>Micrófono incorporado</b>	Estéreo integrado 56db con reducción de ruido automática	Digital 56db	No

<b>Rotación</b>	Clip universal compatible con trípodes para monitores LCD, CRT o laptops	Omni direccional	Clip universal para monitores LCD, CRT o laptops
<b>Plug and Play</b>	Si	Si	Si
<b>Velocidad de fotogramas</b>	30 fps – 40 fps	hasta 30 fps	24fps
<b>Distancia de enfoque</b>	30mm	30 mm	20mm – 50mm
<b>Formato de video</b>	24 bits	24 bits	24 bits
<b>Interfaz</b>	USB 2.0	USB 2.0 y USB 1.1	USB 2.0 y USB 1.1
<b>SopORTE Linux</b>	Si	Si	Si
<b>Precio</b>	60 \$	14\$	12\$

Fuente: Elaborado por Cristian Canacuan, fuente (Logitech, 2017), (Imexx, 2017), (PINCOMPUTERS, 2017).

Tabla 13. Elección de cámara web.

HARDWARE	REQUERIMIENTOS						VALORACIÓN TOTAL
	StSR	SySR	SRSH	SRSH	SRSH	SRSH	
	8	8	3	4	8	13	
<b>Cámara Logitech Pro C920</b>	●	●	●	○	●	○	4
<b>Cámara Imexx IME-41674</b>	●	●	●	●	●	●	6
<b>Cámara MINTON MWC 7105</b>	○	○	●	○	●	●	3
●Cumple ○ No cumple							
Elección: <b>Cámara Imexx IME-41674</b>							

Fuente: Autoría.

**Elección:** De acuerdo a los resultados que se obtuvieron en la Tabla 13 se determinó que el tipo de cámaras a usar serán Imexx IME-41674 se ajustan a los requerimientos necesarios para el desarrollo de este sistema son las más adecuadas debido a sus características, puede operar con normalidad por largos periodos, la resolución de captura de imagen y video es de calidad moderadamente alta, la interfaz de comunicación es USB 2.0, es compatible con

sistemas operativos Linux, tiene la posibilidad de rotación para enfoque y una base tipo clip que permite su fijación y su precio en el mercado es bajo.

### 3.3.3 Selección del HUB USB.

El HUB USB permitirá conectar las cámaras al sistema así como otros periféricos que requiera el sistema de video vigilancia y alarma.

**Tabla 14. HUB USB.**

<b>HUB USB</b>			
<b>Características</b>	Anker Hub USB 3.0	Tp-Link UH700	7 HUB
<b>Descripción grafica</b>			
<b>Cantidad de Puertos</b>	7 puertos con 1 BC 1.2 Puerto de carga	7 Puertos	7 Puertos
<b>Carga rápida</b>	Hasta 1.5 amperios con dispositivos BC 1.2 compatibles	No	No
<b>Fuente de Alimentación</b>	12V- 3A	12V- 2.5A	5V- 2.5A
<b>Velocidad</b>	5Gbps	Hasta 5Gbps	480 Mbps
<b>Condiciones de uso.</b>	Debe ser alimentado por un adaptador de corriente y un puerto USB de PC activo.	Velocidad de transmisión actual está limitada por la configuración del dispositivo conectado.	Cambio automático al adaptador de corriente cuando la energía es baja desde el puerto USB del ordenador.
<b>Plug and Play</b>	Si	Si	Si
<b>Interfaz de entrada</b>	USB 3.0 estándar A soporta USB 2.0	USB 3.0 estándar A soporta USB 2.0 y USB 1.1	USB 2.0 estándar A y USB 1.1
<b>Interfaz de salida</b>	USB 3.0 estándar B	USB 3.0 estándar micro B	USB 2.0 estándar B
<b>Soporte Linux</b>	Si	Si	Si
<b>Precio</b>	35 \$	38\$	20\$

Fuente: Elaborado por Cristian Canacuan, fuente (ANKER, 2017), (TP-LINK, 2017), (Mercadolibre, 2017).

Tabla 15. Elección del HUB USB.

HARDWARE	REQUERIMIENTOS						VALORACIÓN TOTAL
	SySR	SySR	SRSH	SRSH	SRSH	SRSH	
	4	5	8	9	13	14	
<b>Anker Hub USB 3.0</b>	○	●	●	●	○	●	4
<b>Tp-Link UH700 7 HUB</b>	○	●	●	●	○	●	4
	●	●	●	●	●	●	6
●Cumple ○ No cumple Elección: <b>7 HUB</b>							

Fuente: Autoría.

**Elección:** De acuerdo a los resultados que se obtuvieron en la Tabla 15 se determinó que el tipo de HUB USB a usar será el 7 HUB siendo este un HUB de características básicas pero que satisfacen los requerimientos para este sistema. Puede operar con normalidad por largos periodos y velocidad máxima de 480 Mbps, cuenta con 7 puertos de entrada con interfaz USB 2.0 tipo A y un puerto de interfaz de salida USB 2.0 tipo B, tiene alimentación propia con un adaptador de corriente de 5V- 2.5A y su precio en el mercado es relativamente bajo.

### 3.3.4 Selección del Sistema Operativo.

Los sistemas operativos para el Raspberry Pi se pueden encontrar en sitios oficiales y no oficiales.

Tabla 16. Sistemas operativos para Raspberry Pi.

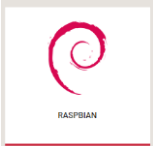


SISTEMAS OPERATIVOS PARA RASPBERRY PI		
	Sitios oficiales	Sitios no oficiales
<b>GNU/ Linux – Uso PC o servidor</b>	RASPBIAN Debian PIDORA Fedora	ARCH LINUX ARM Ubuntu Mate openSUSE pipaOS PiBang
<b>GNU/Linux – Uso Media Center XBMC</b>	RASPBMC OPENELEC	Xbian OSMC
<b>GNU/Linux</b>		Volumio

<b>– Uso Media Center Audio</b>		Rune Audio PiMusicBox piCorePlayer SqueezePlug Linux – Android
<b>No Linux – Uso PC o servidor</b>	RISC OS	FreeBSD Inferno OS Inferno PI Windows 10 IoT core

Fuente: Elaborado por Cristian Canacuan, fuente (Raspberry, 2017).

Al existir una gran lista de sistemas operativos que se pueden instalar en la Raspberry Pi, se debe tener claro el uso que vamos a dar al computador de placa reducida es como PC, servidor y no como una media center.

**Tabla 17. Características de sistemas operativos para Raspberry.**

<b>Sistemas Operativos Para Raspberry Pi</b>			
<b>Características</b>	Raspbian	Ubuntu Mate	Arch Linux ARM
<b>Logo</b>			
<b>Compatible con WiFi y Bluetooth incorporados.</b>	Si	Si	No
<b>Tamaño en tarjeta microSD</b>	4GB o más	6GB o más	6GB o más
<b>Rendimiento de E / S de microSDHC</b>	Utilice una clase 6 o Clase 10 microSDHC	Utilice una clase 10 microSDHC	Utilice clase 10 microSDHC
<b>Entorno de Escritorio</b>	LXDE	MATE	No instalado un entorno LXDE disponible.
<b>Usuario por defecto</b>	Pi	No Configurado	No Configurado

Fuente: Elaborado por Cristian Canacuan, fuente (Raspberry, 2017), (Ubuntu, 2017), (Archlinux, 2017).



Tabla 18. Elección del Sistema operativo.

SOFTWARE	REQUERIMIENTOS				VALORACIÓN TOTAL
	Tamaño mínimo en tarjeta sd.	Compatibilidad con la placa WiFi y Bluetooth.	Rendimiento con la microSDHC de E / S clase 10	Entorno de escritorio interactivo	
<b>Raspbian</b>	●	●	●	●	4
<b>Ubuntu Mate</b>	●	●	○	●	3
<b>Arch Linux ARM</b>	●	○	●	○	2

●Cumple  
○ No cumple

Elección: **Raspbian**




Fuente: Autoría.

**Elección:** El sistema operativo a instalarse en la Raspberry Pi 3 es Raspbian. El tamaño necesario para la instalación del sistema de archivos es relativamente pequeño, tiene total compatibilidad con las tarjetas Bluetooth y WiFi, aprovecha totalmente la velocidad de lectura de archivos aunque la tarjeta SD no sea de clase 10, el entorno de escritorio es interactivo y fácil de usar además Raspbian es un Sistema Operativo libre y gratuito, basado en Linux, de la distribución Debian, optimiza el hardware de la Raspberry Pi, posee un poco más de 35000 paquetes de programas y aplicaciones.

### 3.3.5 Selección del software de gestión de cámaras.

El software para gestión de cámaras permitirá el funcionamiento del sistema de videovigilancia, vinculando las cámaras al sistema, gestionando las imágenes obtenidas para ser transmitidas, presentada en un monitor o generar la alerta correspondiente a un evento de intrusión. Existe algunos softwares de gestión los cuales se analizan en la tabla 18 presentada a continuación.

Tabla 19. Características de softwares para gestión de cámaras.

Softwares para gestión de cámaras			
Características	Motion	Zone Minder	Xeoma
Logo			
Compatibilidad	Linux	Linux	Windows, Mac OS X, Linux.
Monitoreo de movimiento	Configuración de zona, tamaño máximo de objeto, nivel de sensibilidad del sensor. Algoritmo mejorado para evitar falsas alarmas causadas por mascotas o cambios climáticos.	Configuración de zona, tamaño máximo de objeto, nivel de sensibilidad del sensor.	Configuración de zona, tamaño máximo de objeto, nivel de sensibilidad del sensor
Formatos de video	mpeg4, msmpeg4, swf, flv, ffv1, mov, ogg, mp4, mkv, hevc.	mpeg4, msmpeg4, flv, mov, mp4, mkv.	WEBM (VP8 y VP9), MPEG-4, MP4 y MJPEG
Presentación automática	Imágenes en tiempo real	Imágenes en tiempo real	Imágenes en tiempo real
Guardado de archivos	Ruta especificada con grabación cíclica	Ruta especificada con grabación cíclica	Ruta especificada con grabación cíclica
Grabación inteligente	Configurada automáticamente por detección de movimiento.	No configurada, disponible.	No disponible.
Envío de mensajes de texto	No configura, disponible en SMS.	No disponible	No configura, disponible en SMS.
Notificaciones por correo electrónico	No configura, disponible con archivos adjuntos.	No configura, disponible con archivos adjuntos.	No configura, disponible con archivos adjuntos.
Acceso remoto	Acceso remoto completo a configuraciones, archivos y cámaras. Transmisión por Internet y en navegadores web.	Acceso remoto completo a archivos y cámaras. Transmisión por Internet y en navegadores web.	Acceso remoto completo a configuraciones, archivos y cámaras. Transmisión por Internet y en navegadores web.
Fácil integración	Listo para funcionar inmediatamente después de la descarga.	Requiere configuración de inicio.	Requiere configuración de inicio.

<b>Consumo de recursos del sistema</b>	Bajo consumo de recursos del sistema.	Alto consumo de recursos del sistema.	Alto consumo de recursos del sistema.
<b>Configuración</b>	Fácil y flexible	Media	Fácil

Fuente: Elaborado por Cristian Canacuan, fuente (Dave, 2018), (Felenasoft, 2018), (ZoneMinder, 2018).

**Tabla 20. Elección del Software de gestión de cámaras.**

SOFTWARE	REQUERIMIENTOS					VALORACIÓN TOTAL
	Detección de movimiento	Captura de video inteligente	Integración rápida y acceso remoto	Notificaciones por correo y mensajes	Configuración fácil y bajo consumo de recursos	
<b>Motion</b>	●	●	●	●	●	5
<b>Zone Minder</b>	●	○	●	●	○	3
<b>Xeoma</b>	●	○	○	●	○	2

● Cumple  
○ No cumple

Elección: **Motion**




Fuente: Autoría.

**Elección:** El software a instalarse para la gestión de cámaras es Motion. Este software permite detectar el movimiento mediante las cámaras y la configuración de zona, tamaño máximo de objeto, nivel de sensibilidad del sensor, posee un algoritmo mejorado para evitar falsas alarmas causadas por mascotas o cambios climáticos. La captura de video inteligente la realiza automáticamente por detección de movimiento, su integración al sistema es rápida y posee acceso remoto, puede enviar notificaciones por correo y por mensajes, su configuración es fácil y genera un bajo consumo de recursos del sistema.

### 3.3.6 Selección del software para telefonía IP.

Es software para telefonía IP gestionara la alerta por llamada telefónica hacia el gerente y contara con un menú interactivo el cual permitirá seleccionar una opción en respuesta a la alerta generada por el sistema de videovigilancia.

Tabla 21. Características de software para telefonía IP.

Softwares para telefonía IP			
Características	Alpine Linux	Asterisk	Elastix
Logo			
Funcionalidad	Desvíos, capturas, transferencias, Buzones de voz, IVR.	Desvíos, capturas, transferencias, Multi-conferencias Buzones de voz, IVR, CTI, ACD.	Desvíos, capturas, transferencias, Multi-conferencias Buzones de voz, IVR, CTI, ACD.
Escalabilidad	Desde 10 usuarios en una pequeña empresa, hasta 5.000	Desde 10 usuarios en una pequeña empresa, hasta 10.000 de una multinacional repartidos en múltiples sedes.	Desde 10 usuarios en una pequeña empresa, hasta 10.000 de una multinacional repartidos en múltiples sedes
Interoperabilidad y Flexibilidad	Soporte de puertos de interfaz analógicos (FXS y FXO) y RDSI (básicos y primarios), como los de telefonía IP (SIP, H.323, MGCP, SCCP/Skinny)	Soporte de puertos de interfaz analógicos (FXS y FXO) y RDSI (básicos y primarios), como los de telefonía IP (SIP, H.323, MGCP, SCCP/Skinny)	Soporte de puertos de interfaz analógicos (FXS y FXO) y RDSI (básicos y primarios), como los de telefonía IP (SIP, H.323, MGCP, SCCP/Skinny)
Capacidad de ejecutar comandos del sistema	Instalar Modulo	Modulo System.so	Modulo System.so
Soporte para Gateway de voz Bluetooth	No disponible	Modulo Chan_mobile.so	Instalar Modulo Chan_mobile.so
Disponible código fuente	Sistema todo en uno.	Si, compilación e instalación de código fuente de Asterisk en su versión más reciente y estable	Sistema todo en uno.
Soporte para ARM	No disponible	Disponible	Disponible
Manejo del Cli desde líneas de comandos	No disponible	Manejo desde línea de comando en instalación de código fuente para en Cli de Asterisk	Manejo desde línea de comando en instalación de código fuente para en Cli de Asterisk

Fuente: Elaborado por Cristian Canacuan, fuente (Alpine, 2018), (Digium, 2018), (Elastix, 2018).

Tabla 22. Elección del Software para telefonía IP.

SOFTWARE	REQUERIMIENTOS					VALORACIÓN TOTAL
	Soporte para ARM	Disponible código fuente	Soporte para Gateway de voz Bluetooth	Capacidad de ejecutar comandos del sistema	Interoperabilidad y Flexibilidad	
<b>Alpine Linux</b>	○	○	○	●	●	5
<b>Asterisk</b>	●	●	●	●	●	2
<b>Elastix</b>	●	○	○	●	●	3

● Cumple  
○ No cumple

Elección: **Asterisk**

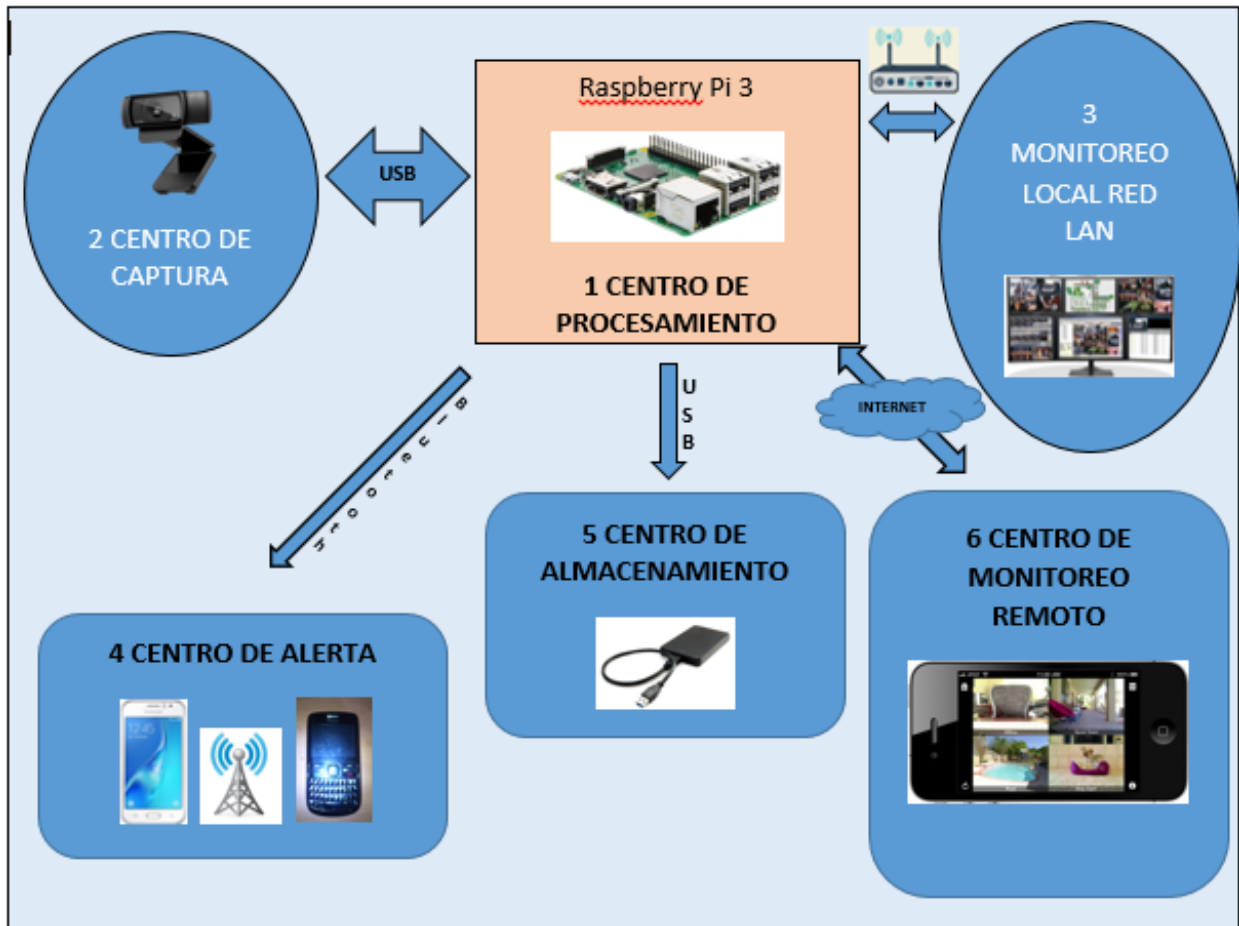
Fuente: Autoría.

**Elección:** El software a instalarse para telefonía IP es Asterisk. Este software es compatible para procesadores ARM, permite compilar su código fuente para optimizar recursos del sistema, cuenta con módulos tanto para que permiten el uso de Gateway de voz por medio de Bluetooth y ejecutar comandos del sistema como si los ejecutáramos directamente desde la línea de comando, esta función mediante un plan de marcado, cuenta con una alta interoperabilidad y flexibilidad en el manejo de extensiones.

### 3.4 Diseño general del sistema

#### 3.4.1 Diagrama de bloques.

A continuación se presenta el funcionamiento del sistema de videovigilancia y alarma por detección de movimiento mediante un diagrama de bloques en el cual se muestra sus elementos y la estructura con la que contará. En la figura 17 se muestra este diagrama mencionado.



**Figura 17. Diagrama de bloques del sistema.**

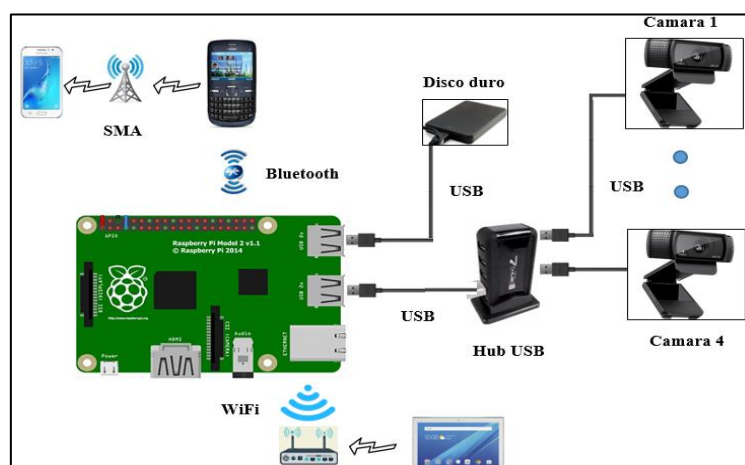
*Fuente: Elaborado por el autor.*

En la Figura 17 se presentan las secciones que conforman el sistema de videovigilancia y alarma basada en movimiento, a continuación se describe cada sección del diagrama de funcionamiento general numera respectivamente.

1. Esta sección corresponde al centro de procesamiento en donde actuará la configuración realizada en el computador de placa reducida, gestionando la captura de imágenes y video, almacenamiento, presentación para monitoreo local y remoto, almacenamiento de datos, control del sistema y alarma.
2. La sección de centro de captura es la encargada obtener las imágenes y video, enviándolas al centro de procesamiento para el análisis y almacenamiento en un disco externo o envío de imágenes por correo.

3. En la sección de monitoreo local se presentan las imágenes obtenidas por el centro de captura por medio de las cámaras, en esta sección se presenta las imágenes obtenidas por las cámaras pudiendo ser visualizadas ya sea en un Monitor, Tableta, Smartphone, PC de escritorio o portátil, se debe estar conectado a la red local.
4. Centro de alerta, encargado de ejecutar la llamada telefónica en caso de detectar un evento de intrusión, esta sección está gestionada y controlada por el centro de procesamiento.
5. En el centro de almacenamiento se guarda la información perteneciente a los eventos ocurridos y la imagen y video capturada por las cámaras.
6. En la sección de monitoreo remoto se presentan las imágenes obtenidas por el centro de captura por medio de las cámaras, en esta sección el centro de procesamiento permite acceder a las imágenes obtenidas por las cámaras a través de internet pudiendo ser visualizadas ya sea en un Monitor, Tableta, Smartphone, PC de escritorio o portátil, se debe tener conexión a internet.

### 3.4.2 Diagrama de conexiones.



**Figura 18. Diagrama de conexiones del sistema.**

*Fuente: Elaborado por el autor.*

La Figura 18 muestra el diagrama de conexión en donde se indica la ubicación de cada elemento electrónico del sistema, esto permite tener una guía para el correcto uso de cada elemento. La conexión entre el centro de procesamiento y el centro de captura se realiza a través de cableado USB 2.0 y cableado USB 2.0 Activo si la distancia supera 5 metros. La conexión del centro de procesamiento con el centro de almacenamiento se realiza con cable USB 2.0, la conexión con el centro de alerta se realiza por medio de tecnología Bluetooth y la conexión hacia el centro de monitoreo se realiza a través de la red área local.

### **3.4.3 Diagramas de flujo.**

El funcionamiento del sistema se define por la activación o desactivación del modo de funcionamiento del sistema, con este variable modo alarma el sistema decidirá si trabaja en Solo Monitoreo o en Monitoreo y Alarma.

Si el Modo Alarma es desactivado el sistema trabaja en modo Solo Monitoreo, las primeras entradas son establecer la ruta de almacenamiento, luego el procedimiento de activar la detección de movimiento, en donde si se detecta movimiento el centro de procesamiento almacenara los datos en la ruta de almacenamiento, activara la transmisión de imágenes para la visualización en el centro de monitoreo.

Si el Modo Alarma es activado el sistema trabaja en modo Monitoreo y Alarma, las primeras estradas son establecer la ruta de almacenamiento, dirección de correo electrónico, número de teléfono celular y dos variables (opción, cont.) para las opciones en la llamada y reintentos de llamada respectivamente. Luego el procedimiento de activar la detección de movimiento, si se detecta movimiento almacenara los datos, activa la visualización, envía correo y mensaje. Ejecuta la llamada, si es contestada presenta las opciones (reiniciar, desactivar) y apaga la sirena, sino reintenta la llamada una vez más si no contesta apaga la sirena finaliza.



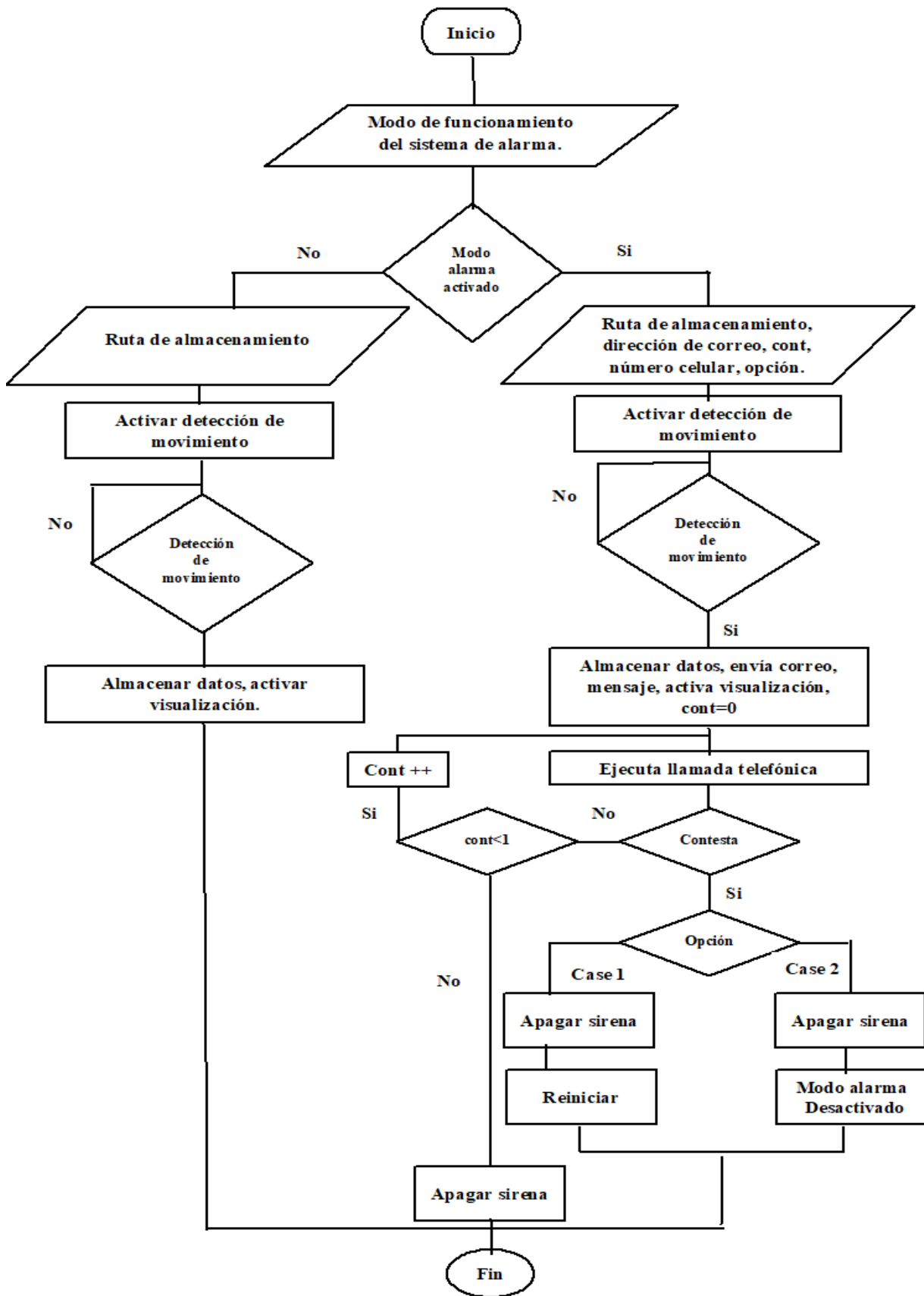


Figura 19. Diagrama de flujo del sistema.

Fuente: Elaborado por el autor.

### **3.4.4 Medios de transmisión**

Para la transferencia de datos en el sistema de video vigilancia y alarma basado en detección de movimiento, se utiliza los siguientes medios de transmisión:

#### **3.4.4.1 Cable USB**

Se utiliza cable USB 2.0 para la conexión de las cámaras web con el Raspberry, si la distancia es mayor a cinco metros se utilizará una extensión de cable USB activo, comercialmente estos cables vienen de fábrica en medidas de 10m, 15m, 20m y 30m. Este cableado permitirá la transferencia de información generada por las cámaras web es decir la transmisión de la captura de video e imágenes.

#### **3.4.4.2 Cable de par trenzado**

Este tipo de cableado se utiliza en caso de tener una cámara IP que no cuente con características inalámbricas, en este proyecto se utilizó un Patch cord para la configuración inicial del Raspberry Pi 3.

#### **3.4.4.3 Transmisión inalámbrica**

Por este medio se realiza la comunicación y transferencia hacia el centro de monitoreo local usando el estándar WiFi b/g/n, también la conexión a de la tarjeta inalámbrica del Raspberry PI utiliza este medio de transmisión.

### **3.4.5 Dispositivo de almacenamiento del sistema**

#### **3.4.5.1 Dimensionamiento**

Se considera:

**Tabla 23. Consideraciones para el dimensionamiento del Disco Externo.**

<b>Número de cámaras web</b>	<b>4</b>
<b>Número de horas al día que está registrando datos</b>	24 horas
<b>Resolución de la imagen</b>	640 x 480
<b>Tipo de compresión de la imagen</b>	JPEG

Fuente: Elaboración propia.

Almacenamiento por hora

Capacidad/hora= Tamaño\_imagen\*Número\_imagenes

$$\text{Capacidad/hora} = \frac{22 \text{ KB}}{\text{Tamaño\_imagen}} \times \frac{2 \text{ imagenes}}{\text{segundos}} \times \frac{3600 \text{ segundos}}{\text{hora}}$$

Capacidad/hora= 158,4 MB/hora

Almacenamiento por día.

$$\frac{\text{Capacidad}}{\text{día}} = \frac{\text{Capacidad}}{\text{hora}} \times 24 \text{ horas}$$

$$\frac{\text{Capacidad}}{\text{día}} = \frac{158,4 \text{ MB}}{\text{hora}} \times 24 \text{ horas}$$

Capacidad/día= 3,8016 GB/día

Almacenamiento Total del sistema por día

**Tabla 24. Almacenamiento por día**

Cámaras Web	Horas De Grabación	MB/Hora	GB/Hora	Total, por Cámaras (Gb)
<b>CAM1</b>	24	158,4	0,1584	3,8016
<b>CAM2</b>	24	158,4	0,1584	3,8016
<b>CAM3</b>	24	158,4	0,1584	3,8016
<b>CAM4</b>	24	158,4	0,1584	3,8016
Almacenamiento Total del sistema por día				15,2064

Fuente: Elaboración propia.

### 3.4.5.2 Elección del dispositivo

El sistema cuenta con un disco de 1 TeraByte (TB), se concluye que el tiempo disponible para una grabación continua es de 67 días; si se sobrepasa éste tiempo, la grabación se realizará en la tarjeta Raspberry Pi, produciendo la saturación de memoria, es decir, el sistema deja de funcionar; entonces se recomienda descargar la información cada 30 días.

### 3.4.6 Diseño de red para el sistema

#### 3.4.6.1 Tabla de direccionamiento

Tabla 25. Tabla de direccionamiento del sistema.

Dispositivo	Dirección IP	Mascara Red	de Dirección de difusión	Gateway
<b>Raspberry Pi 3</b>	192.168.1.12	255.255.255.192	192.168.1.63	192.168.1.1
<b>Cámara web 1</b>	192.168.1.12:8081	255.255.255.192	192.168.1.63	192.168.1.1
<b>Cámara web 2</b>	192.168.1.12:8082	255.255.255.192	192.168.1.63	192.168.1.1
<b>Cámara web 3</b>	192.168.1.12:8083	255.255.255.192	192.168.1.63	192.168.1.1
<b>Cámara web 4</b>	192.168.1.12:8084	255.255.255.192	192.168.1.63	192.168.1.1
<b>Monitoreo</b>	192.168.1.13	255.255.255.192	192.168.1.63	192.168.1.1

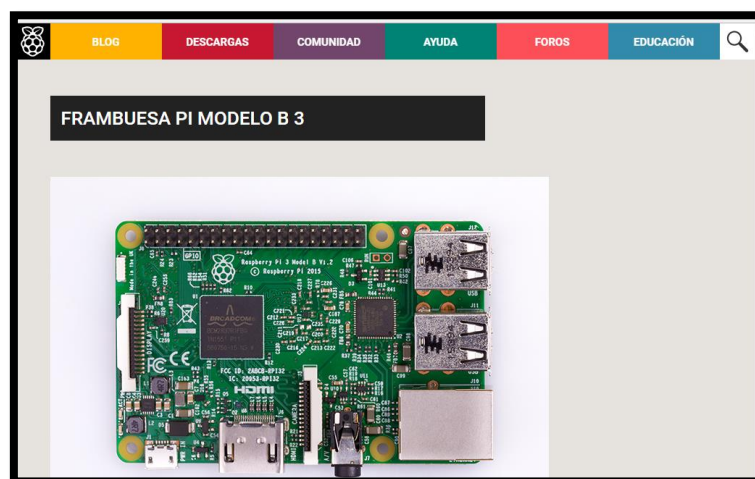
Fuente: Elaboración propia.

## 3.5 Diseño del sistema de video vigilancia

### 3.5.1 Instalación del sistema operativo

El sistema operativo Raspbian está diseñado para las placas Raspberry, siendo un sistema versátil, estable y confiable el cual permite desarrollar múltiples aplicaciones, bajo este sistema operativo funciona el sistema de video vigilancia y alarma basada en la detección de movimiento. Para la instalación del sistema operativo en la Raspberry Pi 3 es necesario una tarjeta micro sd de mínimo 4Gb, para este proyecto se utilizó una tarjeta micro sd de 16 Gb clase 10 para obtener mayor velocidad en la transmisión de datos.

- **Descargar la imagen del sistema operativo**



**Figura 20. Página oficial de Raspberry Pi.**  
**Fuente:** *Captura de pantalla (www.raspberrypi.org).*

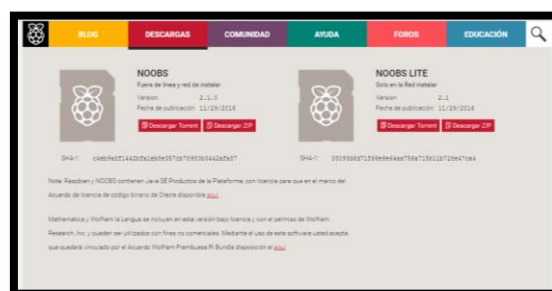
Para descargar el sistema operativo entramos en la página oficial de Raspberry Pi <http://www.raspberrypi.org> y vamos a la sección de descargas como se muestra en la figura 21, tenemos dos opciones NOOBS y Raspbian, se eligió NOOBS para este proyecto por ser una herramienta de asistencia para la instalación de Raspbian y otros sistemas operativos.



**Figura 21. Descargas de Raspbian.**

*Fuente: Captura de pantalla (www.raspberrypi.org).*

Dentro de NOOBS tenemos dos opciones NOOBS asistente de instalación sin conexión a internet y NOOBS LITE asistente de instalación con conexión a internet. Elegimos NOOBS y damos a “Download ZIP”. El cual contiene la última versión que es la Debían Jessie del 29 de noviembre de 2016. Una vez descargado el ZIP, hay que descomprimirlo para obtener el fichero con extensión .img que está dentro.

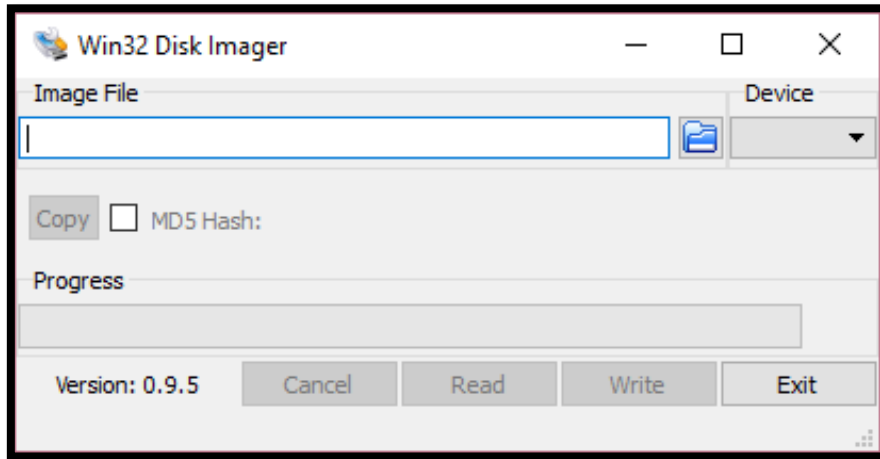


**Figura 22. Selección de NOOBS OFFLINE.**

*Fuente: Captura de pantalla (www.raspberrypi.org).*

Una vez obtenida la imagen del sistema operativo se procede a descomprimirla en nuestro computador, se realizó la copia de la imagen del sistema operativo Raspbian a la tarjeta de memoria micro sd de 16 Gb clase 10, se debe formatear la tarjeta micro sd de forma que sea

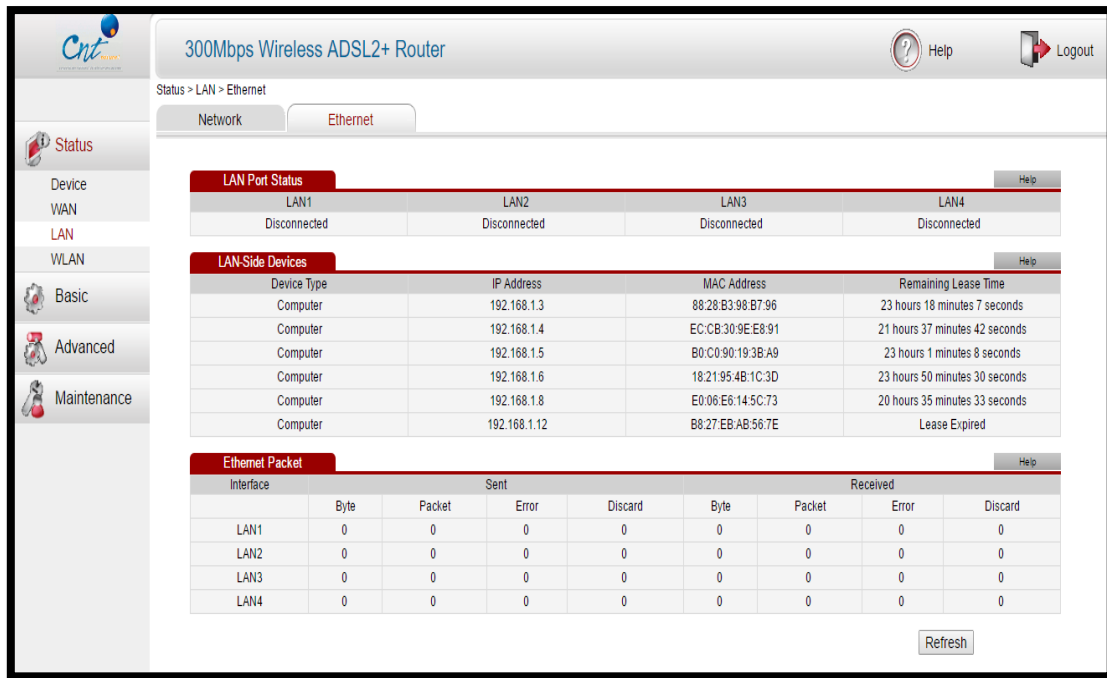
booteable para lo cual se usó el programa Win32DiskImage en en Windows, se puede realizar este proceso con otros softwares similares.



**Figura 23. Interfaz de Win32 Disk Imager.**  
*Fuente: Captura de pantalla software Win32 Disk Imager.*

Cuando el proceso de copiado de la imagen del sistema operativo a la tarjeta micro sd finalice, se debe introducir la tarjeta micro sd en la ranura del Raspberry PI 3, conectamos el equipo a la fuente de energía que debe ser de 2.5 amperios según recomienda el fabricante, una vez conectada la fuente arranca el sistema, si se cuenta con un monitor, teclado y mouse se podrá ver directamente el arranque en el monitor y configurar desde el mismo equipo, caso contrario el sistema operativo arranca con el servicio de ssh activado en el minicomputador.

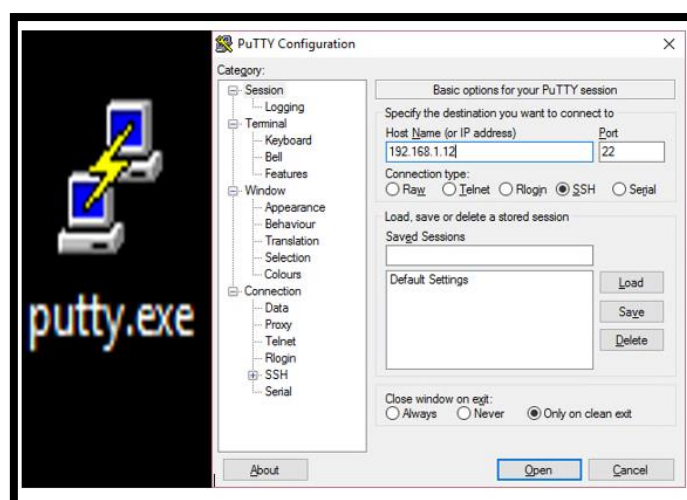
Para conectarnos mediante el servicio ssh al minicomputador debemos conectarlo mediante un cable ethernet a un router y obtener la dirección IP del equipo en la página de administración del router, se puede ver un ejemplo en la figura 24.



**Figura 24. Interfaz de router huawei CNT.**

*Fuente: Captura de pantalla.*

Podemos conectarnos con la ayuda del cliente de conexión ssh PuTTY lo configuramos usando la dirección IP del minicomputador que obtuvimos con anterioridad y la opción SSH con el puerto 22, ahora se conecta remotamente por el servicio SSH al Raspberry Pi, tan sólo tendremos que pulsar sobre Open.

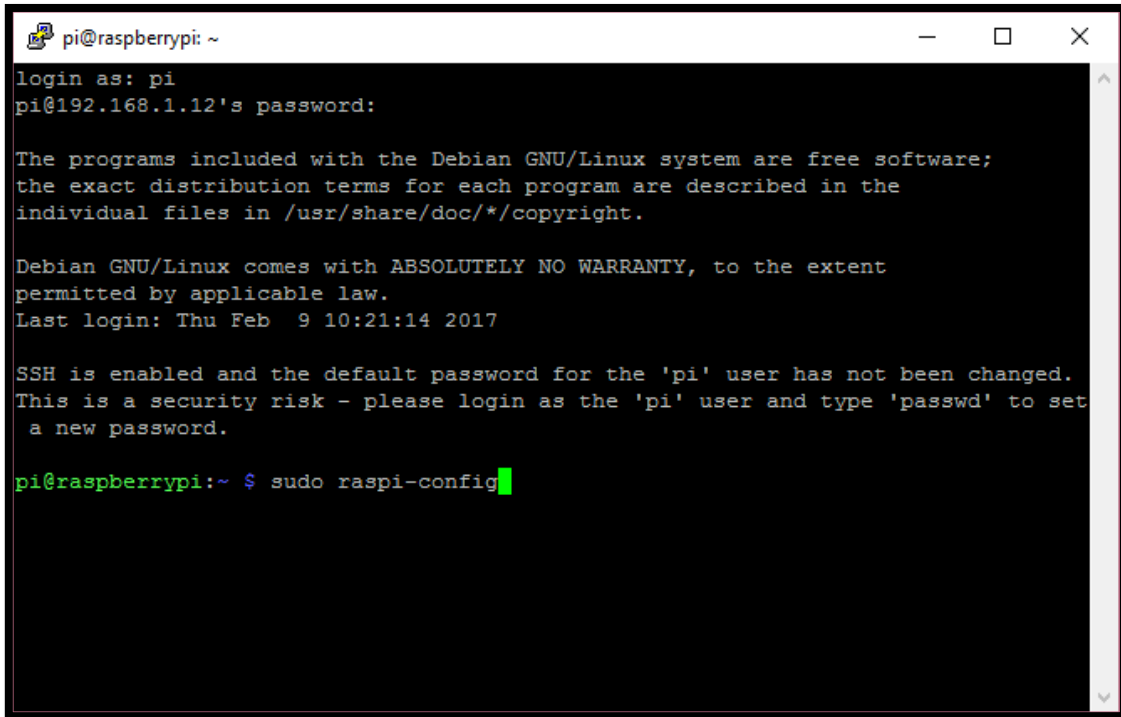


**Figura 25. Interfaz de Putty.**

*Fuente: Captura de pantalla software Putty.*



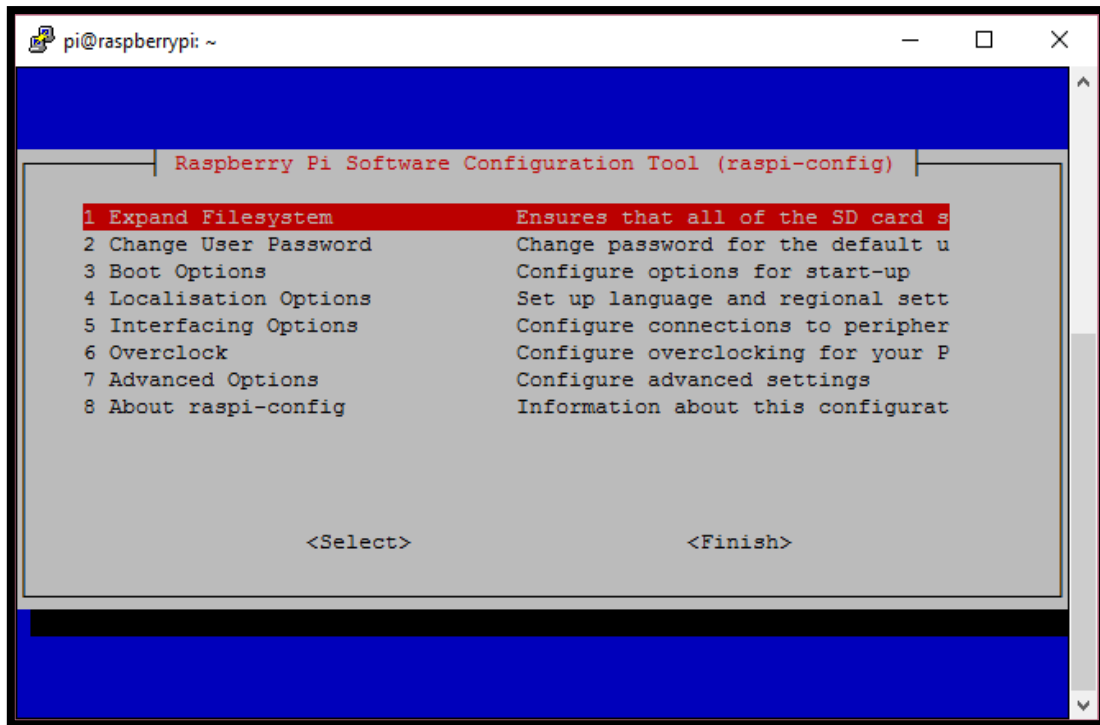
Se abre un terminal en donde iniciaremos una sesión introduciendo el usuario pi y la contraseña raspberry que vienen como usuario por defecto. Seguidamente introducimos este comando en el terminal: **sudo raspi-config**



```
pi@raspberrypi: ~  
login as: pi  
pi@192.168.1.12's password:  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Thu Feb  9 10:21:14 2017  
  
SSH is enabled and the default password for the 'pi' user has not been changed.  
This is a security risk - please login as the 'pi' user and type 'passwd' to set  
a new password.  
  
pi@raspberrypi:~ $ sudo raspi-config
```

**Figura 26. Acceso SSH con Putty.**  
*Fuente: Captura de pantalla terminal Raspbian.*

Utilizando este comando se desplegará un menú en el terminal con distintas opciones, es prácticamente obligatorio extender la partición root de esta forma se usa todo el espacio de nuestra tarjeta micro sd, es conveniente cambiar la contraseña, configurar el layout del teclado a español y la zona horaria para acoplarlas a nuestro horario. El resto de opciones es conveniente dejarlas por defecto si no se sabe configurarlas adecuadamente en especial mención a las opciones de overclock, la cual es mejor no tocar si no se sabe lo que se está haciendo ya que podríamos dañar el Raspberry PI 3.



**Figura 27. Asistente de configuración Raspbian.**

*Fuente: Captura de pantalla.*

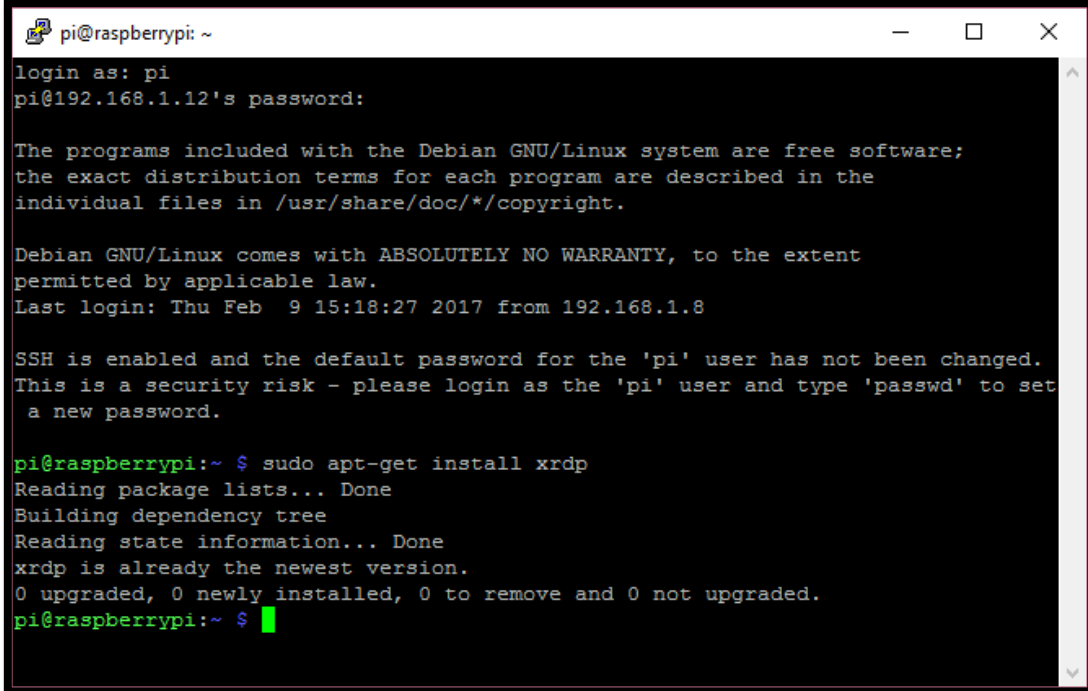
Realizados los pasos correctamente en el asistente raspi-config, se logró tener configurada la distribución Raspbian Jessie en Raspberry Pi 3. En el proceso final se desconectará el cliente ssh. Para la configuración del sistema de video vigilancia y alarma basada en la detección de movimiento es necesaria una administración local la cual se logró mediante la instalación de un agente de conexión a escritorio remoto que proporciona conexiones funcionales entre sistemas operativos basados tanto en Linux como en Windows y obtiene acceso al entorno grafico de escritorio en el sistema operativo Raspbian.

Se inicia una sesión mediante ssh con el minicomputador para instalar los servicios de conexión remota, siguiendo los pasos anteriores se consigue conexión mediante el usuario pi y la contraseña actual.

### 3.5.1.1 Administración local

- Instalación de XRDP para entornos Windows.

Una vez iniciada la sesión en el terminal mediante ssh, para instalar el software XRDP el cual proporciona conexiones a escritorio remoto entre Windows y Linux mediante una interfaz gráfica si necesidad de instalar un cliente de conexión remota en Windows además del que viene por defecto, se debe digitar el siguiente comando: **sudo apt -get install xrdp**, como se muestra en la figura 28.



```
pi@raspberrypi: ~
login as: pi
pi@192.168.1.12's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

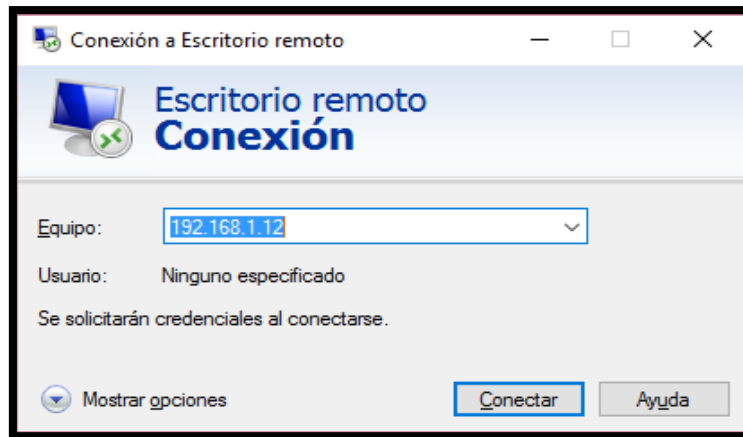
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Feb  9 15:18:27 2017 from 192.168.1.8

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set
a new password.

pi@raspberrypi:~ $ sudo apt-get install xrdp
Reading package lists... Done
Building dependency tree
Reading state information... Done
xrdp is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
pi@raspberrypi:~ $
```

**Figura 28. Instalacion de XRDP.**  
*Fuente: Captura de pantalla.*

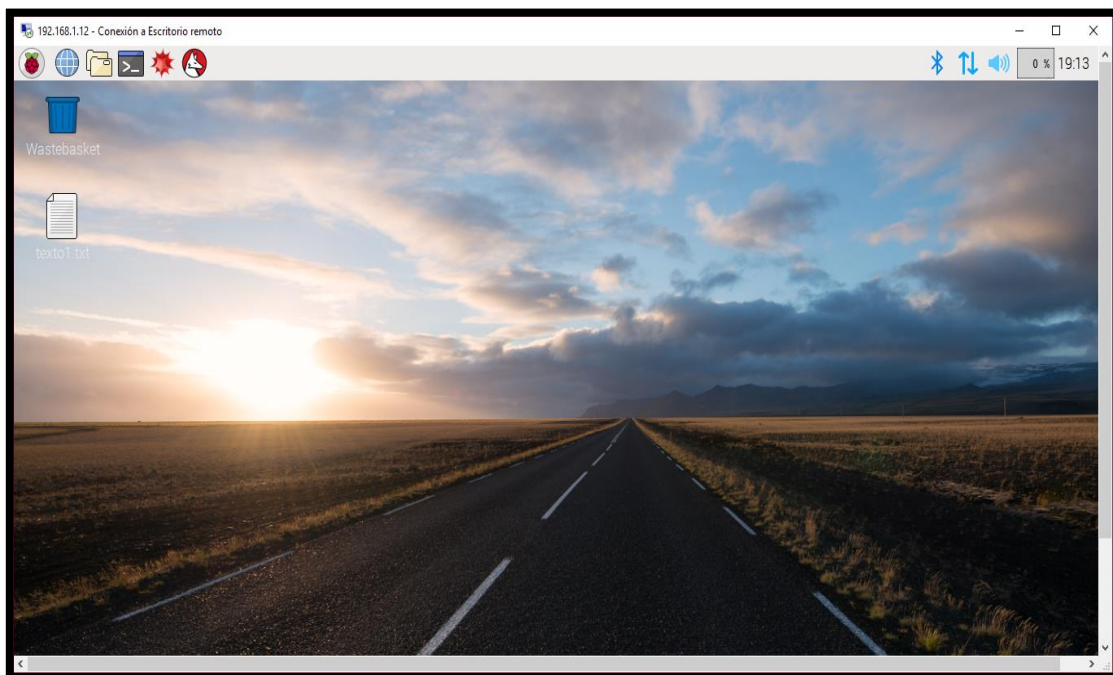
Para acceder al sistema operativo Raspbian por conexión a escritorio remoto desde Windows, solo se necesita acceder a Inicio > Conexión a Escritorio Remoto > e ingresar la IP 192.168.1.12, el usuario y la contraseña.



**Figura 29. Interfaz de conexión a escritorio remoto en Windows.**

*Fuente: Captura de pantalla.*

Pulsamos en conectar y se mostrará el cuadro de dialogo para el inicio de sesión en el entorno XRDP en donde introduciremos el usuario y la contraseña correspondiente para el acceso, presionamos la tecla entrar o pulsamos en ok y el gestor de inicio de sesión sesman comenzará a autenticar. Si la contraseña y usuario son correctas se mostrará el entorno gráfico como se muestra en la figura 30.



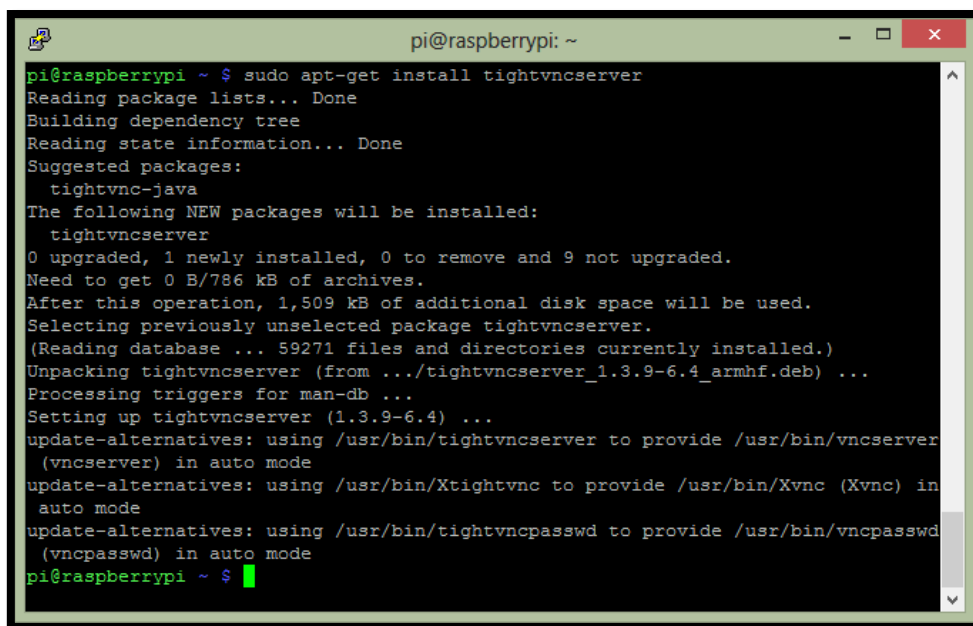
**Figura 30. Entorno grafico de Raspbian conexión desde Windows.**

*Fuente: Captura de pantalla.*

- Instalación de VNC para entornos Linux y Windows.

Es una aplicación para conectarnos al escritorio remotamente, VNC (Virtual Network Computing) que es un software usado por administradores de red y para este proyecto se usa como administración local en forma de aplicación cliente-servidor. Primero se necesita instalar el servidor VNC en el Raspberry Pi, este se encarga de cargar el escritorio remoto. Para esto se ingresa a la terminal del Raspberry Pi 3 a través de SSH usando Putty.

Una vez ha ingresado a la terminal procederemos a instalar `tightvncserver` que es el software que permitirá la conexión al escritorio remoto, se debe digitar el siguiente comando en el terminal: **`sudo apt-get install tightvncserver`**. Se puede ver un ejemplo en la figura 31.

A screenshot of a terminal window titled 'pi@raspberrypi: ~'. The terminal shows the command 'sudo apt-get install tightvncserver' being executed. The output includes: 'Reading package lists... Done', 'Building dependency tree', 'Reading state information... Done', 'Suggested packages: tightvnc-java', 'The following NEW packages will be installed: tightvncserver', '0 upgraded, 1 newly installed, 0 to remove and 9 not upgraded.', 'Need to get 0 B/786 kB of archives.', 'After this operation, 1,509 kB of additional disk space will be used.', 'Selecting previously unselected package tightvncserver.', '(Reading database ... 59271 files and directories currently installed.)', 'Unpacking tightvncserver (from ../tightvncserver\_1.3.9-6.4\_armhf.deb) ...', 'Processing triggers for man-db ...', 'Setting up tightvncserver (1.3.9-6.4) ...', 'update-alternatives: using /usr/bin/tightvncserver to provide /usr/bin/vncserver (vncserver) in auto mode', 'update-alternatives: using /usr/bin/Xtightvnc to provide /usr/bin/Xvnc (Xvnc) in auto mode', 'update-alternatives: using /usr/bin/tightvncpasswd to provide /usr/bin/vncpasswd (vncpasswd) in auto mode', and finally 'pi@raspberrypi ~ \$' with a green cursor.

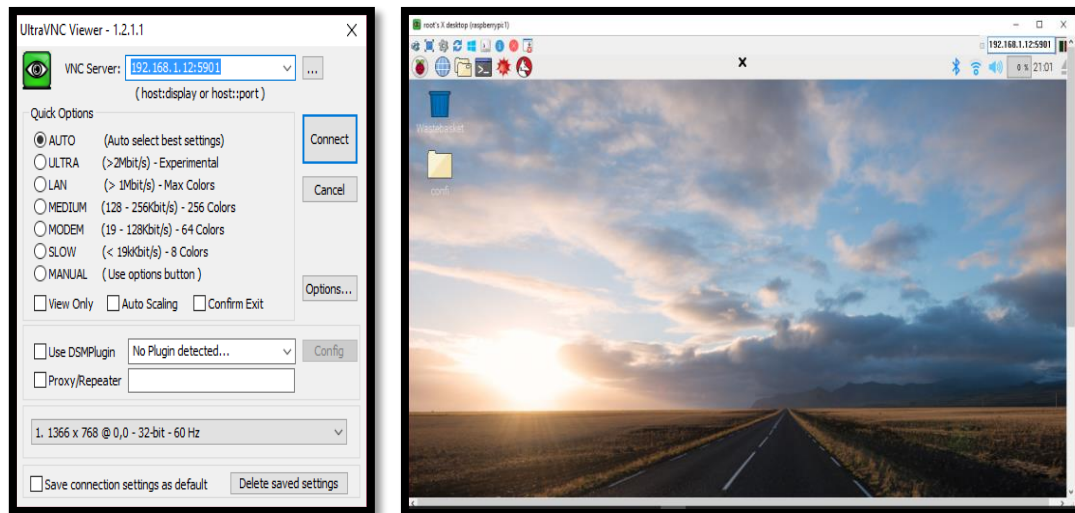
```
pi@raspberrypi ~ $ sudo apt-get install tightvncserver
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  tightvnc-java
The following NEW packages will be installed:
  tightvncserver
0 upgraded, 1 newly installed, 0 to remove and 9 not upgraded.
Need to get 0 B/786 kB of archives.
After this operation, 1,509 kB of additional disk space will be used.
Selecting previously unselected package tightvncserver.
(Reading database ... 59271 files and directories currently installed.)
Unpacking tightvncserver (from ../tightvncserver_1.3.9-6.4_armhf.deb) ...
Processing triggers for man-db ...
Setting up tightvncserver (1.3.9-6.4) ...
update-alternatives: using /usr/bin/tightvncserver to provide /usr/bin/vncserver
(vncserver) in auto mode
update-alternatives: using /usr/bin/Xtightvnc to provide /usr/bin/Xvnc (Xvnc) in
auto mode
update-alternatives: using /usr/bin/tightvncpasswd to provide /usr/bin/vncpasswd
(vncpasswd) in auto mode
pi@raspberrypi ~ $
```

**Figura 31. Instalacion de servidor VNC.**

*Fuente: Captura de pantalla.*

Lo siguiente es iniciar el servicio de VNC, se inicia el servicio digitando en la terminal el comando: **`sudo tightvncserver`**. Al ejecutar este comando se pedirá que registremos una contraseña para el acceso remoto al escritorio, es conveniente se ponga la misma contraseña del usuario actual. Ahora, se puede iniciar una conexión desde un computador, portátil, tableta

o Smartphone. Se puede conectarte sin problemas apuntando a la dirección IP del Raspberry Pi 3 más el puerto 5901 que utiliza el servidor. En la siguiente figura 32 se muestra el acceso a escritorio remoto mediante la aplicación Ultravncviewer.



**Figura 32. Interconexión desde Linux a Raspbian.**

*Fuente: Captura de pantalla*

Para que el servicio de VNC arranque con cada inicio del Raspberry Pi 3 se añade la siguiente línea: **su -c "/usr/bin/tightvncserver -geometry 1280x1024" pi/root** en el fichero **/etc/rc.local**, podemos probarlo haciendo: **sudo nano /etc/rc.local**. Se debe editarlo como se muestra en la figura 33.

```

# /bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
#
# Print the IP address
_IP=$(hostname -I) || true
if [ "$_IP" ]; then
  printf "My IP address is %s\n" "$_IP"
fi
su -c "/usr/bin/tightvncserver -geometry 1280x1024" root
/usr/local/bin/bluetoothd --experimental &
sh /usr/local/bin/inicioapps.sh
exit 0

```

**Figura 33. Fichero rc.local.**

*Fuente: Captura de pantalla.*

Una vez instalados los gestores para la administración local del sistema se debe actualizar los repositorios y el sistema Raspbian, accediendo al entorno grafico por una de las dos opciones de conexión a escritorio remoto en Linux o Windows, una ventana de terminal y se introduce el siguiente comando: `sudo apt-get update && sudo apt-get upgrade` este proceso tardará unos minutos, al finalizar Raspbian estará listo para configurar dentro de él un sistema de video vigilancia y alarma basado en detección de movimiento.

### 3.5.1.2 Administración remota

Para la administración remota se instaló la aplicación Weaved la cual pertenece a una plataforma de desarrollo para aplicaciones de internet de las cosas (IoT) remot3.it, esta tiene como objetivo el manejo remoto de dispositivos desde cualquier lugar. Se creó una cuenta para acceder a los servicios de esta plataforma y administrar el sistema remotamente. La cuenta es gratuita y se crea siguiendo estos pasos:

**Tabla 26. Pasos para crear una cuenta en Weaved IoT.**

<b>Paso número:</b>	<b>Acción</b>
<b>Paso número 1</b>	Ingresar al sitio oficial en la página web de la aplicación para internet de las cosas (IoT) <a href="https://developer.weaved.com/portal/index.php">https://developer.weaved.com/portal/index.php</a> .
<b>Paso número 2</b>	Ingresar un nombre, correo y contraseña.
<b>Paso número 3</b>	Pulsar en “Sign Up”

---

**Paso número 4**

Para ingresar a Weaved se debe introducir el email y el password de la cuenta.

---

**Paso número 5**

Al finalizar dar clic en “Sign In”

---

Fuente: Elaboración propia.

**Figura 34. Interfaz de registro en Weaved IoT.**

*Fuente: Captura de pantalla.*

En el Raspberry Pi 3 se debe instalar el kit de IoT de Weaved el cual permite el acceso al sistema remotamente mediante esta plataforma de Internet de las Cosas en una solución fácil de usar, de modo la conexión remota se puede realizar desde cualquier navegador o un teléfono inteligente. Esta plataforma cuenta también con la aplicación gratuita para iOS y Android.

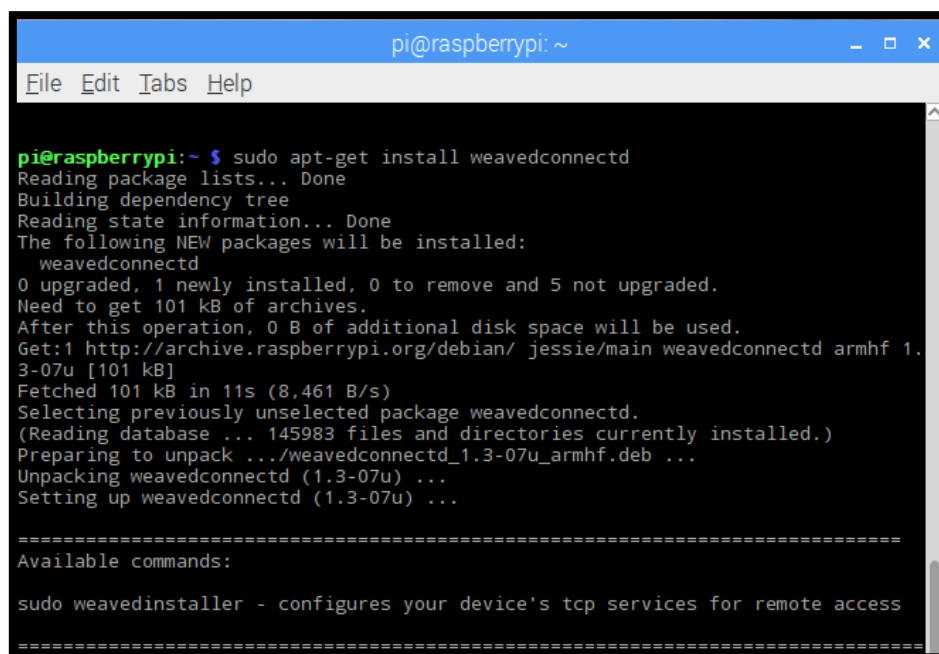
Los servicios de Weaved son accesibles y se conectan fácilmente y de forma segura al Raspberry Pi 3 desde una ventana de aplicación o navegador móvil. Se puede controlar el



minicomputador de forma remota utilizando puertos TCP como ejemplo, ssh (terminal remota) y VNC (Virtual Network Console).

- Instalación del kit Weaved en Raspberry Pi 3

Para descargar el kit Weaved, desde el Raspberry conectado a Internet se abre una ventana de terminal en donde se ingresa el siguiente comando: **sudo apt-get update && sudo apt-get install weavedconnectd** se puede observar esto en la figura 35.



```

pi@raspberrypi: ~
File Edit Tabs Help

pi@raspberrypi:~$ sudo apt-get install weavedconnectd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  weavedconnectd
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 101 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://archive.raspberrypi.org/debian/ jessie/main weavedconnectd armhf 1.3-07u [101 kB]
Fetched 101 kB in 11s (8,461 B/s)
Selecting previously unselected package weavedconnectd.
(Reading database ... 145983 files and directories currently installed.)
Preparing to unpack ../weavedconnectd_1.3-07u_armhf.deb ...
Unpacking weavedconnectd (1.3-07u) ...
Setting up weavedconnectd (1.3-07u) ...

=====
Available commands:

sudo weavedinstaller - configures your device's tcp services for remote access
=====

```

**Figura 35. Instalacion de kit Weaved IoT.**

*Fuente: Captura de pantalla.*

Una vez que finalice la descarga e instalación del kit Weaved, podemos iniciar el asistente para agregar los servicios de conexión remota utilizando el comando: **sudo weavedinstaller**, se desplegará un menú en donde seleccionamos la opción 1 para ingresar a nuestra cuenta creada anteriormente y comenzar a agregar los servicios en Weaved.

```

pi@raspberrypi:~ $ sudo weavedinstaller
remot3.it connection installer Version: v1.3-07_Pi lib_v1.3-07_Pi
Modified: August 22, 2016 (library) November 08, 2016

Checking your network for compatibility...

Your network is compatible with remot3.it services.

***** Sign In Menu *****

    1) Sign in to your existing remot3.it account
    2) Request a code for a new remot3.it account
    3) Enter a verification code received in e-mail
    4) Exit

*****

    Use your Weaved account with remot3.it!
*****

Please select from the above options (1-4):

```

**Figura 36. Interfaz de Weaved en terminal.**

*Fuente: Captura de pantalla.*

Eligiendo la opción 1 ingresamos como usuario el correo electrónico con el que creamos la cuenta y la contraseña, cuando ingresamos por primera vez nos pedirá que demos un nombre para el dispositivo como se muestra en la figura 37.

```

*****

    Use your Weaved account with remot3.it!
*****

Please select from the above options (1-4):
1
Please enter your remot3.it Username (e-mail address):
cristfutnw3.a@gmail.com

Please enter your remot3.it password:
.....

Enter a name for your device (e.g. my_Pi_001).

The Device Name identifies your device in the remot3.it portal.
Your services will be grouped under the Device Name.

Only letters, numbers, underscore, space and dash are allowed.
scdosmil
.
Registering scdosmil.....

```

**Figura 37. Registro de Nombre de dispositivo en Weaved.**

*Fuente: Captura de pantalla.*

Finalizado el registro del nombre del dispositivo se desplegará la información del dispositivo y las aplicaciones creadas para acceso remoto, debajo estará un menú para agregar los servicios y borrarlos. Se elige 1 para agregar los servicios del sistema.

```
Updating /etc/weaved/services/Weavedrmt365535.conf
.
===== Installed remot3.it Services =====
Protocol      Port      Service      remot3.it Service Name
-----
Device Name: scdosmil
=====
***** Main Menu *****

  1) Attach/reinstall remot3.it to a Service
  2) Remove remot3.it attachment from a Service
  3) Remove all remot3.it attachments, then exit
  4) Exit

*****

Please select from the above options (1-4):
1
```

**Figura 38.** Menú de activación de servicio en Weaved.

*Fuente: Captura de pantalla.*

Se muestra un menú con opciones para agregar servicios por defecto como conexión SSH, Web, VNC y una opción para agregar aplicaciones en puertos TCP diferentes a las anteriores.

```
===== Installed remot3.it Services =====
Protocol      Port      Service      remot3.it Service Name
-----
Device Name: scdosmil
=====
***** Protocol Selection Menu *****

  1) SSH on port 22
  2) Web (HTTP) on port 80
  3) VNC on port 5901
  4) Custom (TCP)
  5) Return to previous menu

*****

You can change the port value during install
*****

Please select from the above options (1-5):

```

**Figura 39.** Menú de servicios por defecto en Weaved.

*Fuente: Captura de pantalla.*

Activamos los servicios SSH, VNC y Web insertando en el terminal el número de la opción correspondiente, nos pedirá la identificación del protocolo y el número de puerto interno con el cual trabaja la aplicación que deseamos conectar remotamente, también nos pedirá un nombre para identificar la aplicación.

```

*****
You can change the port value during install
*****
Please select from the above options (1-5):
2
You have selected: 2.
The default port for Web (http) is 80.
Would you like to continue with the default port assignment? [y/n] n
Please enter your desired port number (1-65535):8080
We will attach a remot3.it connection to the following service:

Protocol: web
Port #: 8080
.....
Enter a name for this remot3.it service (e.g. SSH-Pi).
This name will be shown in your remot3.it Service List.
Only letters, numbers, underscore, space and dash are allowed.
scweb-pi:

```

**Figura 40. Registro de un servicio en Weaved.**

*Fuente: Captura de pantalla.*

De esta forma agregamos los servicios de conexión remota XRDP en el puerto 3389, VNC en el puerto 5901, Web para las cámaras cam1 con el puerto 8081, cam2 con el puerto 8082, cam3 con el puerto 8083, cam4 con el puerto 8084, cam5 con el puerto 8085 y pagina web de presentación y visualización scweb-pi en el puerto 8080.

```

===== Installed remot3.it Services =====
Protocol      Port      Service      remot3.it Service Name
-----
TCP           3389     xrdp         xrdp-pi
VNC           5901     WARNING-NONE vnc-pi
HTTP          8888     WARNING-NONE webcontrolsc-pi
HTTP          8081     WARNING-NONE cam1-pi
HTTP          8082     WARNING-NONE cam2-pi
HTTP          8080     WARNING-NONE scweb-pi
HTTP          8083     WARNING-NONE cam3-pi
HTTP          8084     WARNING-NONE cam4-pi
-----
Device Name: scdosmil
=====

```

**Figura 41. Servicios Activados en Weaved Iot.**

*Fuente: Captura de pantalla.*

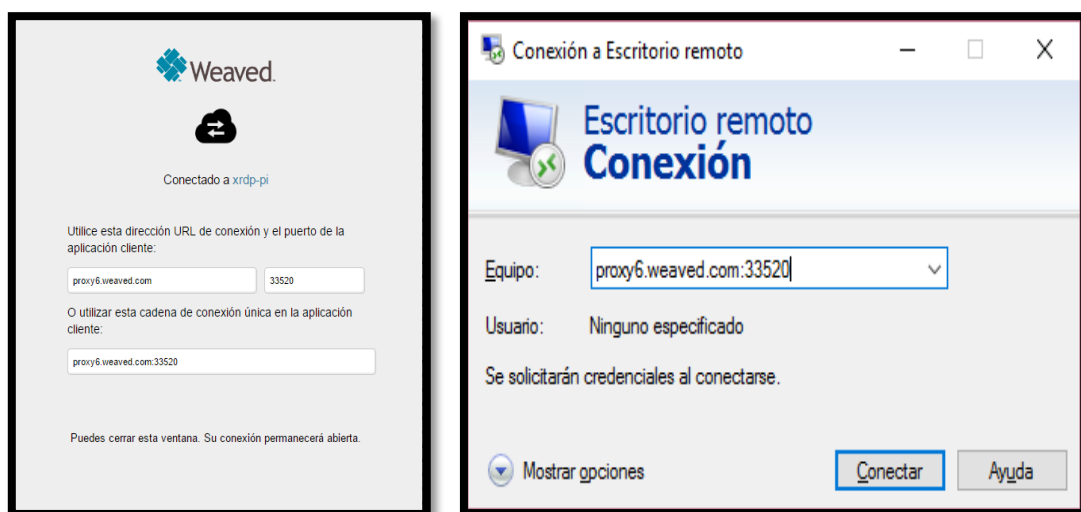
Para comprobar la funcionalidad ingresamos a nuestra cuenta de Weaved y verificamos los servicios que tenemos configurados y conectados en línea, seleccionamos XRDP y la plataforma no devolverá una cadena de caracteres a manera de un socket (host:puerto) el cual podremos ingresar en cliente de conexión a escritorio remoto para la administración remota del sistema, de la misma forma se puede realizar con el servicio VNC.

Nombre	Tipo	Estado	
cam1-pi	HTTP	en línea	Compartir   ajustes
CAM2-pi	HTTP	en línea	Compartir   ajustes
cam3-pi	HTTP	en línea	Compartir   ajustes
cam4-pi	HTTP	en línea	Compartir   ajustes
scweb-pi	HTTP	en línea	Compartir   ajustes
thvnc-pi	TCP genérico	en línea	Compartir   ajustes
VNC-pi	VNC	en línea	Compartir   ajustes
webcontrolsc-pi	HTTP	en línea	Compartir   ajustes
xrdp-pi	TCP genérico	en línea	Compartir   ajustes

**Figura 42. Vista de servicios desde la cuenta Weaved mediante navegador web.**

*Fuente: Captura de pantalla.*

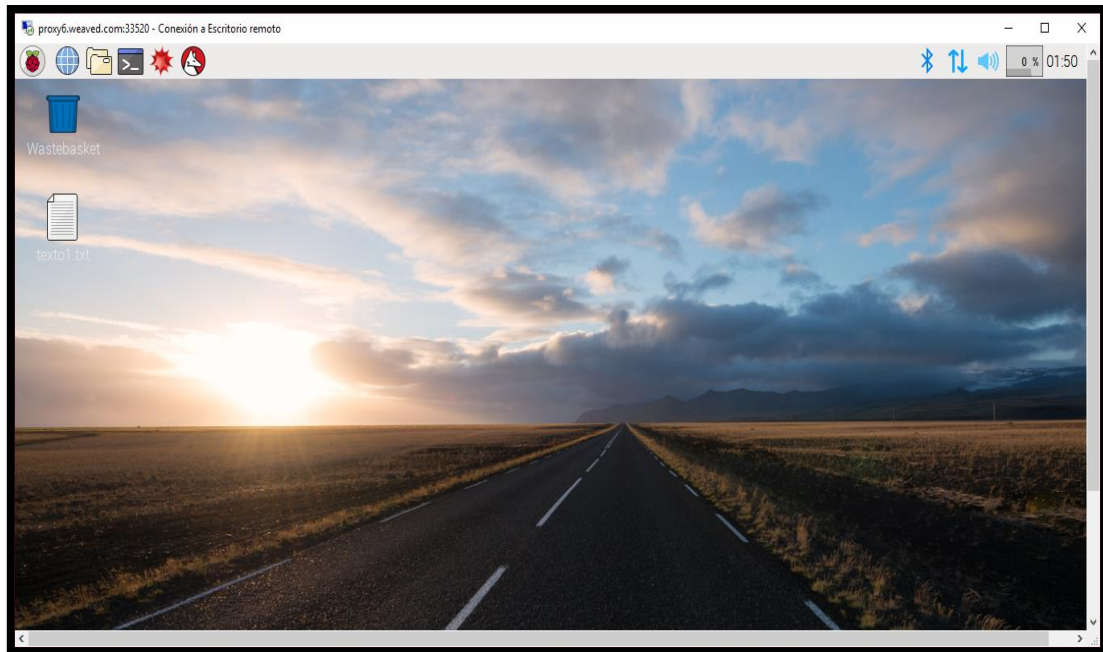
En la figura 43 se muestra el proceso para la conexión a escritorio remoto utilizando la aplicación Weaved IoT.



**Figura 43. Conexión mediante Weaved a escritorio remoto en Raspbian.**

*Fuente: Captura de pantalla.*

Ingresando el usuario y contraseña se mostrará el entorno gráfico del sistema como se muestra en la figura 44.

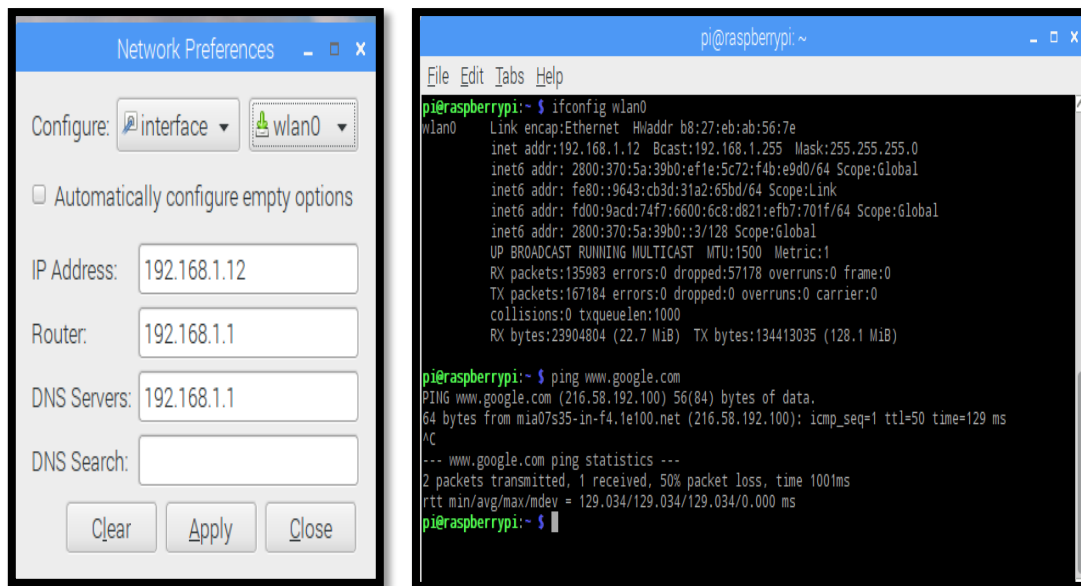


**Figura 44. Interfaz gráfica de Raspbian mediante servicio de Weaved IoT.**

*Fuente: Captura de pantalla.*

### 3.5.2 Instalación del software Motion

Antes de empezar se debe configurar la tarjeta inalámbrica del Raspberry Pi 3 con una dirección IP estática se puede hacer de manera gráfica o editando el fichero en `/etc/network/interfaces` y reiniciar los servicios de red con el comando **sudo service networking restart**, también reiniciar el minicomputador con **sudo reboot**. Comprobamos los cambios con el comando **ifconfig wan0**, si los cambios dieron efecto realizaremos un ping a [www.google.com](http://www.google.com) para verificar la conexión a internet.



**Figura 45. Configuración de interfaz wlan0 con IP estática.**  
*Fuente: Captura de pantalla.*

- Instalación de Motion

El software se encuentra dentro de los repositorios de Raspbian por lo tanto puede ser instalado fácilmente desde el gestor de paquetes o usando un comando a través del terminal para instalarlo. Pero antes de iniciar la instalación de Motion primero se debe ejecutar los siguientes comandos:

```
sudo apt-get update && sudo apt-get upgrade
```

El comando **sudo apt-get update** hace que se actualicen los repositorios; mientras que **sudo apt-get upgrade** permite la actualización de los programas instalados.

Para la instalación de Motion se digita en la terminal el comando:

```
sudo apt-get install motion.
```

Para configurar el software se debe editar el fichero de configuración que se encuentra en: `/etc/motion/motion.conf`, dentro de este fichero se ingresa la información general para el

comportamiento de gestor de cámaras Motion posteriormente se debe crear y configurar un fichero por cada cámara que se incluya al sistema, a estos ficheros de configuración individual se les denomina threads y contienen información específica de cada cámara.

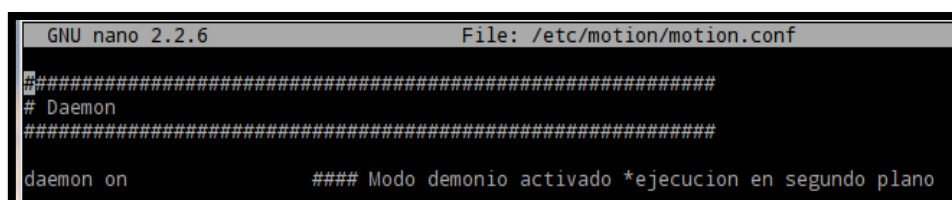
Con el comando **sudo nano /etc/motion/motion.conf** conseguimos editarlo con el siguiente contenido:

- Configuración general del software Motion:

Dentro del fichero de configuración general motion.conf se encuentran muchas opciones las cuales podemos usar para distintas aplicaciones, para este sistema editaremos algunas secciones de este fichero para que el software funcione con las características que este sistema necesita.

La primera sección es para definir el modo de funcionamiento del demonio que inicializa el software, se define en encendido.

daemon on → Para que se inicie en modo demonio (trabaja segundo plano), para las primeras pruebas es recomendable configurarlo en modo “off”, para ver la ejecución del programa en el terminal. En modo off y ejecutando el comando **sudo motion -n** veremos como el software carga los ficheros y prueba las configuraciones indicando si funcionan correctamente.



```
GNU nano 2.2.6 File: /etc/motion/motion.conf
#####
# Daemon
#####
daemon on          ### Modo demonio activado *ejecucion en segundo plano
```

**Figura 46. Fichero motion.conf sección 1.**  
*Fuente: Captura de pantalla.*



En la segunda sección como se observa en la figura 43 se define las opciones de captura para los dispositivos de video (cámaras), podemos elegir la paleta de video que se usará, la entrada de video para el sistema, el ancho y alto de la imagen, numero de imágenes por segundo a capturar, el tiempo entre captura de tramas, configuración de brillo, contraste, saturación y color.

```
#####
# Capture device options
#####

v4l2_palette 3      #### Paleta de video para las camaras

input -1           #### Entrada de video a ser usada -1 para camaras web e IP

width 640          #### Anchura de la imagen en pixeles
height 480         #### Altura de la imagen en pixeles
framerate 30       #### Numero maximo de images por segundo que se captaran
minimum_frame_time 0 #### minimo tiempo entre la captura de tramas de imagen por la camara

auto_brightness off #### Control de brillo automatico a motion solo recomendado si la camara no tiene auto/brillo
brightness 0       #### Setea el brillo de un dispositivo de video
contrast 0         #### Setea el contraste
saturation 0       #### setea la saturacion
hue 0              #### setea el color
```

**Figura 47. Fichero motion.conf sección 2.**

*Fuente: Captura de pantalla.*

La tercera sección define las configuraciones de detección de movimiento, podemos definir la opción de threshold establece la sensibilidad, indicando el número de pixeles cambiados en una imagen para que se active la grabación del movimiento (Por defecto: 1500). Con valores más bajos será más sensible al movimiento y viceversa.

```
#####
# Motion Detection Settings:
#####

threshold 1500     #### Sensibilidad de deteccion de movimiento (detactada por el cambio de pixeles entre imagen)
noise_level 32     #### nivel de sencibilidad de ruido para la detccion de movimiento
noise_tune on      #### Activacion de la sencibilidad de ruido en la deteccion de movimiento
minimum_motion_frames 1 #### Minimo numero de tramas en contener movimiento antes de ser considerada verdadera deteccion
```

**Figura 48. Fichero motion.conf sección 3.**

*Fuente: Captura de pantalla.*

Las secciones cuatro, cinco y seis se refieren a la configuración de salida de imagen y video, definen calidad, formato de salida y compresión. La opción snapshot se activa si se desea hacer una captura de imagen en un intervalo de tiempo programado en segundos, con el parámetro 0 se desactiva.

```
#####
# Image File Output
#####

output_pictures on      #### Salida normal de imagenes cuando un movimiento es detectado
quality 75              #### Calidad en porcentaje a ser usada por la compresion jpeg
picture_type jpeg       #### tipo de salida de imagenes

#####
# FFmpeg related options
# Film (movie) file output
#####

ffmpeg_output_movies on   #### Activa la salida de video
ffmpeg_bps 400000         #### Bitrate a ser usado por el compresor ffmpeg
ffmpeg_video_codec msmpeg4  #### typo de codec de video *extension mp4

#####
# Snapshots (Traditional Periodic Webcam File Output)
#####

snapshot_interval 0      #### Intervalo de tiempo para captura automatica de imagen en 0 desactivada
```

**Figura 49. Fichero motion.conf sección 4-5-6.**

*Fuente: Captura de pantalla.*

La sección siete y ocho definen los textos que se presentaran en la salida de imagen y video indicando la fecha y hora. Se puede observar el formado que siguen estos textos en la figura 50.

```
#####
# Text Display
#####

text_right %Y-%m-%d\n%T-%q #### Pone la fecha en el display de salida de la camara esquina inferior derecha
text_event %Y%m%d%H%M%S     #### Pone la fecha en la detccion de un evento esquina inferior izquierda

#####
# Filenames For Images And Films
#####

snapshot_filename %v-%Y%m%d%H%M%S-snapshot #### nombre de una imagen tomada automaticamente salida
picture_filename %Y%m%d%H%M%S-%q          #### nombre del archivo de imagen de salida
movie_filename %v-%Y%m%d%H%M%S           #### nombre del archivo de video de salida
```

**Figura 50. Fichero motion.conf sección 7-8.**

*Fuente: Captura de pantalla.*

La sección nueve y diez como se visualiza en la figura 51 define los parámetros de transmisión y de control mediante servicio HTTP, define la restricción de conexiones solo locales, numero de puerto de escucha y velocidad de transmisión en streaming.

```
#####
# Live Stream Server
#####

stream_motion off      ##### Salida a 1 fps cuando no se detecta movimiento si se detecta toma el control maxrate
stream_maxrate 10     ##### Maximo framerate para stream
stream_localhost off  ##### Desabilita la restriccion de conexiones solo locales
stream_limit 0        ##### Limita el numero de imagenes por conexion 0 ilimitadas
stream_auth_method 0  ##### Autenticacion para el acceso 0 desactiva

#####
# HTTP Based Control
#####

webcontrol_port 8888   ##### puerto tcp para la interfaz web de control
webcontrol_localhost off ##### Desabilita la restriccion de conexiones solo locales
webcontrol_html_output on ##### Abilita la salida html
```

**Figura 51. Fichero motion.conf sección 9-10.**

*Fuente: Captura de pantalla.*

En la figura 48 se muestra la configuración para la sección once y doce, en donde se define las acciones a ejecutarse en caso de detección de movimiento, en la sección External Commands el segundo parámetro (`#on_event_start sudo /usr/local/bin/cam_event1.sh`) aparece comentado porque precisamente será controlado por el software Asterisk a manera de que se ejecute cuando el sistema esté en el segundo modo de funcionamiento el modo de Monitoreo y Alarma. La última sección define la ubicación de los ficheros de configuración individuales de cada cámara denominados threads.

```
#####
# External Commands
#####

quiet on                ##### evita la emision de beeps cuando detecta movimiento
#on_event_start sudo /usr/local/bin/cam_event1.sh  ##### Acciones a ejecutar a la deteccion de un movimiento *(Script)

#####
# Thread config files - One for each camera.
#####

thread /etc/motion/thread1.conf  ##### fichero de configuracion individual de camara 1
thread /etc/motion/thread2.conf  ##### fichero de configuracion individual de camara 2
thread /etc/motion/thread3.conf  ##### fichero de configuracion individual de camara 3
thread /etc/motion/thread4.conf  ##### fichero de configuracion individual de camara 4
thread /etc/motion/thread5.conf  ##### fichero de configuracion individual de camara 5
```

**Figura 52. Fichero motion.conf sección 11-12.**  
*Fuente: Captura de pantalla.*

### 3.5.2.1 Configuración de ficheros individuales (Threads)

Los threads son ficheros que contienen información específica de cada dispositivo de captura de imagen y video, deben ubicarse en el mismo directorio en donde se encuentra el fichero de configuración general `/etc/motion/`, con el comando **sudo nano /etc/motion/thread1.conf** crearemos este fichero y cada uno de los que necesite el sistema, el número de ficheros thread depende del número de cámaras.

El fichero de configuración `thread1.conf` contiene cuatro secciones, en la primera sección, opciones de captura del dispositivo indicaremos la dirección en donde está ubicado el driver para esta cámara, el identificador el cuales el nombre que se asigna por ejemplo CAMX.

La segunda sección se refiere a la ubicación en donde se guardará las imágenes y videos obtenidos este directorio debe ser el correspondiente al disco de almacenamiento masivo, se define también el nombre con que se guardaran para las imágenes capturadas, podemos ver esta configuración en la figura 53.

La sección tres define el puerto de escucha para la transmisión de video y la sección cuatro define la acción individual a realizarse en caso de detección de movimiento en la alarma.

```

GNU nano 2.2.6                               File: /etc/motion/thread1.conf
# /etc/motion/thread1.conf
# FICHERO DE CONFIGURACION PARTICULAR POR CAMARA

#####
# Capture device options
#####

videodevice /dev/video0  ### Camara a ser usada--ubicacion del driver
text_left CAMARA1      ### Indentificador de camara esquina inferior izquierda

#####
# Target Directories and filenames For Images And Films
#####

target_dir /media/SVGA/cam1      #### Directorio para salvar fotos y videos
picture_filename CAM1_%Y%m%d%H%M%S-%q  #### Nombre con que se guarda la imagen

#####
# Live Stream Server
#####

stream_port 8081          #### Puerto de escucha para la transmision en el servidor http

#####
# Reaccion a la deteccion de movimiento, envio de correo con fotos del evento.#
#####

#on_movie_start sudo /usr/local/bin/cam1_gmail.sh

```

**Figura 53. Fichero thread1.conf.**

*Fuente: Captura de pantalla.*

Los siguientes ficheros de configuración therad2.conf, thread3.conf y thread4.conf los cuales pertenecen a cámaras web contienen la misma estructura que el fichero thread1.conf, se diferencian en que cada cámara cita la ubicación de su driver, identificador de cámara, ubicación de almacenamiento en el disco duro extraíble, nombre con el que se guardan las imágenes, puerto de escucha para transmisión de video y acción a realizarse en caso de detección de movimiento por medio de la llamada a ejecución de un script en donde se programan las acciones a realizar dependiendo de cada cámara. Se puede ver la configuración de cada fichero thread en las figuras 54, 55 y 56 correspondientemente.

```

GNU nano 2.2.6                               File: /etc/motion/thread2.conf
# /etc/motion/thread2.conf
# FICHERO DE CONFIGURACION PARTICULAR POR CAMARA
#####
# Capture device options
#####
videodevice /dev/video1  ### Camara a ser usada--ubicacion del driver
text_left CAMARA2      ### Indentificador de camara esquina inferior izquierda
#####
# Target Directories and filenames For Images And Films
#####
target_dir /media/SVGA/cam2      #### Directorio para salvar fotos y videos
picture_filename CAM2_%Y%m%d%H%M%S-%q  #### Nombre con que se guarda la imagen
#####
# Live Stream Server
#####
stream_port 8082          #### Puerto de escucha para la transmision en el servidor http
#####
# Reaccion a la deteccion de movimiento, envio de correo con fotos del evento.#
#####
#on_movie_start sudo /usr/local/bin/cam2_gmail.sh

```

**Figura 54. Fichero thread2.conf.**  
Fuente: Captura de pantalla.

```

GNU nano 2.2.6                               File: /etc/motion/thread3.conf
# /etc/motion/thread3.conf
# FICHERO DE CONFIGURACION PARTICULAR POR CAMARA
#####
# Capture device options
#####
videodevice /dev/video2  ### Camara a ser usada--ubicacion del driver
text_left CAMARA3      ### Indentificador de camara esquina inferior izquierda
#####
# Target Directories and filenames For Images And Films
#####
target_dir /media/SVGA/cam3      #### Directorio para salvar fotos y videos
picture_filename CAM3_%Y%m%d%H%M%S-%q  #### Nombre con que se guarda la imagen
#####
# Live Stream Server
#####
stream_port 8083          #### Puerto de escucha para la transmision en el servidor http
#####
# Reaccion a la deteccion de movimiento, envio de correo con fotos del evento.#
#####
#on_movie_start sudo /usr/local/bin/cam3_gmail.sh

```

**Figura 55. Fichero thread3.conf.**  
Fuente: Captura de pantalla.

```

GNU nano 2.2.6 File: /etc/motion/thread4.conf
# /etc/motion/thread4.conf
# FICHERO DE CONFIGURACION PARTICULAR POR CAMARA

#####
# Capture device options
#####

videodevice /dev/video3   ### Camara a ser usada--ubicacion del driver
text_left CAMARA4       ### Indentificador de camara esquina inferior izquierda

#####
# Target Directories and filenames For Images And Films
#####

target_dir /media/SVGA/cam4      #### Directorio para salvar fotos y videos
picture_filename CAM4_%Y%m%d%H%M%S-%q  #### Nombre con que se guarda la imagen

#####
# Live Stream Server
#####

stream_port 8084           #### Puerto de escucha para la transmision en el servidor http

#####
# Reaccion a la deteccion de movimiento, envio de correo con fotos del evento.#
#####

#on_movie_start sudo /usr/local/bin/cam4_gmail.sh

```

**Figura 56. Fichero thread4.conf.**  
*Fuente: Captura de pantalla.*

El fichero thread5.conf corresponde a la configuración individual de la cámara IP inalámbrica, lleva una estructura similar a la de las cámaras web a diferencia que en este fichero se debe especificar la dirección IP de la cámara de red y el puerto de escucha en donde transmite el video, se debe también ingresar el usuario y contraseña de acceso para la cámara de red, al igual que en los ficheros anteriores también se le asigna un identificador para la cámara, la ubicación del disco duro externo en donde almacenar las imágenes y video capturados, el nombre con que se guardarán las imágenes, el puerto de transmisión de video en el sistema y la acción a realizar en caso de detección de movimiento realizada por medio de la ejecución de un script programado con las actividades para esta cámara.

En la figura 57 se observa la configuración para la cámara de red inalámbrica y los parámetros necesarios para su funcionamiento en el sistema de video vigilancia y alarma basada en la detección de movimiento.

```

GNU nano 2.2.6                               File: /etc/motion/thread5.conf
#####
# Camara de Red
#####

# URL to use if you are using a network camera, size will be autodetected
# Must be a URL that returns single jpeg pictures or a raw mjpeg stream.

netcam_url http://192.168.1.13:8001  ## Direccion IP y puerto de la camara de red Inalambrica

# Username and password for network camera (only if required).
# Syntax is user:password

netcam_userpass ipcam:12345678  #### usuario y contrasena de acceso a la camara IP
text_left CAMARA5              #### Indentificador de camara esquina inferior izquierda

#####
# Target Directories and filenames For Images And Films
#####

target_dir /home/SVGA/cam5      #### Directorio para salvar fotos y videos
picture_filename CAM5_%Y%m%d%H%M%S-%q  #### Nombre con que se guarda la imagen

#####
# Live Stream Server
#####

stream_port 8085                #### Puerto de escucha para la transmision en el servidor http

#####
# Reaccion a la deteccion de movimiento, envio de correo con fotos del evento.#
#####
#on_movie_start sudo /usr/local/bin/cam5_gmail.sh

```

**Figura 57. Fichero thread5.conf.**  
*Fuente: Captura de pantalla.*

### 3.5.2.2 Verificación de reconocimiento de cámaras web.

Para verificar que las cámaras web han sido reconocidas por el sistema operativo Raspbian debemos ejecutar desde el terminal el siguiente comando: **lsusb**, este comando nos dará un listado de los dispositivos conectados a los puertos USB del Raspberry. Con el comando **ls /dev** veremos los drivers cargados en el directorio /dev a modo de una lista.

En la figura 58 se muestran los resultados de ejecutar los comandos antes mencionados, en la imagen podemos observar la detección de tres cámaras web conectadas, una cámara UVC WebCam y dos cámaras Aveo Technology, las que fueron conectadas al hasta el momento, podemos ver también que que en directorio /dev se han cargado los drivers correspondientes de cada cámara, se puede observar los ficheros video0, video1 y video2 que son los drivers de cada cámara citados en los ficheros thread de configuración individual del software Motion.



```

pi@raspberrypi:~ $ lsusb
Bus 001 Device 009: ID 1e4e:0102 Cubeternet GL-UPC822 UVC WebCam
Bus 001 Device 008: ID 1871:0142 Aveo Technology Corp.
Bus 001 Device 007: ID 1871:0142 Aveo Technology Corp.
Bus 001 Device 006: ID 05e3:0606 Genesys Logic, Inc. USB 2.0 Hub / D-Link DUB-H4
USB 2.0 Hub
Bus 001 Device 005: ID 05e3:0606 Genesys Logic, Inc. USB 2.0 Hub / D-Link DUB-H4
USB 2.0 Hub
Bus 001 Device 004: ID 14cd:6116 Super Top M6116 SATA Bridge
Bus 001 Device 003: ID 0424:ec00 Standard Microsystems Corp. SMSC9512/9514 Fast
Ethernet Adapter
Bus 001 Device 002: ID 0424:9514 Standard Microsystems Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
pi@raspberrypi:~ $ ls /dev
autofs          loop1          ppp            sda            tty2           tty4           tty6           vcs4
block           loop2          ptmx          sda1          tty20         tty40         tty60         vcs5
bsg             loop3          pts           serial1       tty21         tty41         tty61         vcs6
btrfs-control  loop4          ram0          sg0           tty22         tty42         tty62         vcs7
bus             loop5          ram1          shm           tty23         tty43         tty63         vcsa
cachefiles     loop6          ram10         snd           tty24         tty44         tty7          vcsa1
char           loop7          ram11         stderr        tty25         tty45         tty8          vcsa2
console        loop-control  ram12         stdin         tty26         tty46         tty9          vcsa3
cpu_dma_latency mapper         ram13         stdout        tty27         tty47         ttyAMA0       vcsa4
cuse           media0         ram14         tty           tty28         tty48         ttyprintk     vcsa5
disk           media1         ram15         tty0          tty29         tty49         uhid          vcsa6
fb0            media2         ram2          tty1          tty3          tty5          uinput        vcsa7
fd             mem            ram3          tty10         tty30         tty50         urandom       vcsm
full           memory_bandwidth ram4          tty11         tty31         tty51         v4l           vchi
fuse           mmcblk0        ram5          tty12         tty32         tty52         vc-cma        video0
gpiomem       mmcblk0p1      ram6          tty13         tty33         tty53         vchiq         video1
hwrng         mmcblk0p2      ram7          tty14         tty34         tty54         vcio          video2
initctl       mqueue         ram8          tty15         tty35         tty55         vc-mem        watchdog
input         net            ram9          tty16         tty36         tty56         vcs           watchdog0
kmsg          network_latency random         tty17         tty37         tty57         vcs1         xconsole
log           network_throughput raw            tty18         tty38         tty58         vcs2         zero
loop0        null           rfk            tty19         tty39         tty59         vcs3

```

Figura 58. Detección de cámaras web y sus drivers.

Fuente: Captura de pantalla.

Para que las cámaras web funcionen con todos los usuarios del sistema operativo Raspbian es necesario darles permisos a los drivers de cada cámara, la realización de esta acción y se hace por medio del comando **chmod o+wr /dev/videoX**, en donde X es el número de driver de cada cámara web. Al finalizar podemos ver los permisos que tienen estos drivers con el comando **ls /dev/videoX -l**, como se muestra en la figura 59.

```

pi@raspberrypi:~/etc/motion
File Edit Tabs Help
pi@raspberrypi:~/etc/motion $ sudo chmod o+rw /dev/video0
pi@raspberrypi:~/etc/motion $ sudo chmod o+rw /dev/video1
pi@raspberrypi:~/etc/motion $ sudo chmod o+rw /dev/video2
pi@raspberrypi:~/etc/motion $ sudo usermod -a -G video pi
pi@raspberrypi:~/etc/motion $ ls /dev/video0 -l
crw-rw-rw-+ 1 root video 81, 0 Dec 29 23:46 /dev/video0
pi@raspberrypi:~/etc/motion $ ls /dev/video1 -l
crw-rw-rw-+ 1 root video 81, 1 Dec 29 23:46 /dev/video1
pi@raspberrypi:~/etc/motion $ ls /dev/video2 -l
crw-rw-rw-+ 1 root video 81, 2 Dec 29 23:46 /dev/video2
pi@raspberrypi:~/etc/motion $

```

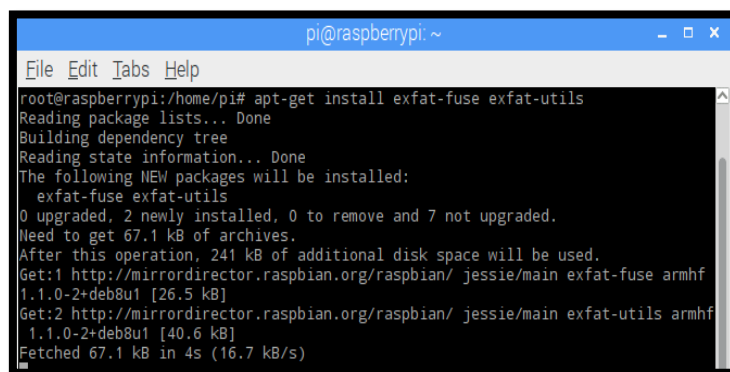
Figura 59. Verificación de permisos de drivers.

Fuente: Captura de pantalla.

### 3.5.2.3 Montaje permanente del disco de almacenamiento externo.

El montaje del disco de almacenamiento externo, permitirá que las imágenes, videos capturados por las cámaras se graben en el disco externo para evitar la saturación de memoria en el sistema operativo Raspbian instalado en el Raspberry Pi 3.

Para que el sistema operativo reconozca el disco es necesario instalar los paquetes `exfat-fuse` y `exfat-utils` introduciendo en el terminal: **`sudo apt-get install exfat-fuse exfat-utils`** como se observa en la figura 60.



```

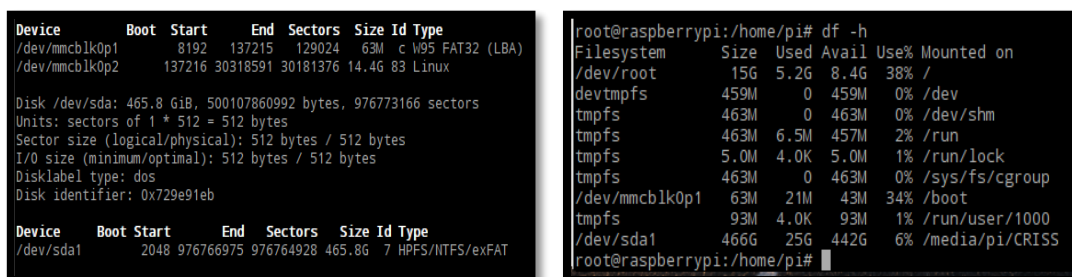
pi@raspberrypi: ~
File Edit Tabs Help
root@raspberrypi:/home/pi# apt-get install exfat-fuse exfat-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  exfat-fuse exfat-utils
0 upgraded, 2 newly installed, 0 to remove and 7 not upgraded.
Need to get 67.1 kB of archives.
After this operation, 241 kB of additional disk space will be used.
Get:1 http://mirrordirector.raspbian.org/raspbian/ jessie/main exfat-fuse armhf
1.1.0-2+deb8u1 [26.5 kB]
Get:2 http://mirrordirector.raspbian.org/raspbian/ jessie/main exfat-utils armhf
1.1.0-2+deb8u1 [40.6 kB]
Fetched 67.1 kB in 4s (16.7 kB/s)

```

**Figura 60. Instalación de paquetes exfat.**

*Fuente: Captura de pantalla.*

Verificamos que el sistema reconozca el disco extraíble mediante el comando **`fdisk -l`** y obtenemos la ruta de montaje actual de disco extraíble con el comando **`df -h`**. en la figura 61 podemos observar los resultados de los comandos **`sudo fdisk -l`** y **`sudo df -h`**.



```

Device Boot Start End Sectors Size Id Type
/dev/mmcblk0p1 8192 137215 129024 63M c W95 FAT32 (LBA)
/dev/mmcblk0p2 137216 30318591 30181376 14.4G 83 Linux

Disk /dev/sda: 465.8 GiB, 500107860992 bytes, 976773166 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x729e91eb

Device Boot Start End Sectors Size Id Type
/dev/sda1 2048 976766975 976764928 465.8G 7 HPFS/NTFS/exFAT

root@raspberrypi:/home/pi# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/root 15G 5.2G 8.4G 38% /
devtmpfs 459M 0 459M 0% /dev
tmpfs 463M 0 463M 0% /dev/shm
tmpfs 463M 6.5M 457M 2% /run
tmpfs 5.0M 4.0K 5.0M 1% /run/lock
tmpfs 463M 0 463M 0% /sys/fs/cgroup
/dev/mmcblk0p1 63M 21M 43M 34% /boot
tmpfs 93M 4.0K 93M 1% /run/user/1000
/dev/sda1 466G 25G 442G 6% /media/pi/CRISS
root@raspberrypi:/home/pi#

```

**Figura 61. Verificación de reconocimiento del disco externo.**

*Fuente: Captura de pantalla.*

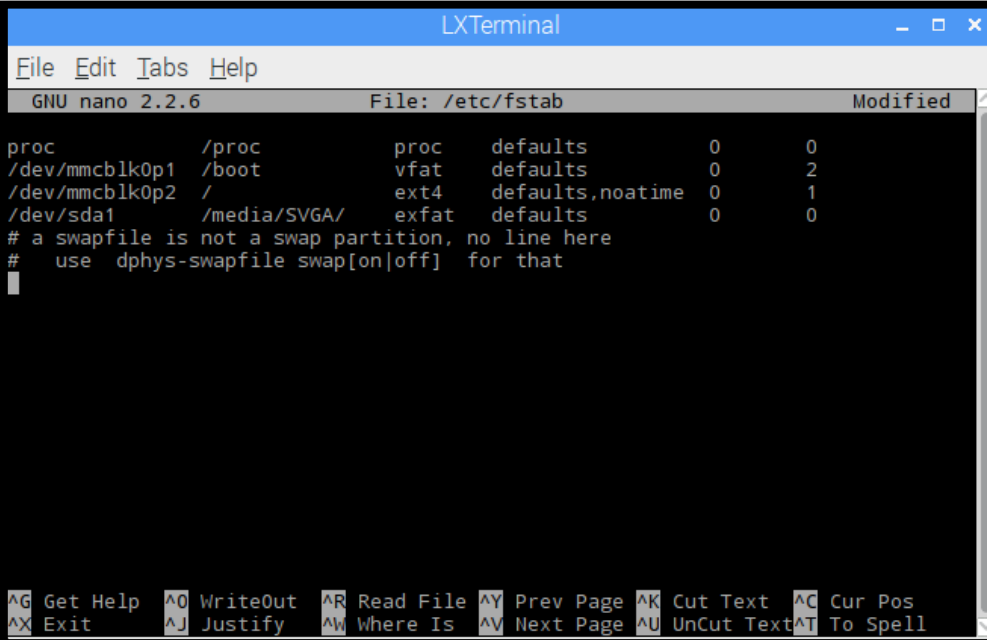
Para que el disco pueda ser usado se debe especificar la ruta de montado, generalmente se suele montar los discos extraíbles dentro del directorio /media, para este proyecto se lo montó en el directorio /media/SVGA, creado el subdirectorio debemos montar el disco dentro.

Comando para crear el subdirectorio: **sudo mkdir /media/SVGA**

Montar el disco en el subdirectorio: **sudo mount /dev/sda1 /media/SVGA**

Ejecutando los comandos anteriores se verá el contenido del disco externo en el directorio de montaje. Si no se monta de forma permanente el disco externo en cada reinicio del sistema se tendrá que realizar los procedimientos anteriores otra vez.

Para hacer permanente el punto de montaje es necesario editar el fichero ubicado en el directorio /etc/fstab, lo podemos hacer con el comando: **sudo nano /etc/fstab**, con la línea siguiente: **/dev/sda1 /media/SVGA exfat defaults 0 0**, se puede ver la edición de este fichero en la figura 62.



```

LXTerminal
File Edit Tabs Help
GNU nano 2.2.6 File: /etc/fstab Modified
proc /proc proc defaults 0 0
/dev/mmcblk0p1 /boot vfat defaults 0 2
/dev/mmcblk0p2 / ext4 defaults,noatime 0 1
/dev/sda1 /media/SVGA/ exfat defaults 0 0
# a swapfile is not a swap partition, no line here
# use dphys-swapfile swap[on|off] for that
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

```

Figura 62. Montaje permanente de disco externo en fichero fstab.

Fuente: Captura de pantalla.

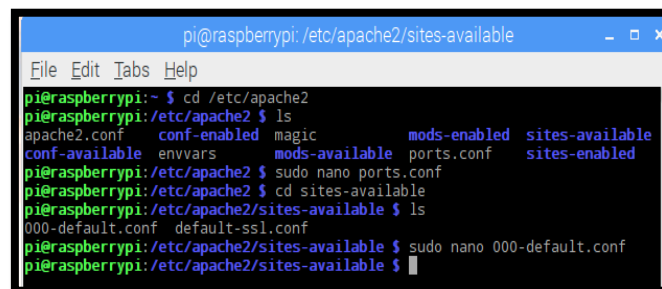
### 3.5.3 Instalación del software Apache2

Se utiliza este software para la presentación del video obtenido por las cámaras del sistema a través de una interfaz web, la instalación del software se la realiza ejecutando el siguiente comando en la terminal: **sudo apt-get install apache2**

Al finalizar la instalación, se debe verificar el funcionamiento del software, por defecto el puerto de escucha para http es el puerto número 80 y para https el puerto número 443, para poder acceder a través de internet a la página web es recomendable cambiar el puerto 80 de http debido a que este número de puerto lo utilizan los proveedores de internet para monitorear el punto de acceso del abonado, el cual es el Gateway de salida hacia Internet en la red local del abonado. Para este proyecto usaremos el puerto el puerto 8080 para http por ello debemos cambiar la configuración por defecto del software Apache2.

#### 3.5.3.1 Configuración de software

La configuración para el cambio de puerto de escucha http se realiza accediendo al directorio `/etc/apache2/` y editando el fichero `ports.conf`, después se accede al subdirectorio `sites-available` y se edita el fichero `000-default.conf`. Después de realizar los cambios, para que estos surtan efecto se debe ejecutar el siguiente comando en el terminal: **systemctl daemon-reload && systemctl restart apache2.**



```

pi@raspberrypi: /etc/apache2/sites-available
File Edit Tabs Help
pi@raspberrypi:~ $ cd /etc/apache2
pi@raspberrypi:/etc/apache2 $ ls
apache2.conf  conf-enabled  magic          mods-enabled  sites-available
conf-available  envvars      mods-available  ports.conf    sites-enabled
pi@raspberrypi:/etc/apache2 $ sudo nano ports.conf
pi@raspberrypi:/etc/apache2 $ cd sites-available
pi@raspberrypi:/etc/apache2/sites-available $ ls
000-default.conf  default-ssl.conf
pi@raspberrypi:/etc/apache2/sites-available $ sudo nano 000-default.conf
pi@raspberrypi:/etc/apache2/sites-available $

```

Figura 63. Acceso al fichero `ports.conf`.

Fuente: Captura de pantalla.

En la figura 64 se observa el cambio del número de puerto de escucha 80 por 8080 en el fichero ports.conf y en la figura 61 se observa el cambio del parámetro <VirtualHost \*=80> a <VirtualHost \*=8080>.

```

pi@raspberrypi: /etc/apache2
File Edit Tabs Help
GNU nano 2.2.6 File: ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 8080

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

AG Get Help  AO WriteOut  AR Read File  AY Prev Page  AK Cut Text  AC Cur Pos
AX Exit      AJ Justify   AW Where Is AV Next Page  AU UnCut Tex AT To Spell

```

**Figura 64. Configuración del fichero ports.conf.**

*Fuente: Captura de pantalla.*

```

pi@raspberrypi: /etc/apache2/sites-available
File Edit Tabs Help
GNU nano 2.2.6 File: 000-default.conf
<VirtualHost *:8080>
# The ServerName directive sets the request scheme, hostname and port
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header
# match this virtual host. For the default virtual host (this file)
# value is not decisive as it is used as a last resort host regardl
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html

# Available loglevels: trace8, ..., trace1, debug, info, notice, wa
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

[ Read 31 lines ]
AG Get Help  AO WriteOut  AR Read File  AY Prev Page  AK Cut Text  AC Cur Pos
AX Exit      AJ Justify   AW Where Is AV Next Page  AU UnCut Tex AT To Spell

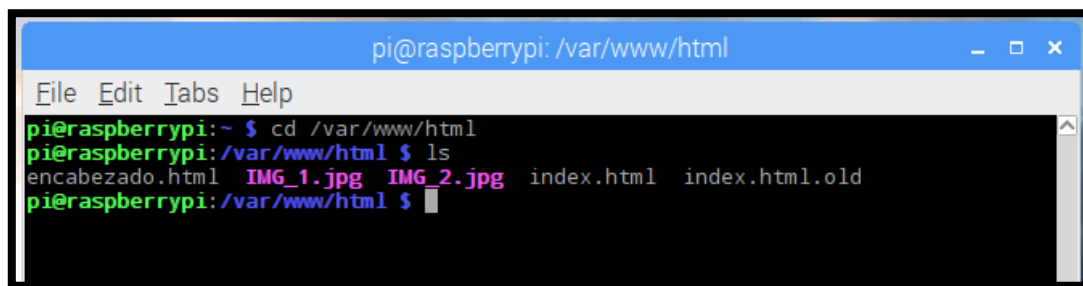
```

**Figura 65. Configuración del fichero 000-default.conf.**

*Fuente: Captura de pantalla.*

### 3.5.3.2 Programación de la interfaz web para el sistema

La configuración de la página web en donde se presenta la salida de las cámaras se debe alojar en el directorio `/var/www/html/`, en donde se carga el diseño de la página web en formato html. El código de este diseño se puede ver en el anexo 6, en la figura 66 observamos los ficheros en formato html y la interfaz web al con las cámaras conectadas hasta el momento.



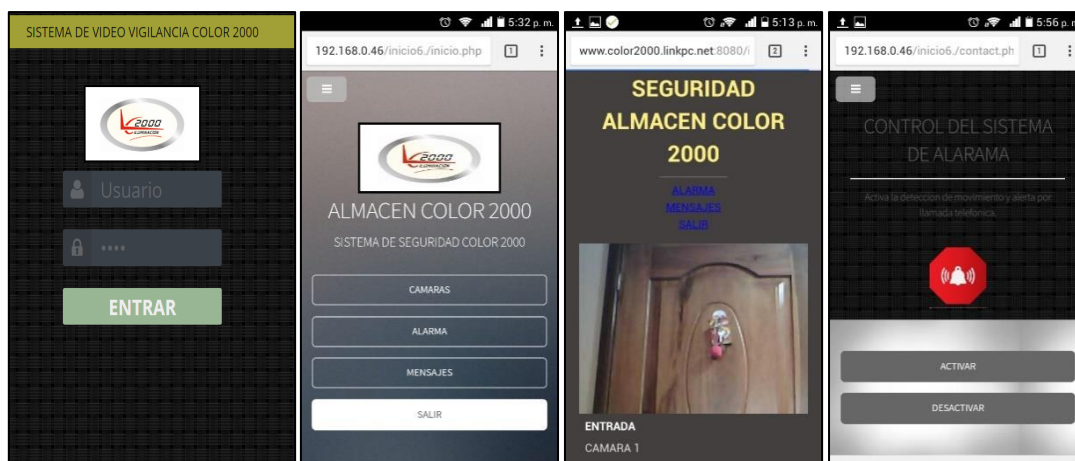
```

pi@raspberrypi: /var/www/html
File Edit Tabs Help
pi@raspberrypi:~ $ cd /var/www/html
pi@raspberrypi:/var/www/html $ ls
encabezado.html  IMG_1.jpg  IMG_2.jpg  index.html  index.html.old
pi@raspberrypi:/var/www/html $
  
```

**Figura 66. Ficheros de página web en el directorio del servidor Apache2.**

*Fuente: Captura de pantalla.*

En la figura 67 se muestra la interfaz de la página web con las cámaras en monitoreo. Para acceder dentro de la red local ingresamos en el navegador web la dirección IP del Raspberry Pi y el puerto 9000 de la siguiente forma: 192.168.1.12:9000.



**Figura 67. Interfaz de página web.**

*Fuente: Captura de pantalla.*

## 3.6 Diseño del sistema de alarma

El sistema de alarma cumple una función complementaria al sistema de video vigilancia, este sistema hará que las cámaras actúen en forma de sensores de movimiento, independientemente de su función de capturar imágenes y video.

Este sistema necesita un método de control para su activación y desactivación, el cual será gestionado por el software Asterisk mediante un plan de marcado y por el software Yowsup por medio de mensajes WhatsApp en un formato específico.

En la gestión de eventos intervienen los softwares Asterisk para realizar una llamada de alerta, Mutt para enviar un correo con imágenes del evento y Telegram para el envío de mensajes en esta red social.

### 3.6.1 Instalación de software Asterisk

Hay muchas versiones de Asterisk disponibles en su página web, en este proyecto se compilo la versión 13. Se descargó el código fuente e instaló en el Raspberry Pi 3, con los pasos siguientes:

En primer lugar, se instala el entorno de construcción: **apt-get install build-essential**, el comando anterior instalará los paquetes básicos que son necesarios en un nuevo servidor para instalar Asterisk 13.

Se instala algunas librerías para el funcionamiento de algunos módulos los cuales son necesarios para el funcionamiento del proyecto y que son directamente dependientes del software Asterisk versión 13: **apt-get install openssl libxml2-dev libncurses5-dev uuid-dev sqlite3 libsqlite3-dev pkg-config libjansson-dev**.

Entrar en el directorio `/usr/src/` con el comando `cd /usr/src/` para descargar el software Asterisk en versión 13 de la página web oficial, para esto utilizaremos el siguiente comando: **wget** <http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-13-current.tar.gz>. En la figura 68 se puede observar el proceso de descarga del software.

```

root@raspberrypi:/# cd /usr/src
root@raspberrypi:/usr/src# wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-13-current.tar.gz
--2017-01-29 10:47:05-- http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-13-current.tar.gz
Resolving downloads.asterisk.org (downloads.asterisk.org)... 2001:470:e0d4::ee, 76.164.171.238
Connecting to downloads.asterisk.org (downloads.asterisk.org)|2001:470:e0d4::ee|80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 32743348 (31M) [application/x-gzip]
Saving to: 'asterisk-13-current.tar.gz'

asterisk-13-current.tar.gz 100%[*****>] 31.23M 125KB/s in 2m 26s

2017-01-29 10:49:33 (219 KB/s) - 'asterisk-13-current.tar.gz' saved [32743348/32743348]

root@raspberrypi:/usr/src#

```

**Figura 68. Descarga de software Asterisk 13.**

*Fuente: Captura de pantalla.*

Extraemos el código fuente del paquete: **tar xvf asterisk-13-current.tar.gz**.

Ingresamos a directorio extraído: **cd asterisk-13.13.1/**.

Instalar los prerequisites del software: **contrib/scripts/install\_prereq install**. Durante el proceso nos pedirá que ingresemos el código telefónico internacional del país 593 y al finalizar veremos el mensaje que se muestra en la figura 69.

```

Setting up libbluetooth-dev (5.23-2+rpi2) ...
Setting up libc-client2007e-dev (8:2007f-dfsg-4) ..
Setting up dh-autoreconf (12-bpo8+1) ...
Setting up debhelper (10.2.2-bpo8+1) ...
Setting up dh-strip-nondeterminism (0.003-1) ...
Setting up vpb-driver-source (4.2.58-1) ...
Processing triggers for libc-bin (2.19-18+deb8u7) .

Current status: 6 updates [-1].
#####
## install completed successfully
#####

```

**Figura 69. Instalación de prerequisites para Asterisk 13.**

*Fuente: Captura de pantalla.*





Instalar el software: **make**, **make install**, **make samples**, **make config**. Este proceso tomará tiempo, en la figura 72.

```
[CC] stasis/convert.o -> stasis/convert.o
[LD] res_stasis.o stasis/cli.o stasis/stasis
ol.o -> res_stasis.so
[CC] res_format_attr_h263.c -> res_format_at
[LD] res_format_attr_h263.o -> res_format_at
[CC] res_config_sqlite3.c -> res_config_sqli
[LD] res_config_sqlite3.o -> res_config_sqli
[CC] res_convert.c -> res_convert.o
[LD] res_convert.o -> res_convert.so
[CC] res_stasis_snoop.c -> res_stasis_snoop.
[LD] res_stasis_snoop.o -> res_stasis_snoop.
[CC] chan_mobile.c -> chan_mobile.o
[LD] chan_mobile.o -> chan_mobile.so
Building Documentation For: third-party channel
+----- Asterisk Build Complete -----+
+ Asterisk has successfully been built, and +
+ can be installed by running:           +
+                                         +
+             make install                +
+-----+
root@raspberrypi:/usr/src/asterisk-13.13.1#

+----- Asterisk Installation Complete -----+
+
+   YOU MUST READ THE SECURITY DOCUMENT   +
+
+ Asterisk has successfully been installed. +
+ If you would like to install the sample  +
+ configuration files (overwriting any     +
+ existing config files), run:            +
+
+ For generic reference documentation:    +
+   make samples                          +
+
+ For a sample basic PBX:                 +
+   make basic-pbx                        +
+
+----- or -----+
+
+ You can go ahead and install the asterisk +
+ program documentation now or later run:   +
+
+             make progdocs                +
+
+ **Note** This requires that you have    +
+ doxygen installed on your local system  +
+-----+
root@rasoberrvoi:/usr/src/asterisk-13.13.1#
```

**Figura 72. Mensajes de Instalación completa de Asterisk 13.**

*Fuente: Captura de pantalla.*

Iniciar el software con el comando: **sudo /etc/init.d/asterisk restart**, entrar a la consola de administración: **sudo asterisk -rvvvvv**. En la figura 73 se muestra el software en ejecución.

```
root@raspberrypi:~# /etc/init.d/asterisk restart
[ ok ] Restarting asterisk (via systemctl): asterisk.service.
root@raspberrypi:~# asterisk -rvvvvv
Asterisk 13.13.1, Copyright (C) 1999 - 2014, Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 13.13.1 currently running on raspberrypi (pid = 27774)
raspberrypi*CLI>
```

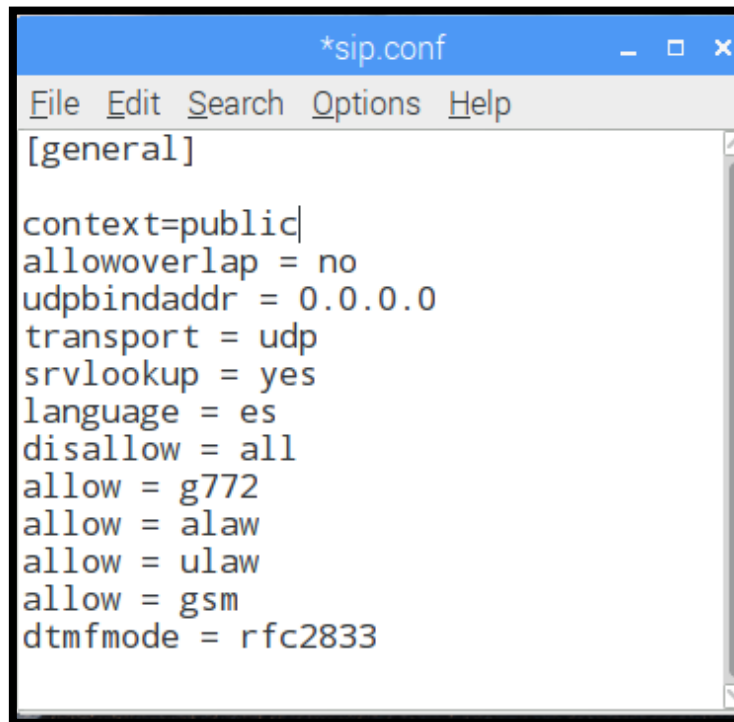
**Figura 73. Asterisk 13 ejecutándose.**

*Fuente: Captura de pantalla.*

El software Asterisk requiere de la configuración de cinco ficheros ubicados en el directorio `/etc/asterisk/`, los ficheros son: `sip.conf`, `extensions.conf`, `users.conf`, `modules.conf` y `chan_mobile.conf` dentro de estos ficheros se realiza la configuración para el funcionamiento de control y reacción ante eventos en el sistema de alarma basada en detección de movimiento.

### 3.6.1.1 Configuración de ficheros del software

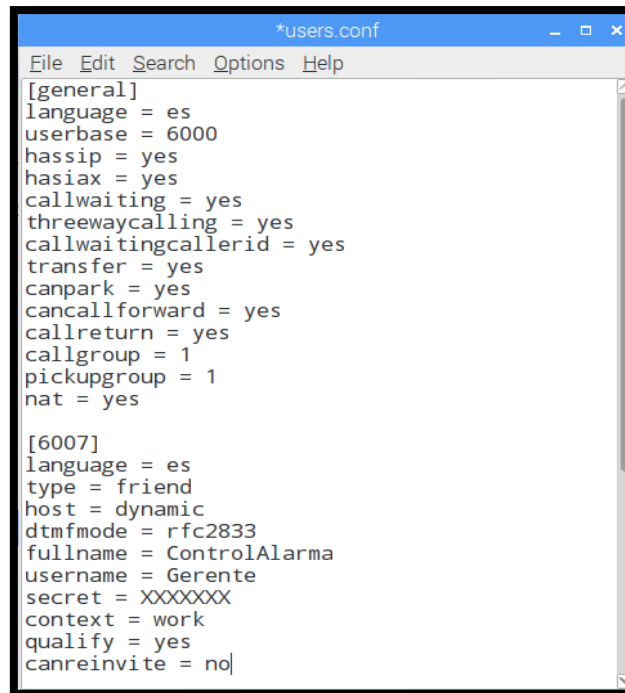
El fichero sip.conf contiene configuración estándar en donde se indica el protocolo de transporte, el idioma a usar, códec de audio y rfc para voz sobre protocolo IP, en la figura 74 se observa el contenido de este fichero.

A screenshot of a text editor window titled '\*sip.conf'. The window has a menu bar with 'File', 'Edit', 'Search', 'Options', and 'Help'. The main text area contains the following configuration: [general] context=public allowoverlap = no udpbindaddr = 0.0.0.0 transport = udp srvlookup = yes language = es disallow = all allow = g772 allow = alaw allow = ulaw allow = gsm dtmfmode = rfc2833.

```
*sip.conf
File Edit Search Options Help
[general]
context=public
allowoverlap = no
udpbindaddr = 0.0.0.0
transport = udp
srvlookup = yes
language = es
disallow = all
allow = g772
allow = alaw
allow = ulaw
allow = gsm
dtmfmode = rfc2833
```

**Figura 74. Fichero sip.conf.**  
*Fuente: Captura de pantalla.*

El fichero users.conf contiene la configuración de los usuarios que se registraran en dentro de esta centralita de voz sobre protocolo IP, este contiene información como: el número de extensión, nombre del usuario, contraseña, contexto en el que funciona la extensión y otros parámetros adicionales. Se creó un usuario el cual será asignado al gerente para el control del sistema de alarma manejado por el plan de marcado. En la figura 75 se puede observar el contenido de configuración del fichero y los parámetros para el usuario asignado al gerente de la empresa el cual controlará el sistema a través de un Softphone instalado en su Smartphone.



```

*users.conf
File Edit Search Options Help
[general]
language = es
userbase = 6000
hassip = yes
hasiax = yes
callwaiting = yes
threewaycalling = yes
callwaitingcallerid = yes
transfer = yes
canpark = yes
cancallforward = yes
callreturn = yes
callgroup = 1
pickupgroup = 1
nat = yes

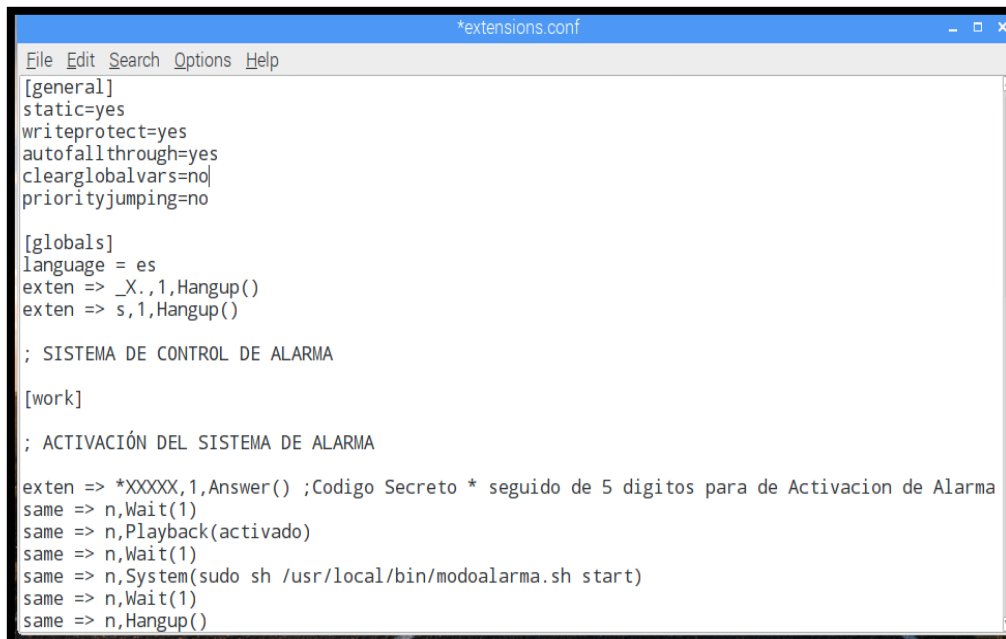
[6007]
language = es
type = friend
host = dynamic
dtmfmode = rfc2833
fullname = ControlAlarma
username = Gerente
secret = XXXXXXXX
context = work
qualify = yes
canreinvite = no

```

**Figura 75. Fichero users.conf.**

*Fuente: Captura de pantalla.*

Fichero extensions.conf contiene el plan de marcado para el control del sistema de alarma indicado en el contexto work y el contexto de reacción a un evento Funcion\_Alarma.



```

*extensions.conf
File Edit Search Options Help
[general]
static=yes
writeprotect=yes
autofallthrough=yes
clearglobalvars=no
priorityjumping=no

[globals]
language = es
exten => _X.,1,Hangup()
exten => s,1,Hangup()

; SISTEMA DE CONTROL DE ALARMA

[work]

; ACTIVACIÓN DEL SISTEMA DE ALARMA

exten => *XXXXX,1,Answer() ;Codigo Secreto * seguido de 5 digitos para de Activacion de Alarma
same => n,Wait(1)
same => n,Playback(activado)
same => n,Wait(1)
same => n,System(sudo sh /usr/local/bin/modoalarma.sh start)
same => n,Wait(1)
same => n,Hangup()

```

**Figura 76. Fichero extensions.conf parte 1.**

*Fuente: Captura de pantalla.*

```

; DESACTIVACIÓN DEL SISTEMA DE ALARMA
exten => *XXXXX|,1,Answer();Codigo Secreto * seguido de 5 digitos para de Desactivacion de Alarma
same => n,Wait(1)
same => n,Playback(desactivado)
same => n,Wait(1)
same => n,System(sudo sh /usr/local/bin/modoalarma.sh stop)
same => n,Wait(1)
same => n,Hangup()

; SISTEMA DE REACCIÓN FRENTE A LA DETECCIÓN DE UN EVENTO

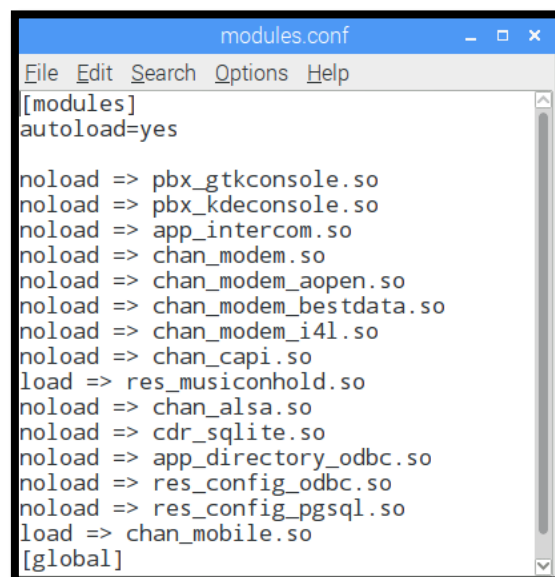
; IVR DE RESPUESTA A LA LLAMADA HACIA EL MOVIL DEL GERENTE
[Funcion_Alarma]
exten => s,1,Answer()
same => n,Wait(1)
same => n,Set(TIMEOUT(digit)=5)
same => n,Set(TIMEOUT(response)=10)
same => n,Set(CHANNEL(language)=es)
same => n,BackGround(menu)
same => n,WaitExten()
exten => 1,1,System(sudo sh /usr/local/bin/modoalarma.sh start)
same => n,Hangup()
exten => 2,1,System(sudo sh /usr/local/bin/modoalarma.sh stop)
same => n,Hangup()
exten => 3,1,System(sudo sh /usr/local/bin/sirena.sh)
same => n,Hangup()
exten => 4,1,System(sudo sh /usr/local/bin/pararsirena.sh)
same => n,Hangup()
exten => i,1,Playback(invalid)
same => n,Goto(s,6)
exten => t,1,Playback(time)
same => n,Hangup()
exten => h,1,Hangup()

```

**Figura 77. Fichero extensions.conf parte 2.**

*Fuente: Captura de pantalla.*

Para el funcionamiento del Gateway de voz hacia la red de telefonía móvil se debe cargar el modulo chan\_mobile.so en el fichero modules.conf, en la figura 78 se observa la configuración de este fichero.



```

modules.conf
File Edit Search Options Help
[modules]
autoload=yes

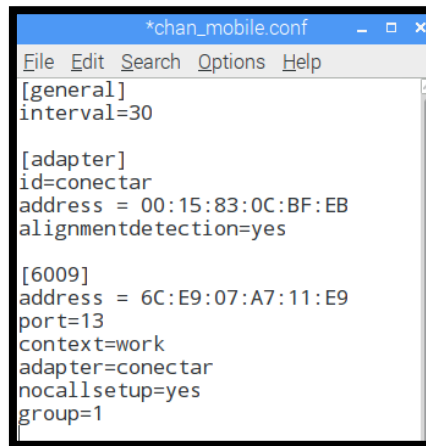
noload => pbx_gtkconsole.so
noload => pbx_kdeconsole.so
noload => app_intercom.so
noload => chan_modem.so
noload => chan_modem_aopen.so
noload => chan_modem_bestdata.so
noload => chan_modem_i4l.so
noload => chan_capi.so
load => res_musiconhold.so
noload => chan_alsa.so
noload => cdr_sqlite.so
noload => app_directory_odbc.so
noload => res_config_odbc.so
noload => res_config_pgsql.so
load => chan_mobile.so
[global]

```

**Figura 78. Fichero modules.conf.**

*Fuente: Captura de pantalla.*

El fichero de configuración `chan_mobile.conf` determina el tiempo de espera para una petición de conexión con el Gateway, identificador del adaptador Bluetooth a usar, dirección MAC del adaptador y corrección en la transmisión de audio. En el tercer apartado se indica las características del Gateway: MAC, puerto de comunicación, contexto, vinculación con adaptador a del sistema, opción para aceptar dialogo entrante (menú), y grupo al que pertenece.



```
*chan_mobile.conf
File Edit Search Options Help
[general]
interval=30

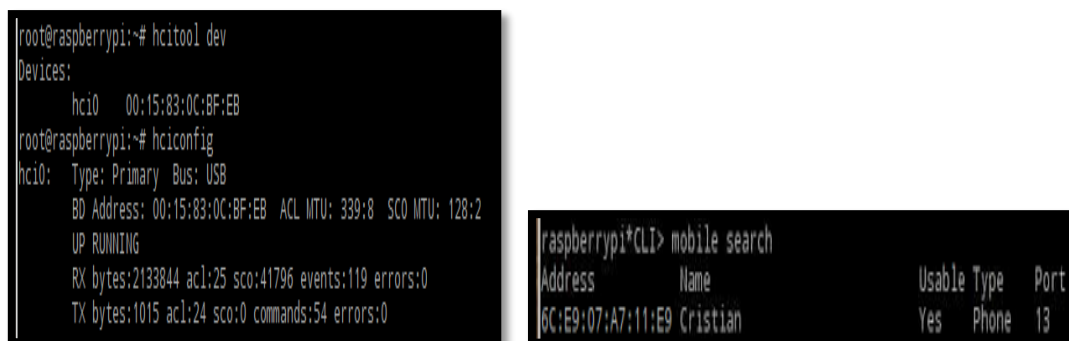
[adapter]
id=conectar
address = 00:15:83:0C:BF:EB
alignmentdetection=yes

[6009]
address = 6C:E9:07:A7:11:E9
port=13
context=work
adapter=conectar
nocallsetup=yes
group=1
```

**Figura 79. Fichero `chan_mobile.conf`.**

*Fuente: Captura de pantalla.*

Para obtener la dirección MAC del adaptador Bluetooth se ejecuta en el terminal el siguiente comando: `hcitool dev && hciconfig`, para obtener la dirección MAC del Gateway con y su puerto, entramos a la consola de Asterisk con el comando: `asterisk -rvv` y ejecutamos dentro de la consola en comando: `mobile search`, como se observa en la figura 80.



```
root@raspberrypi:~# hcitool dev
Devices:
  hci0  00:15:83:0C:BF:EB
root@raspberrypi:~# hciconfig
hci0:  Type: Primary Bus: USB
       BD Address: 00:15:83:0C:BF:EB ACL MTU: 339:8 SCO MTU: 128:2
       UP RUNNING
       RX bytes:2133844 acl:25 sco:41796 events:119 errors:0
       TX bytes:1015 acl:24 sco:0 commands:54 errors:0

raspberrypi*CLI> mobile search
Address      Name      Usable Type  Port
6C:E9:07:A7:11:E9 Cristian  Yes  Phone  13
```

**Figura 80. Direcciones MAC de dispositivos Bluetooth.**

*Fuente: Captura de pantalla.*

### 3.6.2 Instalación del software Yowsup

Se utilizó un programa de software libre y escrito en Python llamado Yowsup, el cual permite utilizar WhatsApp a través de la línea de comandos en Linux. Se debe modificar un poco el programa, para utilizar los mensajes recibidos e interactuar con el sistema de alarma basada en la detección de movimiento.

Requisitos previos instalar las siguientes dependencias, algunas ya estarán instaladas:

- `sudo apt-get install python-dateutil`
- `sudo apt-get install python-argparse`
- `sudo apt-get install python-setuptools`
- `sudo apt-get install python-dev`
- `sudo apt-get install libevent-dev`
- `sudo apt-get install ncurses-dev`
- `sudo apt-get install libglib2.0`
- `sudo apt-get install libglib2.0-dev`
- `sudo apt-get install libxml2`
- `sudo pip install protobuf`
- `sudo pip install python-axolotl`

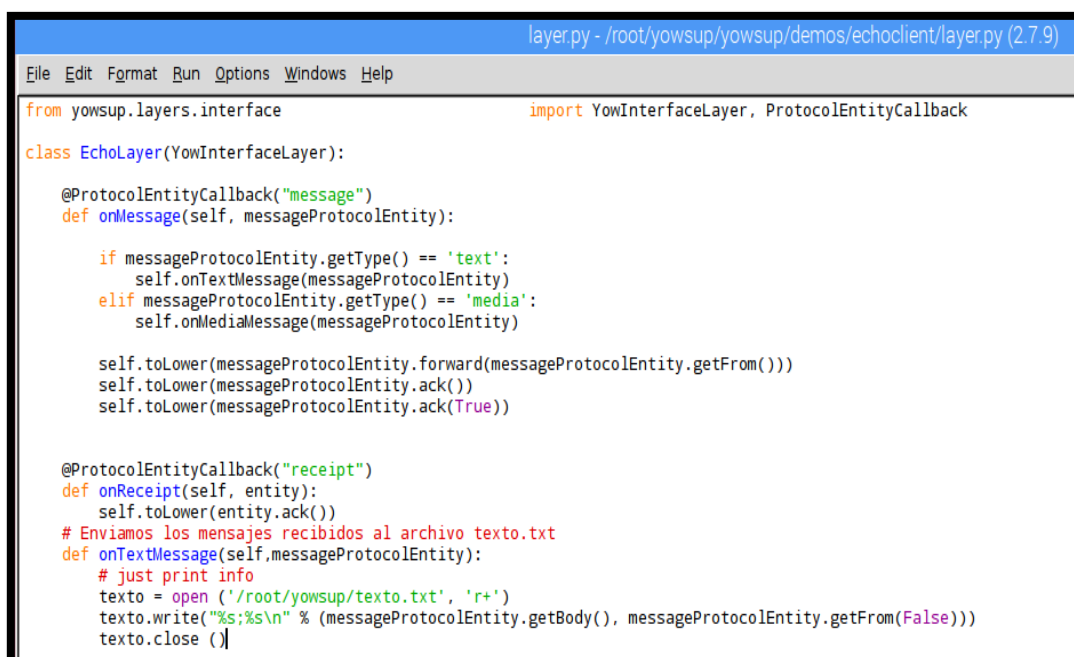
Descargar yowsup, para ello escribimos el siguiente comando:

- `git clone --recursive https://github.com/tgalal/yowsup.git`

Una vez descargado, entrar en la carpeta yowsup y dar permisos de ejecución al archivo yowsup-cli.

- `sudo chmod +x yowsup-cli`

En la figura 81 se observa el cambio en el fichero layer.py ubicado en el directorio /root/yowsup/yowsup/demos/echoclient/, para hacer que los mensajes recibidos se impriman en el fichero texto.txt ubicado en el directorio /root/yowsuo/.



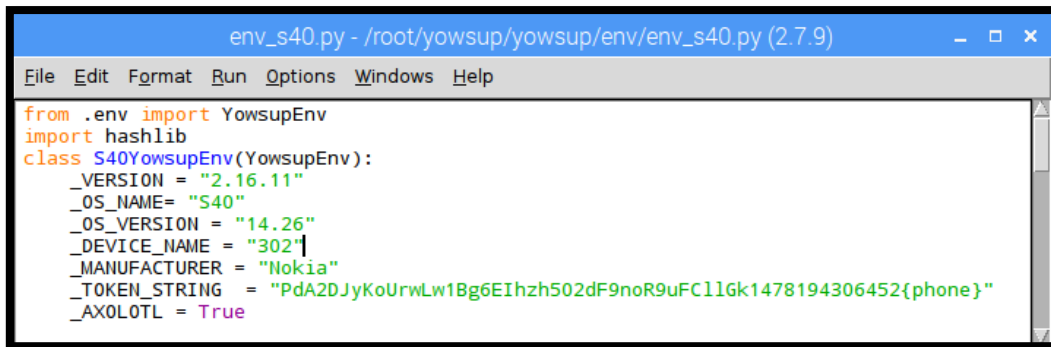
```
layer.py - /root/yowsup/yowsup/demos/echoclient/layer.py (2.7.9)
File Edit Format Run Options Windows Help
from yowsup.layers.interface import YowInterfaceLayer, ProtocolEntityCallback
class EchoLayer(YowInterfaceLayer):
    @ProtocolEntityCallback("message")
    def onMessage(self, messageProtocolEntity):
        if messageProtocolEntity.getType() == 'text':
            self.onTextMessage(messageProtocolEntity)
        elif messageProtocolEntity.getType() == 'media':
            self.onMediaMessage(messageProtocolEntity)
        self.toLower(messageProtocolEntity.forward(messageProtocolEntity.getFrom()))
        self.toLower(messageProtocolEntity.ack())
        self.toLower(messageProtocolEntity.ack(True))
    @ProtocolEntityCallback("receipt")
    def onReceipt(self, entity):
        self.toLower(entity.ack())
        # Enviamos los mensajes recibidos al archivo texto.txt
        def onTextMessage(self, messageProtocolEntity):
            # just print info
            texto = open('/root/yowsup/texto.txt', 'r+')
            texto.write("%s;%s\n" % (messageProtocolEntity.getBody(), messageProtocolEntity.getFrom(False)))
            texto.close ()
```

**Figura 81. Modificación del fichero layer.py de Yowsup.**

*Fuente: Captura de pantalla.*

En la figura 82 se muestra como se debe modificar el fichero env\_S40.py ubicado en el directorio /root/yowsup/yowsup/env/, para que al momento de registrar el número del usuario en WhatsApp no genere un error por ejecutar una simulación de una versión antigua del software de WhatsApp.





```
env_s40.py - /root/yowsup/yowsup/env/env_s40.py (2.7.9)
File Edit Format Run Options Windows Help
from .env import YowsupEnv
import hashlib
class S40YowsupEnv(YowsupEnv):
    _VERSION = "2.16.11"
    _OS_NAME = "S40"
    _OS_VERSION = "14.26"
    _DEVICE_NAME = "302"
    _MANUFACTURER = "Nokia"
    _TOKEN_STRING = "PdA2DJyKoUrwLw1Bg6EIhzh502dF9noR9uFC11Gk1478194306452{phone}"
    _AXOLOTL = True
```

**Figura 82. Actualización de versión WhatsApp en Yowsup.**

*Fuente: Captura de pantalla.*

El siguiente paso es registrar el número de teléfono del sistema para que lo utilice WhatsApp. Este número será el de la tarjeta sim del Gateway de voz.

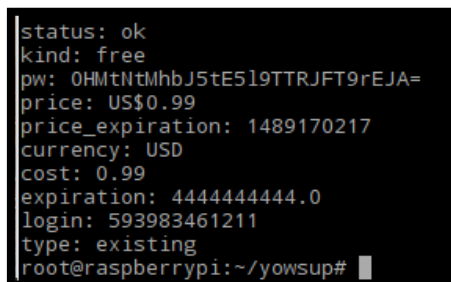
Generar el código de activación para el número de teléfono del sistema, el código llegara en un mensaje de texto enviado por un servidor de WhatsApp, usaremos el comando:

- `python yowsup-cli registration -r sms -p 593XXXXXXXXXX -C 593`

Una vez se reciba el código de activación, se introduce en yowsup: XXX-XXX

`python yowsup-cli registration -R XXX-XXX -p 593XXXXXXXXXX -C 593`

Culminado el proceso se verá una pantalla con los datos de usuario. Se debe copiar el código del parámetro pw: que será la contraseña privada para poder utilizar WhatsApp.



```
status: ok
kind: free
pw: 0HMtNtMhbJ5tE519TTRJFT9rEJA=
price: US$0.99
price_expiration: 1489170217
currency: USD
cost: 0.99
expiration: 444444444.0
login: 593983461211
type: existing
root@raspberrypi:~/yowsup#
```

**Figura 83. Contraseña proporcionada por WhatsApp en Yowsup.**

*Fuente: Captura de pantalla.*

Se guardan los datos de usuario en un fichero, con el fin de que cada vez que utilizemos la línea de comandos solo haya que indicar el fichero donde se encuentran los datos. Este fichero se crea en el directorio de yowsup, en este caso el nombre del fichero es yowsup-cli.config. El contenido del fichero:

```
cc=593
```

```
phone=593XXXXXXXXXX
```

```
id=(vacío)
```

```
password=contraseña recibida en el registro.
```

Para enviar un mensaje WhatsApp desde comandos hay que utilizar la siguiente línea:  
**python yowsup-cli demos -c yowsup-cli.config -s numerodestino "Mensaje".**

Nota: En el primer mensaje habrá un proceso de encriptación, quizás no se envíe volver a ejecutar el comando y funcionará perfectamente.

Para visualizar los mensajes recibidos hay que escribir la siguiente línea:  
**python yowsup-cli demos -e --config yowsup-cli.config.**

### 3.6.3 Instalación del software Mutt

Con esta forma de notificación el sistema enviara un correo al gerente con imágenes capturadas por la cámara de seguridad que detecto el movimiento, tras detectarse una intrusión. Para cumplir con esta función se hace uso del software Mutt, el cual permite enviar correos electrónicos a través del terminal.

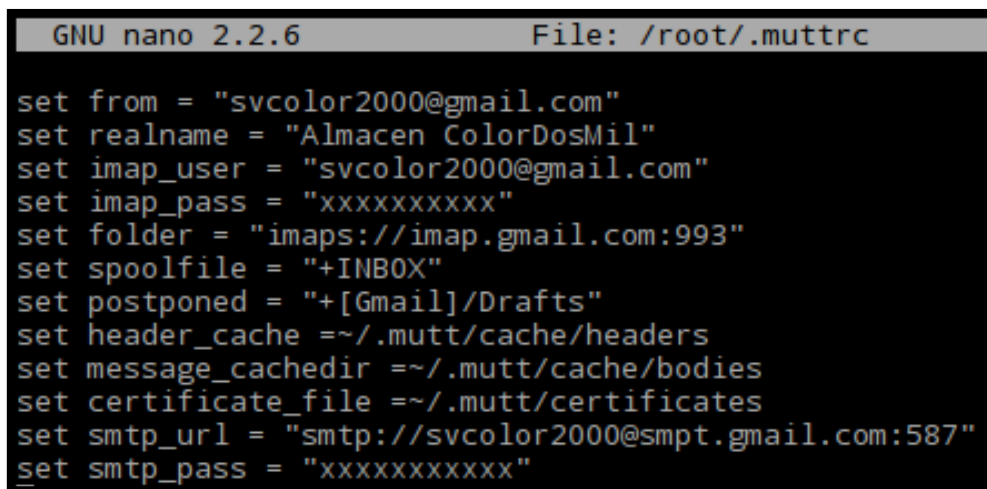
Para esta función se creó primero una cuenta Gmail para el sistema, que será la que se utilizará para enviar y recibir correos a través del software Mutt. Una vez creada la cuenta

Gmail, debe tener permisos para ser utilizada desde “aplicaciones menos seguras” para ello hay que ir a la configuración de google y activar esta opción en la siguiente dirección: <https://www.google.com/settings/security/lesssecureapps>.

Instalación de Mutt:

- Se actualizan los repositorios con el comando **sudo apt-get update**
- Se instala el paquete mutt con el comando **sudo apt-get install mutt**

Para configurar el programa, se debe crear un fichero oculto en el directorio del usuario administrador del sistema como se muestra en la figura 84. Se debe considerar que este caso el usuario va a ser root, por lo que se creará en el directorio /root con el siguiente comando: **sudo nano /root/.muttrc**, se debe sustituir ‘xxxxxxxxx’ por la contraseña del correo Gmail.



```

GNU nano 2.2.6 File: /root/.muttrc
set from = "svcolor2000@gmail.com"
set realname = "Almacen ColorDosMil"
set imap_user = "svcolor2000@gmail.com"
set imap_pass = "xxxxxxxxxxx"
set folder = "imaps://imap.gmail.com:993"
set spoolfile = "+INBOX"
set postponed = "+[Gmail]/Drafts"
set header_cache = ~/.mutt/cache/headers
set message_cachedir = ~/.mutt/cache/bodies
set certificate_file = ~/.mutt/certificates
set smtp_url = "smtp://svcolor2000@smtp.gmail.com:587"
set smtp_pass = "xxxxxxxxxxx"

```

**Figura 84. Fichero de configuración de cuenta Gmail en Mutt.**

*Fuente: Captura de pantalla.*

Se crea el siguiente directorio: **mkdir -p /root/.mutt/cache**

Ahora ya estará configurado el programa mutt para enviar mensajes a través del sistema.

Para enviar un mensaje de texto con archivo adjunto se debe seguir la siguiente sintaxis: **echo**

“Texto del mensaje” | mutt -s “Asunto del mensaje” destinatario @ gmail.com -a /ruta/completa/del/archivo.txt

La utilidad de Mutt, se ve reflejada en los diferentes Script de a ejecutarse en cada cámara, viendo cómo se puede entrelazar las diferentes aplicaciones para así programar medidas de seguridad y utilidades muy eficaces.

#### 6.2.4 Instalación de Telegram con Python

Para hacer más interactivo el sistema, es decir, que se vuelva una herramienta de comunicación con las cámaras de seguridad, se utilizó un programa en Python con una librería no muy conocida pero muy potente llamada Pexpect. Primero clonamos el repositorio a instalar Telegram messenger CLI con el siguiente comando: **git clone --recursive https://github.com/vysheng/tg.git && cd tg**. El proceso se muestra en la figura 85.

```

pi@raspberrypi:~ $ sudo git clone --recursive https://github.com/vysheng/tg.git && cd tg
Cloning into 'tg'...
remote: Counting objects: 4511, done.
remote: Total 4511 (delta 0), reused 0 (delta 0), pack-reused 4511
Receiving objects: 100% (4511/4511), 2.99 MiB | 375.00 KiB/s, done.
Resolving deltas: 100% (3041/3041), done.
Checking connectivity... done.
Submodule 'tgl' (https://github.com/vysheng/tgl.git) registered for path 'tgl'
Cloning into 'tgl'...
remote: Counting objects: 1555, done.
remote: Total 1555 (delta 0), reused 0 (delta 0), pack-reused 1555
Receiving objects: 100% (1555/1555), 1.02 MiB | 369.00 KiB/s, done.
Resolving deltas: 100% (1138/1138), done.
Checking connectivity... done.
Submodule path 'tgl': checked out 'ffb04caca71de0cddf28cd33a4575922900a59ed'
Submodule 'tl-parser' (https://github.com/vysheng/tl-parser) registered for path 'tl-parser'
Cloning into 'tl-parser'...
remote: Counting objects: 65, done.
remote: Total 65 (delta 0), reused 0 (delta 0), pack-reused 65
Unpacking objects: 100% (65/65), done.
Checking connectivity... done.
Submodule path 'tgl/tl-parser': checked out '36bf1902ff3476c75d0b1f42b34a91e944123b3c'
pi@raspberrypi:~/tg $

```

**Figura 85. Clonación del repositorio para Telegram.**

*Fuente: Captura de pantalla.*

Instalamos las siguientes librerías: `sudo apt-get install libreadline-dev libconfig-dev libssl-dev lua5.2 liblua5.2-dev libevent-dev`.

Ejecutamos el archivo de configuración y compilamos el programa

```
./configure # configura automáticamente el programa
```

```
make # compila el programa
```

Ejecutamos el programa, pasándole la clave pública

```
./bin/telegram-cli -k tg-server.pub
```

Al ejecutarse por primera vez, el programa nos pide un número telefónico con el siguiente formato +593XXXXXXXXXX se ingresa el número del móvil del proyecto. Si aún no estamos registrados el programa preguntará si queremos registrarnos, pedirá nuestro nombre y apellido. Posteriormente enviará un código de verificación a nuestro móvil. Después podremos añadir los contactos.

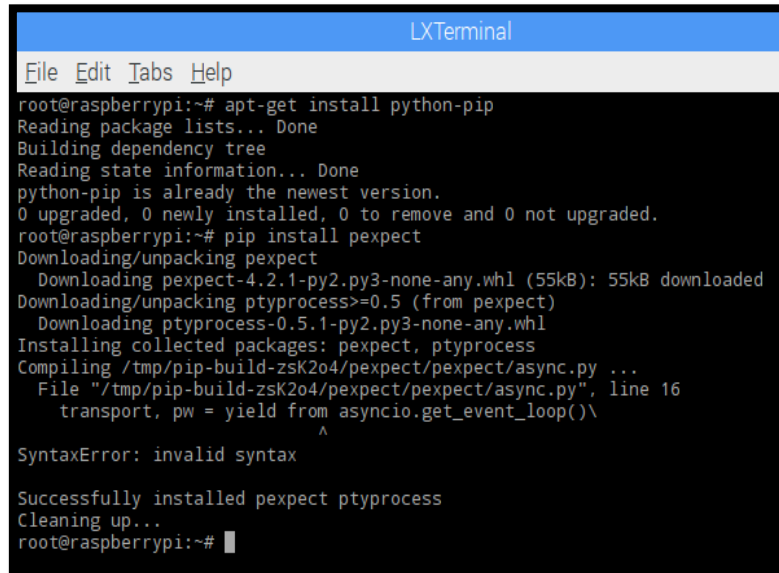
```
phone number: +593981595810
code ('CALL' for phone code): 43534
User Almacen ColorDosMil online (was online [2017/01/30 23:22:08])
> contact_list
Criss Movi
> msg Criss_Movi hola
[23:21] Criss Movi <<< hola
User Criss Movi online (was online [2017/01/30 23:26:59])
User Criss Movi marked read 1 outbox and 0 inbox messages
User Almacen ColorDosMil offline (was online [2017/01/30 23:22:07])
User Criss Movi is typing
[23:22] Criss Movi >>> Hola
User Criss Movi offline (was online [2017/01/30 23:22:33])
> █
```

Figura 86. Registro en inicio en Telegram-cli.  
Fuente: Captura de pantalla.

Pexpect

Pexpect se encuentra dentro PyPi, que es un repositorio lleno de programas de Python, este se instala ejecutando el siguiente comando en la terminal: **sudo apt-get install python-pip**.

Después descargamos Pexpect del repositorio ejecutando en la terminal: **pip install pexpect**.



```
LXTerminal
File Edit Tabs Help
root@raspberrypi:~# apt-get install python-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
python-pip is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@raspberrypi:~# pip install pexpect
Downloading/unpacking pexpect
  Downloading pexpect-4.2.1-py2.py3-none-any.whl (55kB): 55kB downloaded
Downloading/unpacking ptyprocess>=0.5 (from pexpect)
  Downloading ptyprocess-0.5.1-py2.py3-none-any.whl
Installing collected packages: pexpect, ptyprocess
Compiling /tmp/pip-build-zsK2o4/pexpect/pexpect/async.py ...
  File "/tmp/pip-build-zsK2o4/pexpect/pexpect/async.py", line 16
    transport, pw = yield from asyncio.get_event_loop()\
                    ^
SyntaxError: invalid syntax

Successfully installed pexpect ptyprocess
Cleaning up...
root@raspberrypi:~#
```

**Figura 87. Instalación de librería pexpect en Python.**

*Fuente: Captura de pantalla.*

## Agregar Contactos

Telegram sólo permite enviar mensajes a números agregados a la lista de contactos. Se logró este cometido con el siguiente programa a través de Python el cual debe guardarse en la misma carpeta que esta Telegram en el directorio /root/tg/:

```
#!/usr/bin/env
import pexpect
import time

telefono = '+593xxxxxxxxx'
nombre = 'xxxxxxx'
apellido = 'xxxxxxx'
telegram = pexpect.spawn('./telegram -k tg.pub')
self.child.expect('0m')
self.child.sendline('add_contact '+telefono+' '+nombre+' '+apellido)
print ('El contacto '+nombre+' '+apellido+' con el teléfono '+telefono)
self.child.expect('0m')
self.child.sendline('quit')
```

**Figura 88. Guardado de Contactos en Telegram.**

*Fuente: Captura de pantalla.*

Envió de un mensaje

Con Telegram sólo podemos enviar mensajes a contactos ya agregados anteriormente.

Para enviar un mensaje guardamos el siguiente código en la misma carpeta que esta Telegram en el directorio /root/tg/.

```
#!/usr/bin/env
import pexpect

contacto = "xxxx_xxxx"          #Contacto a quien va el mensaje
mensaje = "Probando desde Python!!" #Mensaje a enviar
telegram = pexpect.spawn('./telegram -k tg.pub') #Inicia Telegram
telegram.expect('0m')          #Espera a que termine de iniciar
telegram.sendline('msg '+contacto+' '+mensaje) #Ejecuta el comando msg
print ('Mensaje enviado a '+ contacto)        #Notifica que ya se ha mandado el mensaje
telegram.sendline('quit')        #cierra Telegram
```

**Figura 89. Envío de mensaje con Telegram.**

*Fuente: Captura de pantalla.*

### 3.6.5 Creación de Scripts para el control y alerta de eventos del sistema

El control para la activación y desactivación de la alarma es realizado por la ejecución de scripts que contienen una secuencia de comandos programada. Esta acción es controlada por el software Asterisk mediante un plan de marcado, y un softphone para ejecutar el control en el entorno local, de forma remota se utiliza la aplicación Zoiper configurada con una cuenta IAX para el control de la alarma.

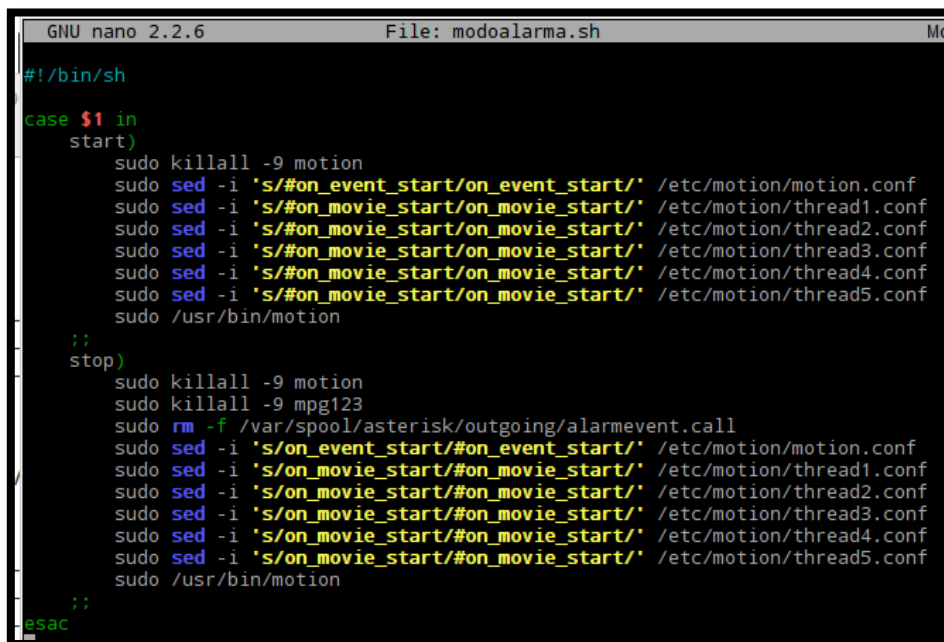
La reacción frente a la detección de un evento será controlada por scripts, en los cuales está programada una secuencia de comandos a ejecutarse, en donde interviene la acción de softwares como Asterisk que ejecuta la llamada al gerente por medio de un teléfono móvil el cual actúa como Gateway de voz hacia la red de telefonía móvil, el software Mutt como gestor de envío de correo electrónico con imágenes de la cámara que ha detectado el movimiento, el

software Mpg123 el cual permite la reproducción de la sirena, y el software Telegram para el envío de mensajes a través de la red social del mismo nombre.

### 3.6.5.1 Scripts para el control del sistema

Los scripts presentados a continuación contienen una secuencia de comandos que serán ejecutados para el control del sistema de alarma. Estos scripts serán gestionados por el software Asterisk y el software Yowsup.

Figura 90 Script de control de activación y desactivación de alarma: **modoalarma.sh**.



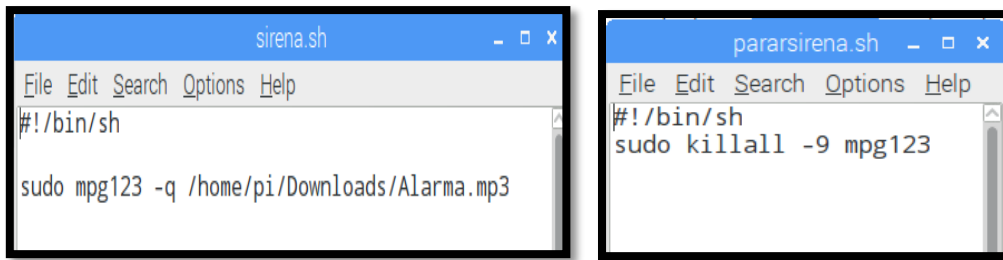
```
GNU nano 2.2.6 File: modoalarma.sh
#!/bin/sh
case $1 in
start)
sudo killall -9 motion
sudo sed -i 's/#on_event_start/on_event_start/' /etc/motion/motion.conf
sudo sed -i 's/#on_movie_start/on_movie_start/' /etc/motion/thread1.conf
sudo sed -i 's/#on_movie_start/on_movie_start/' /etc/motion/thread2.conf
sudo sed -i 's/#on_movie_start/on_movie_start/' /etc/motion/thread3.conf
sudo sed -i 's/#on_movie_start/on_movie_start/' /etc/motion/thread4.conf
sudo sed -i 's/#on_movie_start/on_movie_start/' /etc/motion/thread5.conf
sudo /usr/bin/motion
;;
stop)
sudo killall -9 motion
sudo killall -9 mpg123
sudo rm -f /var/spool/asterisk/outgoing/alarmevent.call
sudo sed -i 's/on_event_start/#on_event_start/' /etc/motion/motion.conf
sudo sed -i 's/on_movie_start/#on_movie_start/' /etc/motion/thread1.conf
sudo sed -i 's/on_movie_start/#on_movie_start/' /etc/motion/thread2.conf
sudo sed -i 's/on_movie_start/#on_movie_start/' /etc/motion/thread3.conf
sudo sed -i 's/on_movie_start/#on_movie_start/' /etc/motion/thread4.conf
sudo sed -i 's/on_movie_start/#on_movie_start/' /etc/motion/thread5.conf
sudo /usr/bin/motion
;;
esac
```

Figura 90. Script de control modoalarma.sh.

*Fuente: Captura de pantalla.*

En la figura 91 se muestran los scripts que controlan la activación independiente del sonido de sirena reproducido por los altavoces mediante el software Mpg123 previamente instalado con el comando: **sudo apt-get install mpg123**. Esta acción se integra en la detección de un evento cuando el sistema de alarma por detección de movimiento este activado.



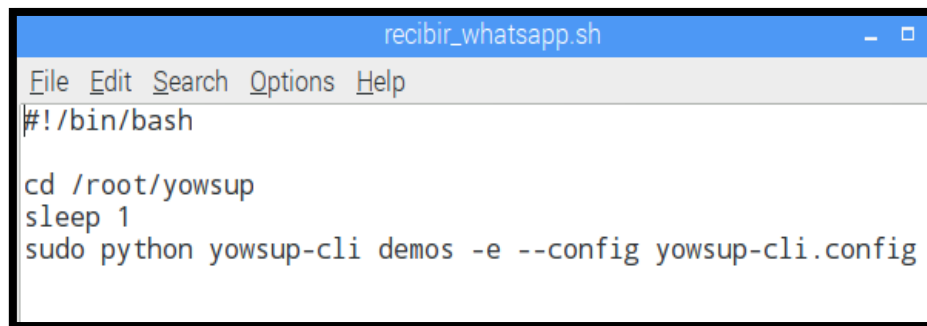


The image shows two terminal windows side-by-side. The left window is titled 'sirena.sh' and contains the following code: `#!/bin/sh` followed by `sudo mpg123 -q /home/pi/Downloads/Alarma.mp3`. The right window is titled 'pararsirena.sh' and contains the following code: `#!/bin/sh` followed by `sudo killall -9 mpg123`. Both windows have a menu bar with 'File', 'Edit', 'Search', 'Options', and 'Help'.

**Figura 91. Scripts de activación y desactivación de la sirena.**

*Fuente: Captura de pantalla.*

El script mostrado en la figura 92 es el encargado de recibir los mensajes de WhatsApp y enviarlos a un fichero de texto, esto fue configurado en la instalación del software Yowsup, este script se ejecuta continuamente en segundo plano.

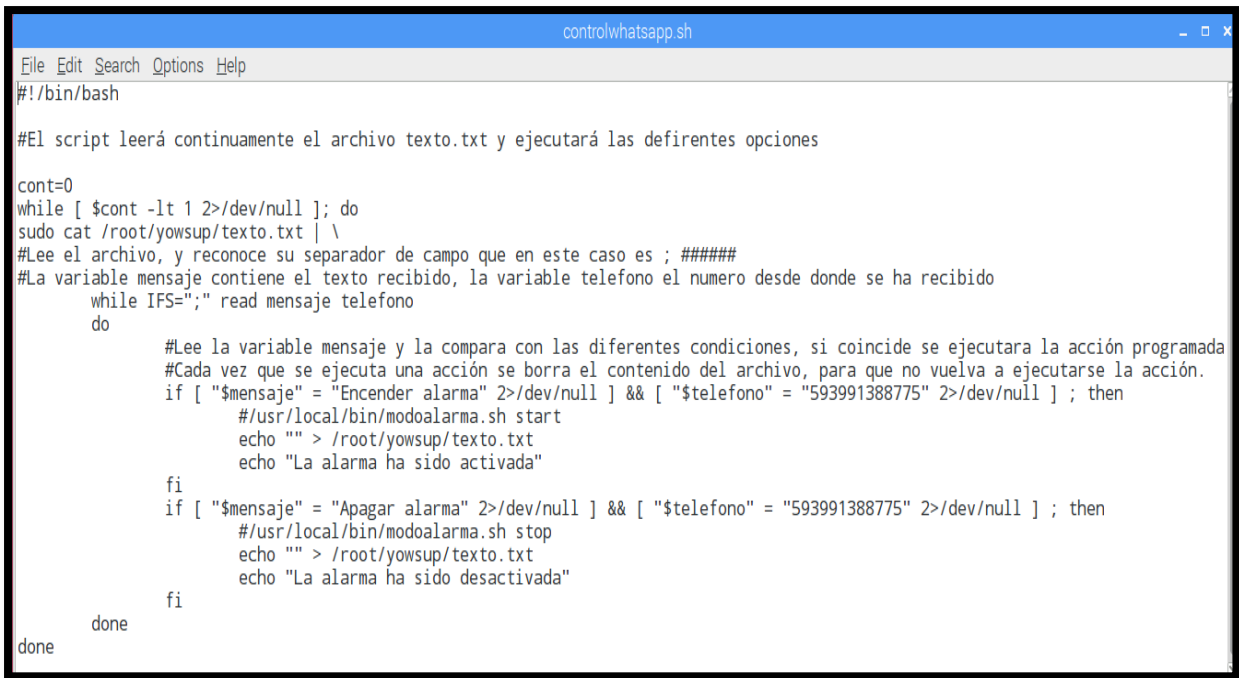


The image shows a terminal window titled 'recibir\_whatsapp.sh'. The code inside is: `#!/bin/bash`, `cd /root/yowsup`, `sleep 1`, and `sudo python yowsup-cli demos -e --config yowsup-cli.config`. The window has a menu bar with 'File', 'Edit', 'Search', 'Options', and 'Help'.

**Figura 92. Script de recepción de mensajes WhatsApp.**

*Fuente: Captura de pantalla.*

El script controlwhatsapp.sh también se ejecuta en segundo plano y lee continuamente el fichero de texto, en donde se guardan los mensajes recibidos por WhatsApp, comprueba que el mensaje tenga el texto exacto y corresponda al número de teléfono del gerente para ejecutar la activación o desactivación del sistema de alarma. Se muestra el script en la figura 93.



```

controlwhatsapp.sh
File Edit Search Options Help
#!/bin/bash

#El script leerá continuamente el archivo texto.txt y ejecutará las defirentes opciones

cont=0
while [ $cont -lt 1 2>/dev/null ]; do
sudo cat /root/yowsup/texto.txt | \
#Lee el archivo, y reconoce su separador de campo que en este caso es ; #####
#La variable mensaje contiene el texto recibido, la variable telefono el numero desde donde se ha recibido
  while IFS=";" read mensaje telefono
  do
    #Lee la variable mensaje y la compara con las diferentes condiciones, si coincide se ejecutara la acción programada
    #Cada vez que se ejecuta una acción se borra el contenido del archivo, para que no vuelva a ejecutarse la acción.
    if [ "$mensaje" = "Encender alarma" 2>/dev/null ] && [ "$telefono" = "593991388775" 2>/dev/null ] ; then
      #/usr/local/bin/modoalarma.sh start
      echo "" > /root/yowsup/texto.txt
      echo "La alarma ha sido activada"
    fi
    if [ "$mensaje" = "Apagar alarma" 2>/dev/null ] && [ "$telefono" = "593991388775" 2>/dev/null ] ; then
      #/usr/local/bin/modoalarma.sh stop
      echo "" > /root/yowsup/texto.txt
      echo "La alarma ha sido desactivada"
    fi
  done
done

```

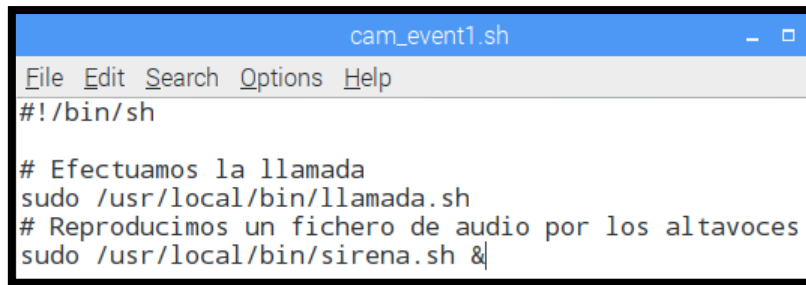
**Figura 93. Script de control de alarma por WhatsApp.**

*Fuente: Captura de pantalla.*

### 3.6.5.2 scripts para alerta de eventos

Los scripts presentados a continuación contienen una secuencia de comandos que serán ejecutados frente a la detección de movimiento en un área vigilada siempre que el sistema de alarma este activado. Estos scripts serán gestionados por el software Motion el cual mediante la gestión de las cámaras dispara el primer evento a realizarse, el software Asterisk gestiona la llamada al móvil del gerente, el software Mutt envían un correo electrónico con imágenes capturadas por la cámara que detectó el evento y el software Telegram envía un mensaje a la aplicación del gerente en esta red social.

El script `cam_event1.sh` el cual se muestra en la figura 94, en primera instancia hace la petición de una llamada hacia el gerente, seguidamente dispara un sonido de sirena frente a la detección de un movimiento. El software Asterisk se encargará de la gestión de la llamada presentando las opciones programadas en el IVR del plan de marcado.



```

cam_event1.sh
File Edit Search Options Help
#!/bin/sh

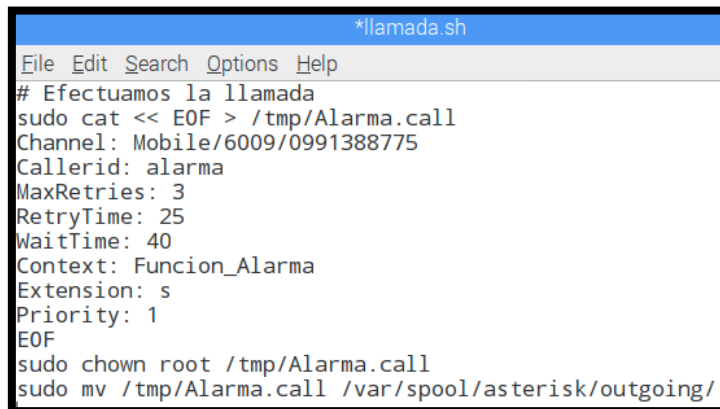
# Efectuamos la llamada
sudo /usr/local/bin/llamada.sh
# Reproducimos un fichero de audio por los altavoces
sudo /usr/local/bin/sirena.sh &|

```

**Figura 94. Script disparo de evento.**

*Fuente: Captura de pantalla.*

El script llamada.sh mostrado en la figura 95 realiza la petición de una llamada hacia el número telefónico móvil del gerente, en donde se especifica el canal hacia la red telefonía móvil por medio del Gateway de voz, se realizarán 3 intentos dentro del contexto Funcion\_Alarma en donde encuentra el IVR con las opciones para esta llamada.



```

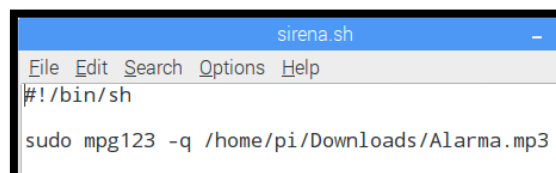
*llamada.sh
File Edit Search Options Help
# Efectuamos la llamada
sudo cat << EOF > /tmp/Alarma.call
Channel: Mobile/6009/0991388775
Callerid: alarma
MaxRetries: 3
RetryTime: 25
WaitTime: 40
Context: Funcion_Alarma
Extension: s
Priority: 1
EOF
sudo chown root /tmp/Alarma.call
sudo mv /tmp/Alarma.call /var/spool/asterisk/outgoing/

```

**Figura 95. Script generación de llamada.**

*Fuente: Captura de pantalla.*

La figura 96 muestra el contenido del script sirena.sh el cual dispara el sonido.



```

sirena.sh
File Edit Search Options Help
#!/bin/sh

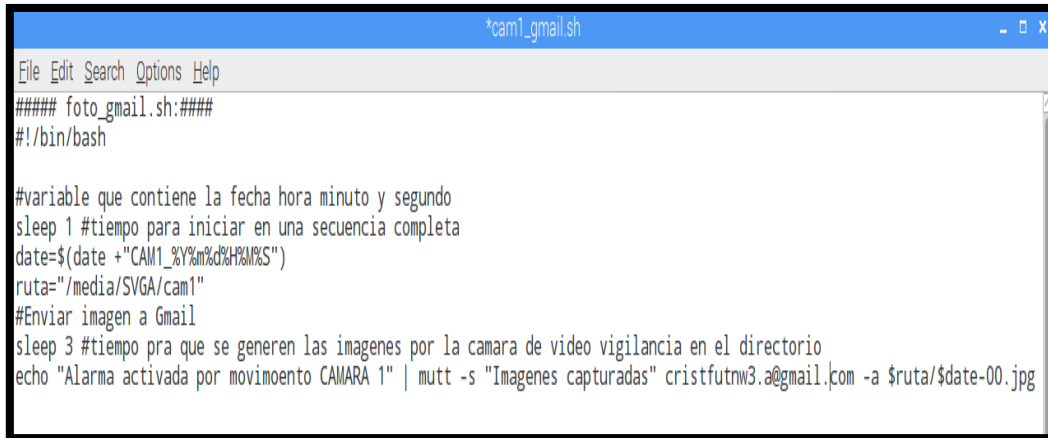
sudo mpg123 -q /home/pi/Downloads/Alarma.mp3

```

**Figura 96. Script generación de sirena.**

*Fuente: Captura de pantalla.*

En la figura 97 se muestra la configuración del script para el envío de un correo con la captura de imágenes generada por la cámara que detectó el movimiento y también un mensaje por Telegram indicando la cámara que detecto el movimiento y un mensaje de alerta.



```

*cam1_gmail.sh
File Edit Search Options Help
##### foto_gmail.sh:####
#!/bin/bash

#variable que contiene la fecha hora minuto y segundo
sleep 1 #tiempo para iniciar en una secuencia completa
date=$(date +"CAM1_%Y%m%d%H%M%S")
ruta="/media/SVGA/cam1"
#Enviar imagen a Gmail
sleep 3 #tiempo pra que se generen las imagenes por la camara de video vigilancia en el directorio
echo "Alarma activada por movimoento CAMARA 1" | mutt -s "Imagenes capturadas" cristfutw3.a@gmail.com -a $ruta/$date-00.jpg

```

**Figura 97. Script de envío de correo y mensaje por Telegram.**

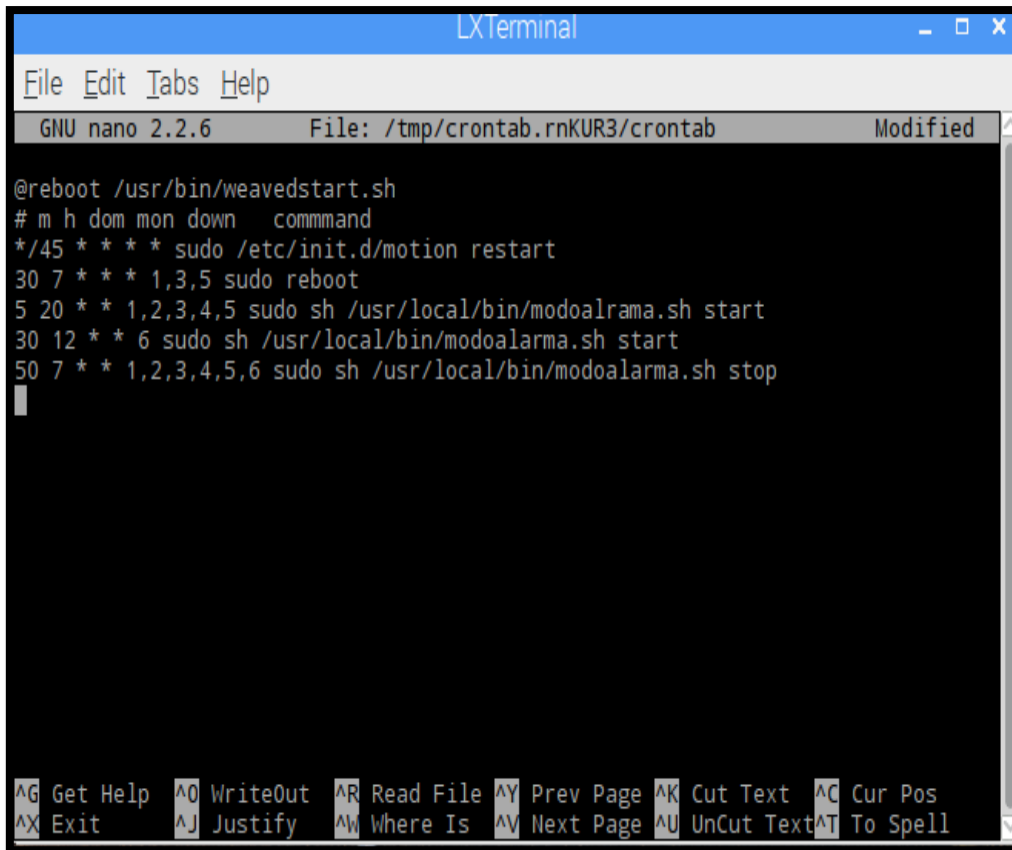
*Fuente: Captura de pantalla.*

## 3.7 Administración de tareas usando Cron

Para editar el fichero de configuración crontab se ingresa como usuario root dentro del fichero se programar las tareas a ejecutarse automáticamente:

### 3.7.1 Herramienta Crontab

Ingresando el comando: **crontab -e**, inmediatamente se despliega un menú para seleccionar el editor de texto que deseamos usar, la opción dos es el editor nano. Posteriormente accederá al fichero de configuración de la herramienta, como se observa en la figura 98. Se debe recordar que después de cada modificación en el fichero crontab es necesario reiniciar el servicio de Cron para que el sistema tome las nuevas instrucciones programas, esto se realiza insertando en el terminal de root el comando: **sudo service cron restart**.

A screenshot of an LXTerminal window showing the nano text editor editing a crontab file. The window title is "LXTerminal". The editor's status bar shows "GNU nano 2.2.6", "File: /tmp/crontab.rnKUR3/crontab", and "Modified". The crontab file content is as follows:

```
@reboot /usr/bin/weavedstart.sh
# m h dom mon dow   command
*/45 * * * * sudo /etc/init.d/motion restart
30 7 * * * 1,3,5 sudo reboot
5 20 * * 1,2,3,4,5 sudo sh /usr/local/bin/modoalrama.sh start
30 12 * * 6 sudo sh /usr/local/bin/modoalarma.sh start
50 7 * * 1,2,3,4,5,6 sudo sh /usr/local/bin/modoalarma.sh stop
```

The bottom of the terminal shows the nano editor's help menu with various keyboard shortcuts.

**Figura 98.** Fichero crontab administración automática de procesos.  
*Fuente: Captura de pantalla.*

## **CAPÍTULO IV**

### **4. PRUEBAS DE FUNCIONAMIENTO Y CORRECCIÓN DE ERRORES**

#### **4.1 Generalidades**

En este capítulo se realizó las pruebas para verificar el funcionamiento del Sistema de video vigilancia y alarma basada en la detección de movimiento siguiendo el manual de pruebas en el anexo 8.

Se verificó que los softwares instalados funcionen e inicien correctamente en función de los ficheros de configuración de cada software, se inició por el reconocimiento de las cámaras por el software Motion y se probó el funcionamiento del primer modo del sistema de solo monitoreo, con el control activación y desactivación del sistema de alarma por medio del software Asterisk local y remotamente.

La funcionalidad del segundo modo del sistema fue verificada, de modo que se recibieron todas las alertas programadas en los scripts controladores de eventos. Se verificó la generación de la llamada, el disparo de la sirena, envío de mensajes tanto de correo como por Telegram.

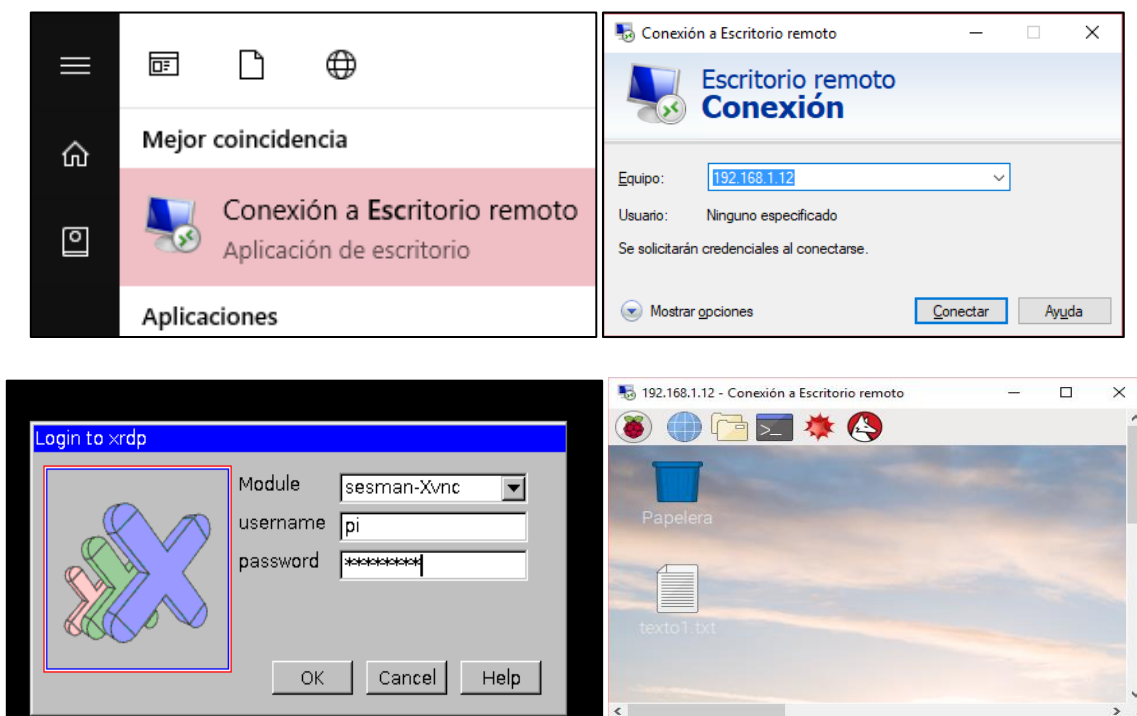
Para finalizar se comprobó el acceso al sistema local y remotamente por medio de un Smartphone y desde una computadora portátil, se comprobó la presentación del video en la página web en un monitor en el establecimiento de la empresa Almacén Color 2000.

## 4.2 Métodos de acceso para administración y configuración del sistema de video vigilancia.

Siguiendo el manual de pruebas de funcionamiento del sistema del anexo 8, se procedió a la verificación de acceso local y remoto al sistema.

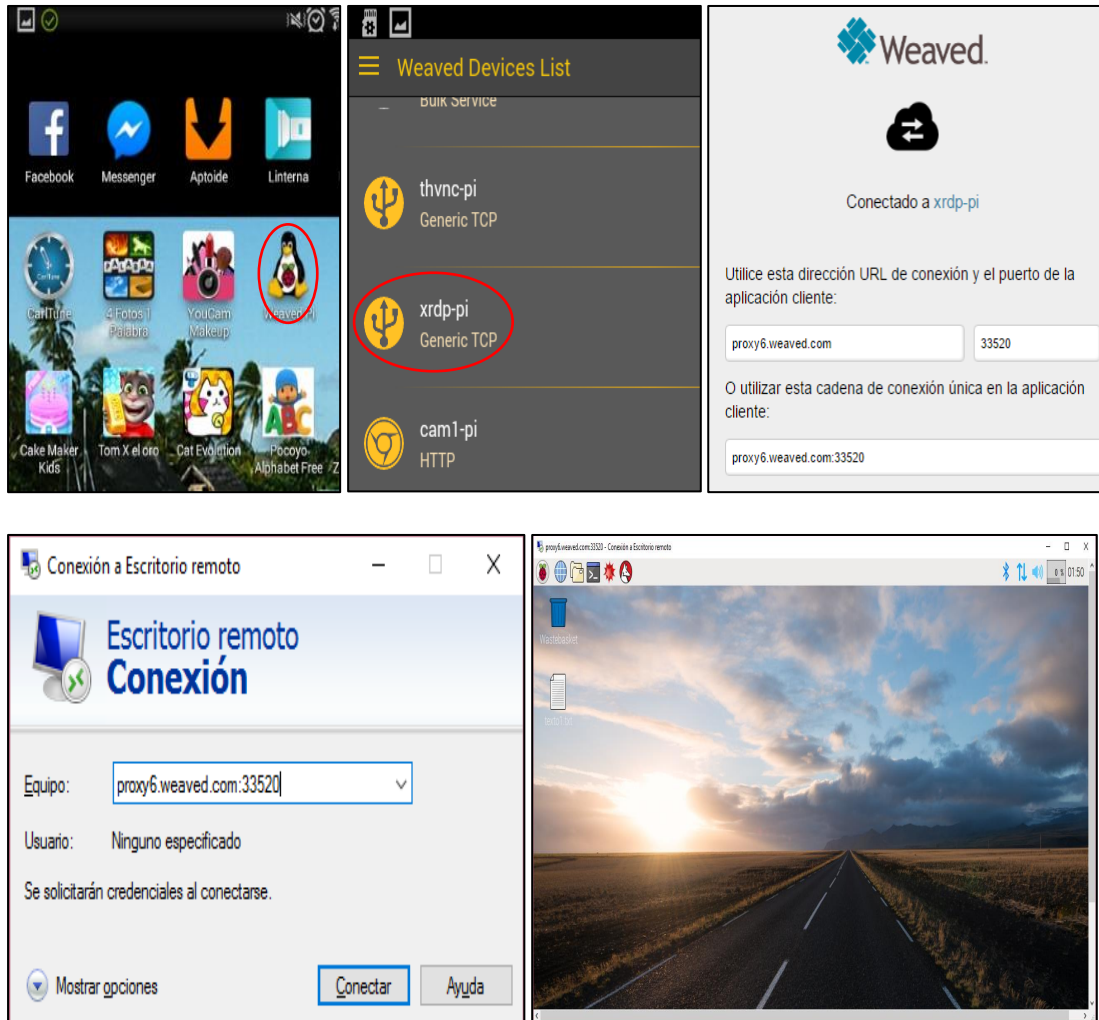
En primer lugar se comprobó la conexión por escritorio remoto del sistema en donde es posible administrar y realizar configuraciones si se requieren, la verificación se realizó en el entorno de la red local de la empresa, se utilizó una Laptop, Tablet y un Smartphone. Para la conexión mediante la Tablet y Smartphone se utilizó la aplicación Remote ToGo.

En la figura 99 se muestran los resultados del acceso al sistema conectado desde la red de área local de la empresa siguiendo el anexo 8, para el acceso se solicitara el usuario y contraseña correspondiente al administrador.



**Figura 99. Acceso al sistema desde red local.**  
*Fuente: Captura de pantalla.*

En la figura 100 se muestran los resultados del acceso al sistema conectado desde Internet siguiendo el anexo 8, para el acceso se solicitara el usuario y contraseña correspondiente al administrador.



**Figura 100. Acceso al sistema desde Internet.**  
Fuente: Captura de pantalla.

### 4.3 Comprobación del funcionamiento del software de gestión de cámaras.

Primero se comprobó que el software Motion esté en funcionamiento y tenga un proceso activo, lo siguiente fue comprobar el reconocimiento de las cámaras por el sistema.



1. `sudo /etc/init.d/motion status` # comprueba estado del software.
2. `pidof motion` # indica el número del proceso actual.
3. `lsusb && ls /dev` # lista los dispositivos USB y sus drivers.

Se reinició el sistema y en la figura 101 se observa el estado del software Motion es activo, tiene signado un numero de proceso, las cámaras han sido reconocidas y sus drivers cargados.

```

pi@raspberrypi: ~
File Edit Tabs Help
pi@raspberrypi:~$ sudo /etc/init.d/motion status
● motion.service - LSB: Start Motion detection
   Loaded: loaded (/etc/init.d/motion)
   Active: active (exited) since Fri 2017-02-10 18:34:34 ECT; 3 days ago

Feb 10 18:34:33 raspberrypi systemd[1]: Starting LSB: Start Motion detection...
Feb 10 18:34:34 raspberrypi motion[529]: Not starting motion daemon, disable...
Feb 10 18:34:34 raspberrypi systemd[1]: Started LSB: Start Motion detection.
Hint: Some lines were ellipsized, use -l to show in full.
pi@raspberrypi:~$ pidof motion
10756
pi@raspberrypi:~$ lsusb
Bus 001 Device 042: ID 1908:2311 GEMBIRD
Bus 001 Device 041: ID 1871:0142 Aveo Technology Corp.
Bus 001 Device 040: ID 0a12:0001 Cambridge Silicon Radio, Ltd Bluetooth Dongle (
HCI mode)
Bus 001 Device 038: ID 0424:ec00 Standard Microsystems Corp. SMC9512/9514 Fast
Ethernet Adapter
Bus 001 Device 037: ID 0424:9514 Standard Microsystems Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
pi@raspberrypi:~$ ls /dev
autofs          mapper          ram7            tty23           tty5            vcs
block          media0         ram8            tty24           tty50           vcs1
btrfs-control  media1         ram9            tty25           tty51           vcs2
bus            mem            random          tty26           tty52           vcs3
cachefiles     memory_bandwidth raw             tty27           tty53           vcs4
char           mmcblk0        rfcill         tty28           tty54           vcs5
console        mmcblk0p1     serial1        tty29           tty55           vcs6
cpu_dma_latency mmcblk0p2     shm            tty3            tty56           vcs7
cuse           mqueue        snd            tty30           tty57           vcsa
disk           net            stderr         tty31           tty58           vcsa1
fb0            network_latency stdin          tty32           tty59           vcsa2
fd             network_throughput stdout         tty33           tty6            vcsa3
full           null           tty            tty34           tty60           vcsa4
fuse           ppp           tty0           tty35           tty61           vcsa5
gpiomem        ptmx          tty1           tty36           tty62           vcsa6
hwrng          pts           tty10          tty37           tty63           vcsa7
initctl        ram0          tty11          tty38           tty7            vcsm
input          ram1          tty12          tty39           tty8            vhci
lmsg           ram10         ttv13          ttv4            ttv9            video0

```

Figura 101. Estado de Motion y detección de cámaras.

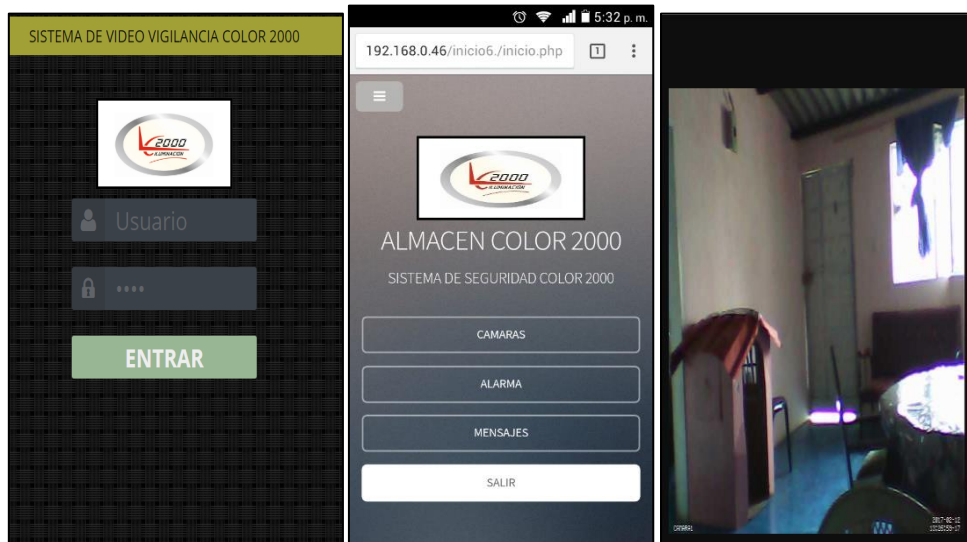
Fuente: Captura de pantalla.

## 4.4 Verificación de los modos de funcionamiento del sistema.

### 4.4.1 Verificación del modo de Solo Monitoreo.

En el siguiente paso se comprobó la funcionalidad en el sistema de videovigilancia, arrancando el sistema en modo de solo monitoreo, para ello se accedió a la interfaz web, mediante un navegador y se digitó la dirección IP del Raspberry con el puerto de escucha perteneciente a cada cámara, se verifico la visualización de vídeo transmitido en red local e Internet capturado por cada cámara.

En la Figura 102 se visualiza el resultado obtenido ingresando al navegador web y digitando la dirección IP más el puerto de comunicación de la cámara correspondiente y mediante la aplicación Weaved pi en la Tablet y Smartphone, esto en la red local de la empresa.




**Figura 102. Captura de video de cámaras.**

*Fuente: Captura de pantalla.*

En la Figura 103 se visualiza el resultado obtenido ingresando al navegador web y digitando la dirección URL <https://developer.weaved.com/portal/login.php>, ingresar a la cuenta con el usuario y contraseña correspondiente y seleccionar la cámara que desea observar,

para visualizar mediante la aplicación Weaved pi en la Tablet y Smartphone, esto requiere conexión a Internet.



Nombre	Tipo	Estado	
cam1-pi	HTTP	en línea	Compartir   ajustes
CAM2-pi	HTTP	en línea	Compartir   ajustes
cam3-pi	HTTP	en línea	Compartir   ajustes
cam4-pi	HTTP	en línea	Compartir   ajustes



**Figura 103. Acceso a una cámara desde Internet.**

*Fuente: Captura de pantalla.*

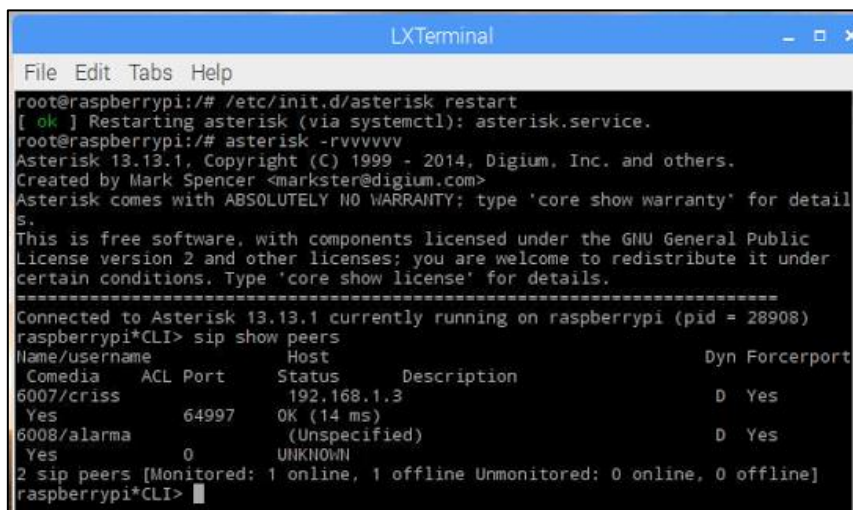
En este modo de funcionamiento el sistema, graba el video e imágenes capturadas en el disco del almacenamiento, clasificándolo en un directorio por cada cámara.

#### 4.4.2 Verificación del modo de Alarma y Monitoreo.

Primero se verificó que el software Asterisk este ejecutándose, luego se comprobó el registro y funcionamiento del softphone con la centralita de voz sobre Ip Asterisk, también se verificó que el Gateway de voz hacia la red de telefonía móvil esté conectado mediante la tecnología Bluetooth. Esto se realizó dentro de la consola de Asterisk.

1. `sudo /etc/init.d/asterisk status` # Muestra estado del software.
2. `sudo asterisk -rvvvvv` # Ingresa a la consola de Asterisk.
3. `sip show peers` # Muestra el estado de los usuarios sip.
4. `mobile show devices` # Muestra el estado del Gateway de voz.

En la figura 104 se muestran los resultados de la verificación del control del sistema.



```

LXTerminal
File Edit Tabs Help
root@raspberrypi:/# /etc/init.d/asterisk restart
[ ok ] Restarting asterisk (via systemctl): asterisk.service.
root@raspberrypi:/# asterisk -rvvvvv
Asterisk 13.13.1, Copyright (C) 1999 - 2014, Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
-----
Connected to Asterisk 13.13.1 currently running on raspberrypi (pid = 28908)
raspberrypi*CLI> sip show peers
Name/username      Host                Dyn Forcerport
-----
Comedia    ACL Port    Status    Description
6007/criss  192.168.1.3  D Yes
Yes        64997      OK (14 ms)
6008/alarma  (Unspecified)  D Yes
Yes        0          UNKNOWN
2 sip peers [Monitored: 1 online, 1 offline Unmonitored: 0 online, 0 offline]
raspberrypi*CLI>

```

**Figura 104. Verificación del software de control Asterisk.**

*Fuente: Captura de pantalla.*

En la figura 105 a continuación se muestra la inicialización del Gateway de voz y su estado, el cual es fundamental para la alerta de eventos.

```

Asterisk Ready.
> Saved useragent "Zoiper rv2.8.26" for peer 6007
raspberrypi*CLI> sip show peers
Name/username      Host                               Dyn Forcerport
Comedia    ACL Port      Status      Description
6007/criss  192.168.1.3   OK (42 ms)  D Yes
Yes        64997
6008/alarma (Unspecified) D Yes
Yes        0            UNKNOWN
2 sip peers [Monitored: 1 online, 1 offline Unmonitored: 0 online, 0 offline]
-- Bluetooth Device 6009 has connected. initializing...
-- Bluetooth Device 6009 initialized and ready.
raspberrypi*CLI> mobile show devices
ID      Address          Group Adapter      Connected State      SMS
6009   6C:E9:07:A7:11:E9 1   raspberrypi3     Yes      Free      No
raspberrypi*CLI>

```

**Figura 105. Verificación de esta del Gateway de voz en Asterisk.**

*Fuente: Captura de pantalla.*

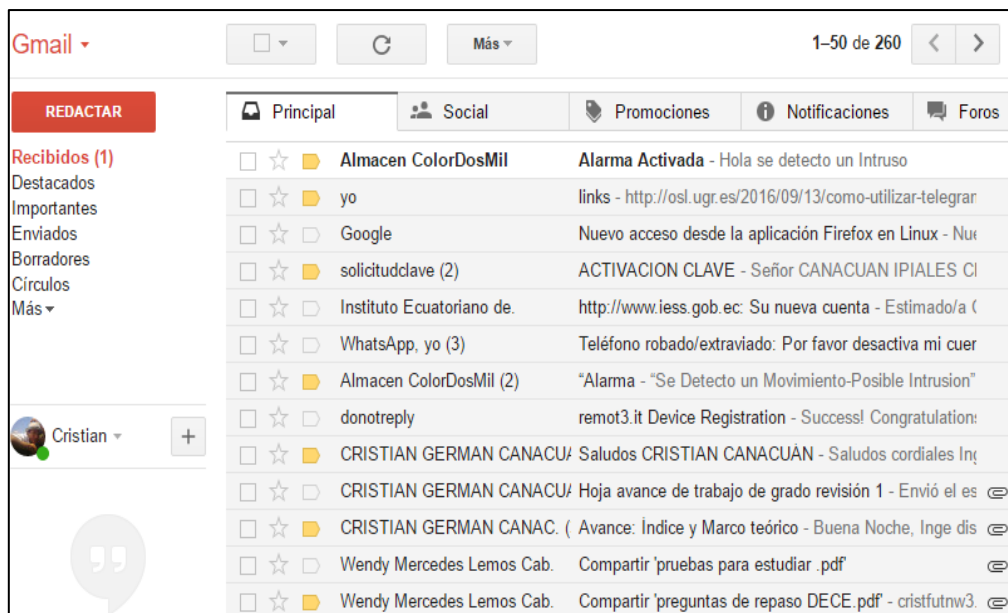
Siguiendo el anexo 8 para la verificación de detección de movimiento y control de eventos, se simuló una intrusión, de esta forma se verificó que tanto la configuración de los softwares y scripts actúen correctamente.

#### **4.4.3 Verificación de detección de movimiento y control de eventos.**

En primera instancia se evidencia el sonido reproducido por los altavoces que corresponde a la ejecución del script de activación de alarma (sirena.sh) y el software mpg123 que gestiona la reproducción del sonido.

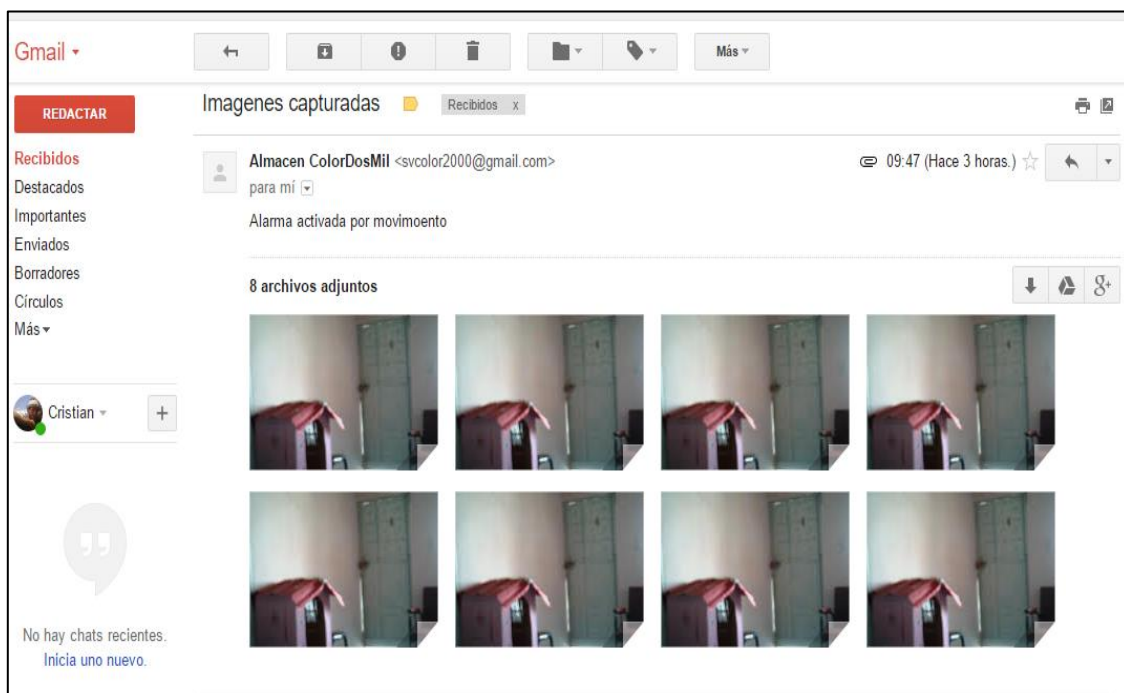
Simultáneamente se envía un correo electrónico con imágenes correspondientes a la intrusión, esta acción es ejecutada por el script (camx\_gmail.sh), es gestionado por el software mutt. Se envía un mensaje instantáneo por medio de Telegram esto es gestionado por el script (mesj\_tel.py) y gestionado por el software Telegram.

En las figuras 106, 107 y 108 se verificó el envío del correo con las imágenes capturadas por la cámara, y el envío del mensaje por Telegram.



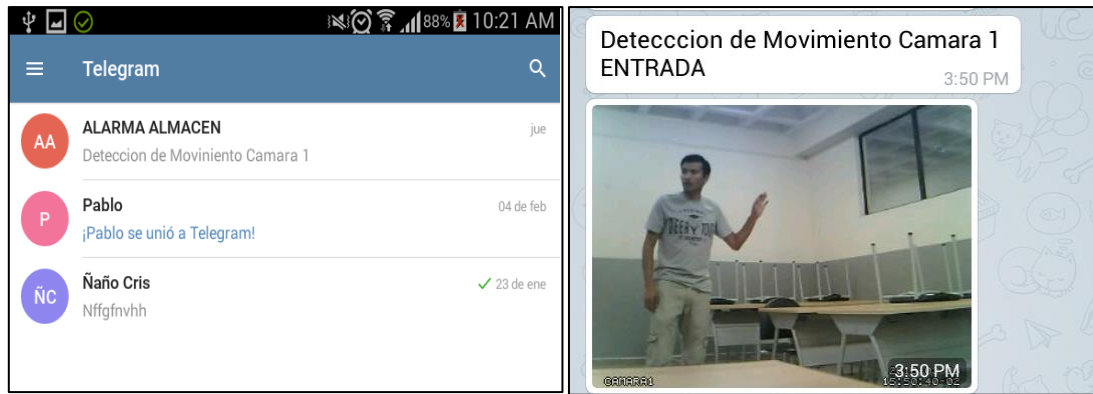
**Figura 106. Verificación de envío de correo.**

*Fuente: Captura de pantalla.*



**Figura 107. Verificación de envío de Imágenes al correo.**

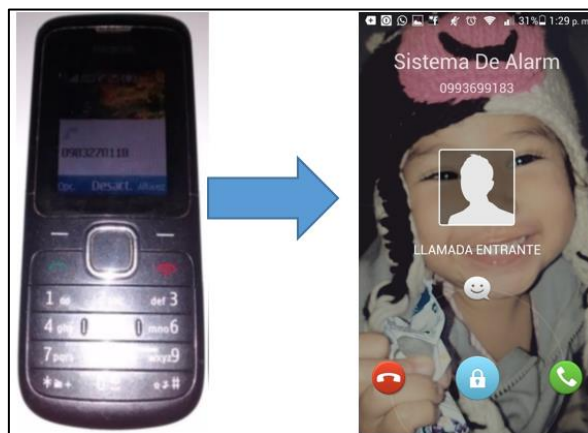
*Fuente: Captura de pantalla.*



**Figura 108. Verificación de envío de mensaje por Telegram.**

*Fuente: Captura de pantalla.*

Cuando se detecta la intrusión el script (`cam1_event.sh`) ejecuta la llamada hacia el gerente, la cual es gestionada por el software Asterisk. Al detectar movimiento dentro de un área de monitoreo, se produce una llamada al gerente en donde podrá responder antes las opciones que se presentan en forma de audio presionando las teclas que indica el IVR del Plan de marcado para reiniciar el sistema o desactivarlo.



**Figura 109. Ejecución de la llamada al gerente.**

*Fuente: Captura de pantalla.*

#### 4.4.3.1 Opciones de la llamada.

- Opción 1/costo

Reinicia el sistema de alarma

Duración aproximada de la llamada 20 segundos costo de llamada 10 centavos

- Opción 2/costo

Detiene el sistema de alarma y activa el sistema de video vigilancia.

Duración de la llamada 30 segundos costo de llamada 15 centavos

- Opción 3/costo

Opción adicional activa de forma inmediata la sirena.

Duración de la llamada 20 segundos costo de llamada 10 centavos

- Opción 4/costo

Opción adicional silencio de forma inmediata la sirena.

Duración de la llamada 20 segundos costo de llamada 10 centavos

#### **4.4.3.2 Recomendación de disponibilidad para la llamada telefónica.**

Para tener siempre disponibilidad de minutos en el chip del Gateway de voz y que la llamada se ejecute siempre que ocurra un evento de detección de movimiento se recomienda contratar un plan de minutos de una operadora local.

Este plan de preferencia se debe asociar a un método de pago automático como una cuenta bancaria o a una tarjeta de crédito o débito, esta recomendación tiene el fin de evitar fallos humanos por falta de pago del plan.

Entre las operadoras locales de servicios de telefonía móvil se encuentran las siguientes:  
CNT, CLARO, MOVISTAR, TUENTI.



CNT Plan voz, precio final: 14,56 dolares.

PLAN VOZ		
Tarifa mensual:	Recibe	Habla a:
Desde	Noches y Fines de semana	\$0,04* a Fijos y Móviles CNT
<b>\$13.00*</b>	<b>SIN LÍMITES</b>	
<small>\$14.56 incluido impuestos</small>		
<small>* No incluye impuestos</small>		
		Desde: <b>\$13.00*</b> <small>\$14.56 incluido impuestos</small>
		Beneficios: Navega bajo demanda a la mejor tarifa del mercado \$0.0214
		<a href="#">Ver más</a>

**Figura 110. Plan CNT.**

*Fuente: <https://www.cnt.gob.ec/movil/tipo/pospago/>*

Movistar plan ilimitado 20 dólares.

¡Me quedé sin saldo!  
Deja esa frase en el pasado, contrata un **Plan Ilimitado desde \$20** y comunícate con todos.

[Lo Quiero](#) [Ver más](#)

Habla sin parar

Olvídate de los límites

**Figura 111. Plan Movistar.**

*Fuente: <https://www.movistar.com.ec/productos-y-servicios/pospago/planes/>*

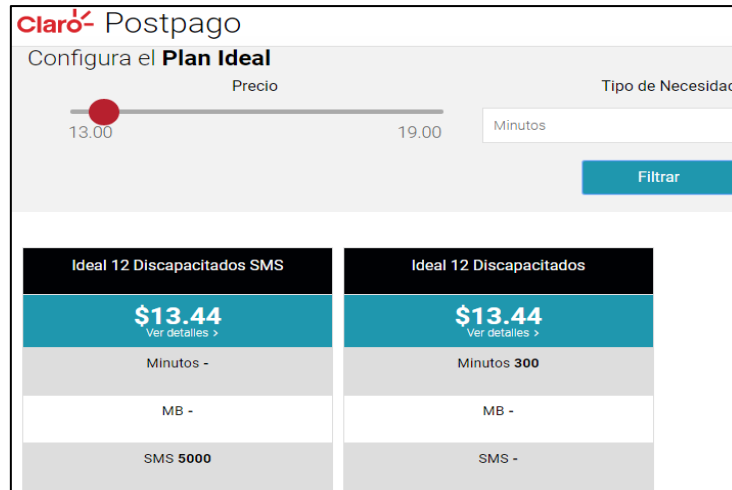
TUENTI Combos pre plan.

¡Todos nuestros combos duran 30 días!

<b>3GB</b> GRATIS 100 MIN VOZDIGITAL \$15	<b>2GB</b> GRATIS 50 MIN VOZDIGITAL \$10	<b>750MB</b> GRATIS 15 MIN VOZDIGITAL \$5
--	---	--

**Figura 112. Plan Tuenti.**  
**Fuente:** <https://www.tuenti.ec/productos/>

CLARO Plan Ideal 12.



**Figura 112. Plan CLARO.**  
**Fuente:** <https://www.claro.com.ec/personas/servicios/servicios-moviles/postpago/planes-y-precios/>

Se recomienda usar el plan de Claro que presenta la opción de solo minutos ideal para el sistema que no requiere de mensajería o datos móviles.

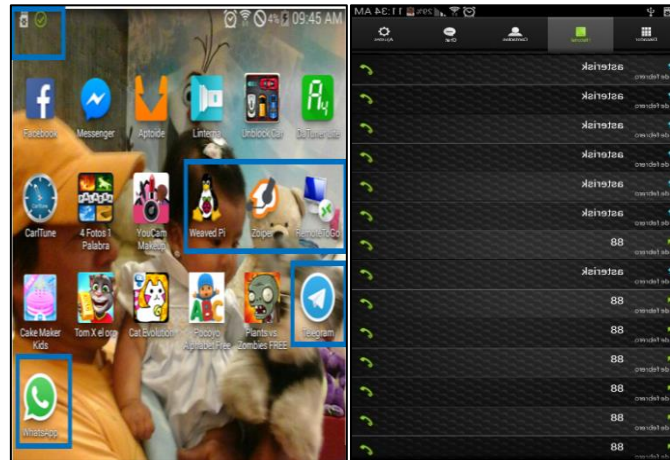
#### 4.5 Método de control local y remoto para el sistema de video vigilancia.

La activación del sistema en modo Alarma y Monitoreo se realiza con un Softphone instalado en el Smartphone del gerente. La activación se realiza digitando el código secreto y llamando a la centralita de voz IP Asterisk que gestionara el control de encendido o apagado del sistema de alarma. El funcionamiento del control requiere de conexión a la red local o conexión a internet.

Se probó la activación del sistema dentro de la red de área local, usando el softphone Zoiper con cuenta SIP instalado en una tableta con sistema operativo Android.

Primero se verificó que el software este en línea con la centralita instalada en el Raspberry Pi se indica con un símbolo de visto en la parte superior, entramos en la aplicación,

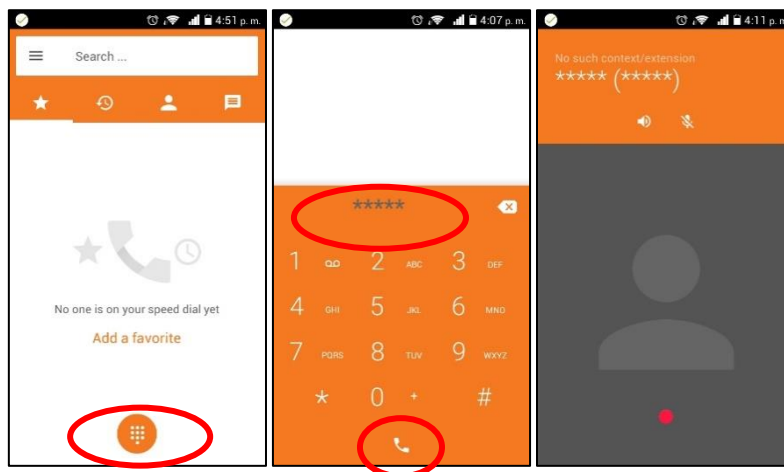
se digita el código de activación y se realiza el marcado la centralita nos responderá con un audio indicando la activación o desactivación del sistema, se puede observar en la figura 113.



**Figura 113. Verificación de control mediante Softphone Zoiper con cuenta SIP.**

*Fuente: Captura de pantalla.*

Se probó la activación del sistema desde internet, usando Zoiper con cuenta IAX instalado en una tableta, se verificó que el software este en línea con la centralita, entramos en la aplicación, se digita el código de activación y se realiza el marcado, responderá con un audio indicando la activación o desactivación del sistema, se puede observar en la figura 114.



**Figura 114. Verificación de control mediante Softphone Zoiper con cuenta IAX.**

*Fuente: Captura de pantalla.*

## CAPÍTULO V

### 5. ANÁLISIS COSTO-BENEFICIO

#### 5.1 Introducción

Es necesario analizar los costos que generará la posible implementación de este diseño en la matriz de la empresa Almacén Color 2000 y los beneficios e impactos que generará este sistema de video vigilancia y alarma. Para evaluar estos parámetros utilizaremos la siguiente formula:

$$\frac{B}{C} = \frac{\sum \text{Beneficios}}{\sum \text{Costos y Gastos}}$$




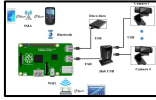
Este análisis permitirá definir el rendimiento en términos de valor por unidad monetaria invertida, el cual generará el proyecto en caso de ser implementado.

#### 5.2 Comparativa de elementos del sistema de video vigilancia.

Se realizó una comparativa para evaluar las características del prototipo del sistema frente a soluciones en el mercado en la siguiente tabla se destaca las características de los sistemas de video vigilancia analógicos más asequibles en el mercado.

Cabe destacar que se considera solo el costo de los equipos y materiales que incluye el kit el cual ofertan las distintas soluciones, no se considera la instalación del sistema en la infraestructura de destino, se analiza las marcas Floureon, Hikvision y Epcom.

Tabla 27. Comparativa sistemas de video vigilancia analógicos vs prototipo del proyecto.

COMPARATIVA SISTEMAS DE VIDEO VIGILANCIA ANALÓGICOS VS PROTOTIPO DEL PROYECTO.				
	Kit Dvr 900tvl CCTV Floureon.	Kit HIKVISION dvr 720p	KIT EPCOM	Prototipo con el Raspberry pi 3 del Proyecto.
<b>Detalle grafico</b>				
<b>Sistema operativo</b>	Propietario	Propietario	Propietario	Linux
<b>Compresión de video.</b>	H 264	H 264	H 264	H 264
<b>Interfaz de entrada de video.</b>	Limitada 8 canales.	Limitada 8 canales.	Limitada 8 canales.	7 puertos USB 2.0 escalable.
<b>Servicio de red</b>	Ethernet conector RJ-45	Ethernet conector RJ-45	Ethernet conector RJ-45	Ethernet RJ-45 y WI-FI
<b>Salida HDMI</b>	Si	Si	Si	Si
<b>Salida de audio</b>	RCA	No	No	RCA – Altavoces
<b>Sistema de acceso remoto.</b>	Si	Si	Si	Si
<b>Modo de grabación</b>	Automático	Automático	Automático	Detección de movimiento.
<b>Reproducción simultanea de video</b>	Si	Si	Si	Si
<b>Reproducción en Smartphone</b>	Soportada	Soportada	Soportada	Soportada
<b>Alimentación</b>	110V~ 60HZ	110V~ 60HZ	110V~ 60HZ	5V DC – 2,5 A
<b>Almacenamiento</b>	Disco no incluido	Disco no incluido	Disco no incluido	Disco de 1 TB incluido
<b>Envío de correo</b>	NO	NO	NO	Si
<b>Envío de mensajes Instantáneos</b>	NO	NO	NO	Si - Telegram.
<b>Sirena de Alarma</b>	NO	NO	NO	Si - Altavoces
<b>Llamada Telefónica</b>	NO	NO	NO	Si
<b>Aplicación de Control remoto por Smartphone.</b>	NO	Si	Si	Si
<b>Costo estimado del equipo en dólares.</b>	380	390	430	306

Fuente: Elaborado por el autor, fuente (HIKVISION, 2018), (EPCOM, 2018), (FLOUREON, 2018).

En la tabla 27 se observa las características de algunos sistemas de video vigilancia, las ventajas del sistema del proyecto resaltan en escalabilidad debido a que la interfaz de entrada de video es a través de puertos USB, la grabación por detección de movimiento, mensajería instantánea a través de Telegram, envío de correo electrónico de la detección de movimiento y la característica principal la alerta de intrusión mediante llamada telefónica.

En la tabla 28 se observa las características de cámaras correspondientes a las marcas de las soluciones anteriores y las características de la cámara web usada en el proyecto.

**Tabla 28. Comparativa cámaras de sistemas de video vigilancia analógicos vs cámaras prototipo del proyecto.**

<b>COMPARATIVA CÁMARAS DE SISTEMAS DE VIDEO VIGILANCIA ANALÓGICOS VS CÁMARAS PROTOTIPO DEL PROYECTO.</b>				
	Cámara Floureon. Domo	Cámara Hikvision. Domo	Cámara Epcom. Domo	Cámara Imexx IME-41674. Web Cámara.
<b>Detalle grafico</b>				
<b>Lente</b>	4mm	3,6mm	2.8mm	3,0 mm
<b>Resolución</b>	720 P	720 P	720 P	720 P
<b>Aplicación</b>	Interior	Interior	Interior	Interior
<b>Tipo de sensor</b>	CMOS 1/4"	CMOS 1/3"	CMOS 1/3"	CMOS 1/4"
<b>Alimentación</b>	12V DC	12 V DC±10%	12 V DC±10%	USB 5V
<b>Angulo de visión</b>	75° (3.6 mm)	75° (3.6 mm)	75° (2.8 mm)	75° (3.0 mm)
<b>Costo</b>	25	30	30	14

Fuente: Elaborado por el autor, fuente (HIKVISION, 2018), (EPCOM, 2018), (FLOUREON, 2018).

### 5.3 Determinación de los gastos a invertir

Los gastos en este Proyecto están determinados por la adquisición del equipamiento, los dispositivos de captura de video, el cableado y demás materiales necesarios para la implementación del sistema de video vigilancia IP y alarma basada en movimiento.

Tabla 29. Análisis del costo.

Descripción	Cantidad	Costo unitario	Costo total
<b>Kit Raspberry Pi 3</b>	1	70,00	70,00
<b>Hub USB 2.0 de 7 puertos con alimentación propia.</b>	1	20,00	20,00
<b>Cámara web para PC</b>	4	14,00	56,00
<b>Extensión de Cable USB 2.0 Activo 15m</b>	2	25,00	50,00
<b>Disco Duro Extraíble 1Tb</b>	1	70,00	70,00
<b>Teléfono celular con Bluetooth (Gateway)</b>	1	40,00	40,00
<b>Costo de la instalación</b>	1	200,00	200,00
<b>Total</b>			506,00

Fuente: Elaborado por el autor.

## 5.4 Determinación de los beneficios

Para determinar los beneficios del proyecto se hace un análisis, enfocado a los aspectos que protegerá este sistema en forma de valores monetarios, indicando los como antecedentes las pérdidas por robos de productos, pérdida de materiales de bodega, entre otros aspectos.

Se debe indicar que este sistema es una alternativa frente a los sistemas de video vigilancia convencionales, enfocado hacia aplicaciones basadas en software libre. Se definirá en una tabla los valores de beneficio.

### 5.4.1 Cálculo de beneficios.

Mediante una reunión con la gerencia en donde se determina que las pérdidas ocasionadas por sustracción de productos y pérdidas de materiales en el año de 2016 suman un estimado de 1000 dólares, en las cuales no se tuvo un respaldo para generar la debida acción legal.

Con el fin de optimizar las labores de los empleados de la empresa y evitar los tiempos de ocio, se realiza el monitoreo a través de las cámaras en tiempo real de las actividades realizadas por los trabajadores en la empresa, datos de la gerencia indican que al menos 10 minutos (0.17h) al día cada trabajador toma un receso sin consentimiento de la gerencia. Se

toma esta relación de tiempo enfocándola al valor que percibe el trabajador y multiplicado por las 0.17 h (10min) que el trabajador no labora y se obtiene el beneficio por día sobre una jornada de 8 horas laborables normales.

**Tabla 30. Análisis de beneficios.**

<b>Descripción personal operativo</b>	<b>Remuneración</b>	<b>Valor/hora</b>	<b>Beneficio</b>
<b>Encargado de bodega</b>	450	2,82	0,49
<b>Atención al cliente 1</b>	430	2,69	0,46
<b>Atención al cliente 2</b>	400	2,50	0,43
<b>Técnico de colorimetría 1</b>	650	4,06	0,69
<b>Técnico de colorimetría 2</b>	600	3,75	0,64
<b>Total, al día</b>			2,71
<b>Total, a la semana</b>			13,55
<b>Total, al mes</b>			54,20
<b>Total, al año</b>			650,40
<b>Perdida por robo de productos</b>			1000,00
<b>Beneficio total</b>			1650,40
<b>Beneficio general mensual</b>			137,53

Fuente: Elaborado por el autor.

Al finalizar el análisis de los costos y beneficios que generará la implementación de este sistema de video vigilancia y alarma basa en la detección de movimiento, se aplica la fórmula para la determinación del beneficio sobre el costo de la implementación, para lo cual se utilizará los siguientes parámetros de evaluación:

- 1.- Si B/C es mayor que 1 se acepta el proyecto
- 2.- Si B/C es igual que 1 el proyecto es indiferente
- 3.- Si B/C es menor que 1 se rechaza el proyecto

Remplazando los valores en la formula tendremos:

$$\frac{B}{C} = \frac{\sum \text{Beneficios}}{\sum \text{Costos y Gastos}}$$



$$\frac{B}{C} = \frac{1650,40}{506,00}$$

$$\frac{B}{C} = 3.26$$

Esta relación indica que por cada dólar invertido en el proyecto, se devuelve 2,26 dólares como rentabilidad del proyecto.

## 5.5 Periodo de recuperación

El periodo de recuperación de la inversión que se requiere para la implementación del proyecto. Se basa en los beneficios que cubre en cada periodo de vida útil, en la tabla 31 se muestra el cálculo:

**Tabla 31. Periodo de recuperación del proyecto.**

<b>Mes</b>	<b>Beneficios Mensuales</b>	<b>Costo total</b>
<b>0</b>		-506,00
<b>1</b>	137,53	137,53
<b>2</b>	137,53	275,06
<b>3</b>	137,53	412,59
<b>4</b>	137,53	550,12
<b>Periodo de recuperación</b>		3 meses 21 días

Fuente: Elaborado por el autor.

Para determinar el tiempo exacto de recuperación se realizó el siguiente cálculo:

$$\sum \text{de 3 meses} \rightarrow \$ 412,59$$

$$PR = 3 \text{ meses} + \frac{\text{Inversión} - \sum \text{de 3 meses}}{\text{Beneficio general mensual}}$$

$$PR = 3 \text{ meses} + \left( \frac{506,00 - 412,59}{137,53} \right)$$

$$PR = 3 \text{ meses} + \left(\frac{93,41}{137,53}\right)$$

$$PR = 3 \text{ meses} + 0,68 \text{ de mes}$$

$$PR = 3 \text{ meses} + (0,68 \text{ de mes} \times 30 \text{ días})$$

$$PR = 3 \text{ meses} + 21 \text{ días}$$

Con los cálculos anteriores podemos determinar que el periodo de recuperación del Proyecto será de 3 meses con 21 días.

## **5.6 Beneficiarios del proyecto**

Se clasifico en beneficiarios directos e indirectos los cuales usan el sistema de video vigilancia y alarma en donde se benefician de sus aplicaciones y características.

### **5.6.1 Beneficiarios directos.**

Dentro de los beneficiarios directos se encuentran los funcionarios que desempeñan sus labores en la matriz de la empresa Almacén Color 2000 que suman un numero de 7 los cuales están distribuidos entre personal operativo y administrativo de la empresa.

### **5.6.2 Beneficiarios indirectos.**

Los beneficiarios indirectos son todas las personas que usan los servicios que presta esta empresa, clientes, proveedores y distribuidores que acuden a esta empresa en busca de sus servicios y productos y que serán beneficiados dentro del concepto de seguridad por video vigilancia para salvaguardar la integridad del cliente.

## 5.7 Impacto del proyecto

Este análisis permite determinar factores y aspectos que generara este proyecto en ámbitos sociales, económico, institucional y educativo.

### 5.7.1 Impacto económico.

**Tabla 32. Indicadores de evaluación económica.**

<b>Indicador</b>	<b>Impacto positivo</b>	<b>Impacto negativo</b>
<b>1 Protección de robo de productos.</b>	X	
<b>2 mejoramiento de producción</b>	X	
<b>3 Protección hacia clientes</b>	X	
<b>Impacto final</b>		Positivo

Fuente: Elaborado por el autor.

El impacto económico se ve reflejado en el mejoramiento de la producción y la prevención de robo de productos y materiales, así también como la protección de la integridad de la empresa frente a los clientes.

### 5.7.2 Impacto social.

**Tabla 33. Indicadores de evaluación en impacto social.**

<b>Indicador</b>	<b>Impacto positivo</b>	<b>Impacto negativo</b>
<b>1 Protección de integridad de empleados</b>	X	
<b>2 Protección de integridad de clientes</b>	X	
<b>3 Imagen hacia la ciudad</b>	X	
<b>Impacto final</b>		Positivo

Fuente: Elaborado por el autor.

Describe el grado de involucramiento con la sociedad al implementarse este proyecto, brindando servicios de calidad y seguridad para el cliente y el trabajador de la empresa, creando una imagen de empresa de calidad ante la sociedad.

### 5.7.3 Impacto institucional.

Tabla 34. Indicadores de evaluación institucional.

<b>Indicador</b>	<b>Impacto positivo</b>	<b>Impacto negativo</b>
<b>1 Modelo de monitoreo</b>	X	
<b>2 Modelo de seguridad</b>	X	
<b>3 Manejo de recursos</b>	X	
<b>Impacto final</b>		Positivo

Fuente: Elaborado por el autor.

Mantiene un orden mediante la monitorización en la ejecución de tareas programa, actividades realizándose y cumplimiento de las metas. El modelo de seguridad previene la sustracción y daño de los bienes materiales.

### 5.7.4 Impacto educativo.

Tabla 35. Indicadores de evaluación de impacto educativo.

<b>Indicador</b>	<b>Impacto positivo</b>	<b>Impacto negativo</b>
<b>1 Aporte de experiencias</b>	X	
<b>2 Mejoramiento de conocimientos</b>	X	
<b>3 Fuente de consultas</b>	X	
<b>Impacto final</b>		Positivo

Fuente: Elaborado por el autor.

La elaboración de este trabajo servirá de base para la ejecución de proyectos similares, su documentación servirá de fuente de consulta para el aprendizaje de nuevos conocimientos y técnicas de diseño de sistemas alternativos de video vigilancia y alarma basa en la detección de movimiento.

## CAPÍTULO VI

### 6. CONCLUSIONES Y RECOMENDACIONES

En este último capítulo se presentan las conclusiones y recomendaciones de todos los puntos relevantes o de interés obtenidos en el desarrollo de este trabajo de grado.

#### 6.1 Conclusiones

- ✚ La elaboración de este diseño enfocado a la matriz de empresa Almacén Color 2000 permite solventar problemas de seguridad y el mejoramiento de productividad del personal operativo por medio de monitoreo del sistema de video vigilancia.
- ✚ Los componentes para el sistema de video vigilancia y alarma no son heterogéneos, esto indica que el sistema puede funcionar tanto con cámaras web, cámaras IP o con la interacción mixta, puede soportar toda clase de marcas de equipos sin problemas, siempre y cuando se compruebe su compatibilidad con el Raspberry Pi 3.
- ✚ El computador de placa reducida Raspberry Pi 3 demuestra ser un equipo fiable y robusto del cual se aprovecharon sus características y funcionalidades como si se tratase de un computador convencional, en donde se desarrolló en funcionamiento completo de este sistema, cabe destacar que puede soportar mejoras al sistema de video vigilancia y alarma sin que esto afecte su funcionalidad.

- ✚ El modulo para la conexión con el Gateway de voz hacia la red de telefonía móvil (teléfono celular con Bluetooth), cumple su función a cabalidad, alertando por medio de una llamada al gerente de la empresa y presentado las opciones para el evento.
  
- ✚ La integración de alertas por medio de aplicaciones como WhatsApp y Telegram hace de este sistema una herramienta funcional mejorando la forma de control y notificación sobre un evento utilizando redes sociales de uso cotidiano.
  
- ✚ El diseño de este proyecto es una solución alternativa de video vigilancia y alarma personalizada, para el funcionamiento en la matriz de la empresa Almacén Color 2000, está desarrollada para competir frente a sistemas de video vigilancia propietarios ofertados en el mercado.
  
- ✚ Mediante el desarrollo de un análisis costos sobre beneficios se concluye que la posible implementación de este sistema mejora la productividad y crea un ambiente de seguridad y confort tanto para el personal operativo, personal administrativo y clientes de la empresa.
  
- ✚ Existe una gran variedad de sistemas de video vigilancia que incorporan características algunas características como las presentadas en este trabajo de grado, sin embargo presentan un costo elevado por ser sistemas propietarios y no incorporan todas las funcionalidades que este proyecto oferta.

## 6.2 Recomendaciones

- ✚ Para proteger el equipo de acciones vandálicas, acceso no autorizado y daños por efectos de la intemperie, se sugiere la ubicación del equipo en un lugar seguro dentro de un rack pequeño para equipos de comunicaciones.
- ✚ Si la implementación y configuración del sistema se lleva a cabo por una persona diferente al autor es recomendable, leer cuidadosamente la sección de configuración del software Motion para la gestión de cámaras en el capítulo 3.
- ✚ Es recomendable usar un cargador con las especificaciones que sugiere el fabricante del computador de placa reducida Raspberry Pi 3, en donde indica que debe ser de una salida de 5v a 2.5 A.
- ✚ Para agregar al sistema más cámaras web se debe hacer lo por medio de un hub USB con alimentación propia se sugiere esto por la capacidad de 4 puertos USB que tiene la placa del Raspberry Pi 3 y debido al consumo de energía de las cámaras web.
- ✚ Si se desea agregar más cámaras al sistema se sugiere seguir la guía para la adición de equipos y basarse en los apartados cámara web o cámara IP.
- ✚ Si el aumento de cámaras IP para el sistema es considerablemente alto se sugiere realizar una evaluación del consumo de ancho de banda, para evitar problemas de acceso a las aplicaciones de monitoreo. Si el resultado arroja una deficiencia en el ancho de banda es recomendable aumentarlo.

- ✚ Es recomendable seguir la guía para el correcto mantenimiento del sistema de video vigilancia y alarma basada en detección de movimiento, el cual se sugiere realizarlo cada mes.



## Bibliografía

Alam, M. (2018). *shinobi*. Obtenido de CCTV software de código abierto escrito en Node.JS:

<https://moeiscool.github.io/Shinobi/>

Alpine, L. (2018). *Alpine*. Obtenido de Alpine: <https://alpinelinux.org/>

ANKER. (2017). Obtenido de HUB USB 7 PUERTOS:

<https://www.anker.com/products/variant/7-Port-USB-3.0-Hub--/A7505112>

Archlinux. (2017). *Archlinux Arm*. Obtenido de <https://archlinuxarm.org/>

Barbieri, S. (2012). *Ethernet / IEEE 802.3*. Buenos Aires - Argentina: Universidad Nacional

de Centro de la Provincia de Buenos Aires. Obtenido de

<http://www.exa.unicen.edu.ar/catedras/comdat1/material/Ethernet2010.pdf>

Betancourt, E. G. (2013). *Sistema de videovigilancia remota de bajo costo con*

*microcomputadora y celdas solares*. Costa Rica: Universidad de Costa Rica.

Bicom. (2018). *Bicom systems*. Obtenido de PBXware:

<https://www.bicomsystems.com/products/pbxware>

CubieBoard. (2016). *CubieBoard*. Obtenido de CubieBoard: <http://cubieboard.org/model/>

Dave. (2018). *Motion*. Obtenido de Motion: [https://motion-](https://motion-project.github.io/motion_guide.html)

[project.github.io/motion\\_guide.html](https://motion-project.github.io/motion_guide.html)

Digium. (2018). *Asterisk*. Obtenido de AsteriskNOW:

<http://www.asterisk.org/downloads/asterisknow>

Edwards, R. (12 de Julio de 2012). *Historia de las redes Ethernet*. Obtenido de DefinicionyCableadoII:

<https://definicionycableado.wikispaces.com/file/detail/Historia%20de%20las%20redes%20Ethernet.pdf>

Elastix. (2018). *Elastix*. Obtenido de Elastix: <https://www.elastix.org/>

EPCOM. (2018). *EPCOM*. Obtenido de <https://epcom.net/product/LE7-TURBO-WP-EPCOM-82101.html>

Felenasoft. (2018). *Vigilancia*. Obtenido de Xeoma: <http://felenasoft.com/xeoma/en/features/>

Fernández, J. R. (2013). *Circuito cerrado de televisión y seguridad electrónica*. Madrid: Paraninfo.

FLOUREON. (2018). *FLOUREN*. Obtenido de [http://www.floureon.com/product-g\\_285.html](http://www.floureon.com/product-g_285.html)

Fonality. (2018). *Fonality*. Obtenido de Trixbox Business Phone Solutions is now Fonality: <http://www.fonality.com/trixbox>

Gacitúa, M. S. (2007). *Plan comercial para la introducción de un nuevo servicio de vigilancia de la empresa prosegur*. Concepción-Chile: Universidad La Concepción.

Ganchala, M. A. (2011). *Optimización del sistema de CCTV del edificio comercial de la empresa pública metropolitana de agua potable y saneamiento*. Sangolquí: Escuela Politécnica del Ejército.

García, D. M. (2016). *Sistema de navegación para robots móviles basado en un ordenador de placa simple*. Valencia: Universidad Politecnica de Valencia.

Hardkernel. (2013). *ODRID*. Obtenido de Odroid: <http://www.hardkernel.com/>

HIKVISION. (2018). *HIKVISION*. Obtenido de <http://www.hikvision.com>

Imexx. (2017). *PREMIUM 5MP WEBCAM*. Obtenido de <http://www.imexx.com/IME-41674>

Intel. (2017). *Especificaciones del producto*. Obtenido de <https://ark.intel.com/#@BoardsAndKits>

Jaguarboard, E. (2015). *Jaguarboard*. Obtenido de <http://www.jaguarboard.org/>

Junghanss, R. (2012). *Circuito Cerrado de Televisión*. Buenos Aires: .data tecnica.

LinkSprite. (2016). *LinkSprite pcDuino*. Obtenido de <http://www.linksprite.com/linksprite-pcduino/>

Logitech. (2017). *Catalogo*. Obtenido de <https://www.logitech.com/es-mx/product/hd-pro-webcam-c920#specification-tabular>

Martinez, R. (2014). *El rincón de Linux*. Obtenido de [Distribuciones de Linux: http://www.linux-es.org/distribuciones](http://www.linux-es.org/distribuciones)

Mata, F. J. (2011). *Videovigilancia: CCTV usando vídeos IP*. Madrid: Vértice.

Mercadolibre. (2017). *Mercado Libre*. Obtenido de [https://articulo.mercadolibre.com.ec/MEC-413400821-mini-hub-de-7-puertos-usb-20-con-fuente-de-poder-\\_JM](https://articulo.mercadolibre.com.ec/MEC-413400821-mini-hub-de-7-puertos-usb-20-con-fuente-de-poder-_JM)

Mesias, B. (2011). *Sistema de vigilancia en tiempo real mediante camaras IP*. Ambato: Universidad Tecnica de Ambato.

Olguín, E., & J. G. (2010). *WCDMA*. Chile: Universidad Técnica Federico Santa María.

Ortiz, F., F. C., J. P., P. G., & L. C. (2012). *Práctica de Redes*. San Vicente (Alicante): Editorial Club Universitario.

Ovtoaster. (18 de Febrero de 2014). *Ovtoaster*. Obtenido de Introducción a los scripts en Linux: <http://ovtoaster.com/introduccion-los-scripts-en-linux/>

Pimentel, G. (2018). *Gustavo Pimentel's GNU/Linux Blog*. Obtenido de [Version Final] DigAnTel 3: <http://gustavo.pimentel.eu/2010/05/version-finaldigantel-3/#more-1162>

PINCOMPUTERS. (2017). *PINCOMPUTERS*. Obtenido de <http://pinsoft.ec/cod-028-web-cam-minton-mwc-7105-1mp-usb-2-0/p-4625.html>

Raspberry, F. (2017). *Raspberry Pi - Teach, Learn and Make with Raspberry Pi*. Obtenido de Raspberry Pi: <https://www.raspberrypi.org>

Rodriguez, J. (28 de Septiembre de 2008). *Metodología de desarrollo de software. El Modelo en V o de Cuatro Niveles*. Obtenido de <http://www.iiia.csic.es/udt/es/blog/jrodriguez/2008/metodologia-desarrollo-sotware-modelo-en-v-o-cuatro-niveles>

Rohde & Schwarz. (2016). *Tecnología Bluetooth*. Obtenido de [https://www.rohde-schwarz.com/es/tecnologias/conectividad-inalambrica/bluetooth/tecnologia-bluetooth/tecnologia-bluetooth\\_55694.html](https://www.rohde-schwarz.com/es/tecnologias/conectividad-inalambrica/bluetooth/tecnologia-bluetooth/tecnologia-bluetooth_55694.html)

Stallman, R. M. (2004). *Software libre para una sociedad libre*. Madrid: Traficantes de Sueños.

Techies, 3. P. (2016). *3rd Planet Techies*. Obtenido de Diferencia entre GPRS, EDGE, 3G, HSPA, HSPA + y LTE 4G: <http://www.3ptechies.com/differences-between-gprs-edge-3g-hsdpa-hspa4g-lte.html>

Technologies, S. (2018). *FreePBX*. Obtenido de FreePBX: <https://www.freepbx.org/>

TP-LINK. (2017). *Accesorios electronicos*. Obtenido de [http://www.tp-link.es/products/details/cat-5688\\_UH700.html#specifications](http://www.tp-link.es/products/details/cat-5688_UH700.html#specifications)

Ubuntu. (2017). *Ubuntu MATE para Raspberry Pi 2 y Raspberry Pi 3*. Obtenido de <https://ubuntu-mate.org/raspberry-pi/>

Valdéz, J. L. (s.f.). *Enciclopedia Virtual*. Obtenido de <http://www.eumed.net/tesis-doctorales/2014/jlcv/software.htm>

Vargas, G. A. (2015). Análisis, diseño e implementación de una aplicación móvil para el monitoreo en tiempo real de CCTV para dispositivos android, haciendo uso de la red celular. Guayaquil.

Xunlong, S. (2016). *Orange Pi*. Obtenido de Orange Pi: <http://www.orangepi.org>

ZoneMinder. (2018). *ZoneMinder*. Obtenido de ZoneMinder: <https://zoneminder.com/features/>

## Anexos

### ANEXO 1.- Formulario de entrevista realizada a la Gerente Ing. Alicia Ramos

<b>Formulario de Entrevista</b>	
<p>Información general</p> <p><b>Entrevistador:</b> Cristian Canacuan                      <b>Cargo:</b> Estudiante-CIERCOM</p> <p><b>Entrevistado:</b> Ing. Alicia Ramos                      <b>Cargo:</b> Gerente Almacén Color 2000</p>	
<p>Cuestionario</p> <ol style="list-style-type: none"> <li>1. ¿Cuál es la razón por la cual se desea realizar la instalación de un sistema de videovigilancia?</li> <li>2. ¿Cuál es la debilidad en la empresa que desea cubrir con un sistema de videovigilancia?</li> <li>3. ¿Cuáles son los aspectos que se pretende mejorar con un sistema de videovigilancia?</li> <li>4. ¿El sistema que se desea es para dar seguridad exterior o controlar más de cerca a los empleados?</li> <li>5. ¿Qué áreas en específico desea cubrir con el sistema de videovigilancia?</li> <li>6. ¿Se quiere enfocar algo específico por ejemplo placas de los vehículos, rostros, dinero en las cajas registradoras?</li> <li>7. ¿Cómo desea obtener la visualización de las cámaras?</li> <li>8. ¿Cómo se desea recibir las alertas del sistema frente a un evento de intrusión?</li> </ol>	
<p>Firmas de Responsabilidad</p>   <div style="display: flex; justify-content: space-around; align-items: flex-end;"> <div style="text-align: center;"> <hr style="width: 200px; margin: 0 auto;"/> <p>Cristian Canacuan Entrevistador</p> </div> <div style="text-align: center;"> <hr style="width: 200px; margin: 0 auto;"/> <p>Ing. Alicia Ramos Entrevistado</p> </div> </div>	

## ANEXO 2.- GUÍA DE USO PARA EL SISTEMA

- 1.- Como activar y desactivar el sistema de alarma.
- 2.- Como Monitorear las cámaras.
- 3.- Como manejar las alertas del sistema

### 1.- COMO ACTIVAR Y DESACTIVAR EL SISTEMA DE ALARMA.

🚦 Activación o desactivación del sistema con Softphone (**Zoiper-Localmente**)

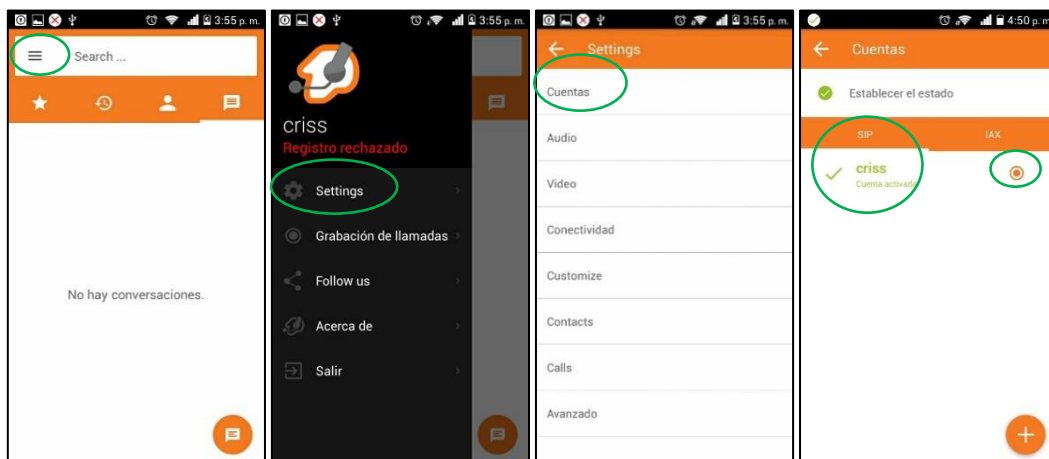
Paso 1.- Conectar el Smartphone a la red inalámbrica de la empresa.



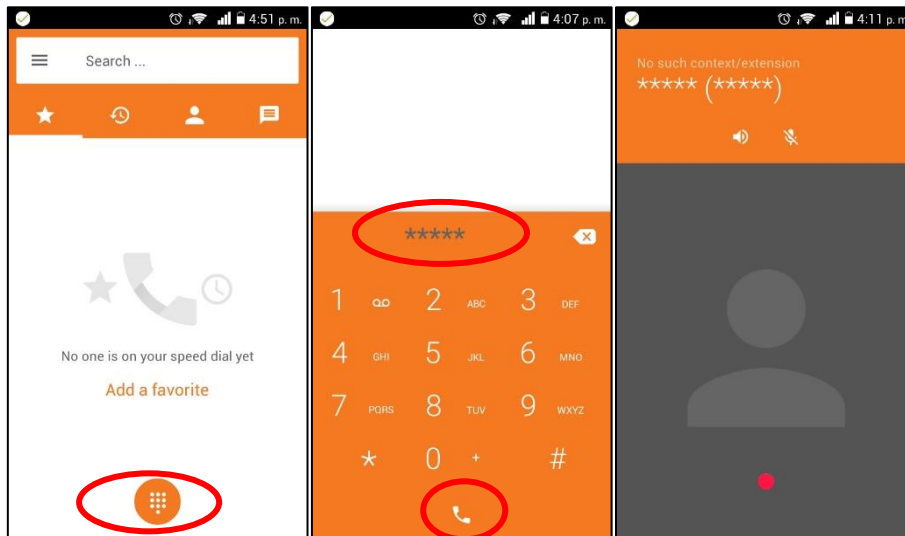
Paso 2.- Acceder a la aplicación Zoiper.



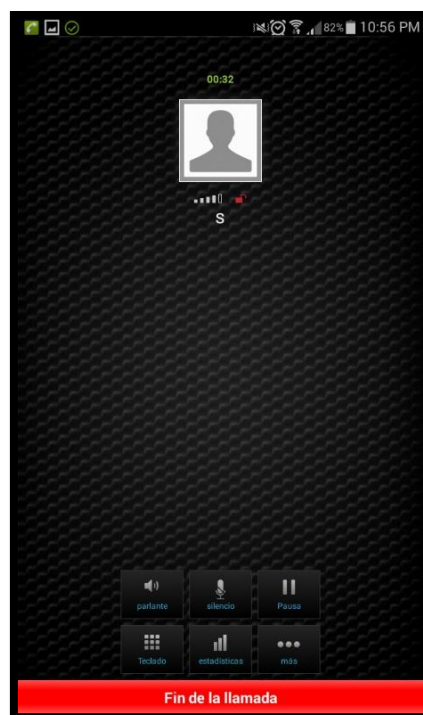
Paso 3.- Verificar que la aplicación este operativo y la cuenta SIP este seleccionada.



Paso 4.- Regresar a la pantalla de marcado y digitar la clave de activación o desactivación.



Paso 5.- Pulse el botón de llamada.



Nota: El sistema confirmará la activación o desactivación con un audio indicando el estado actual del sistema.



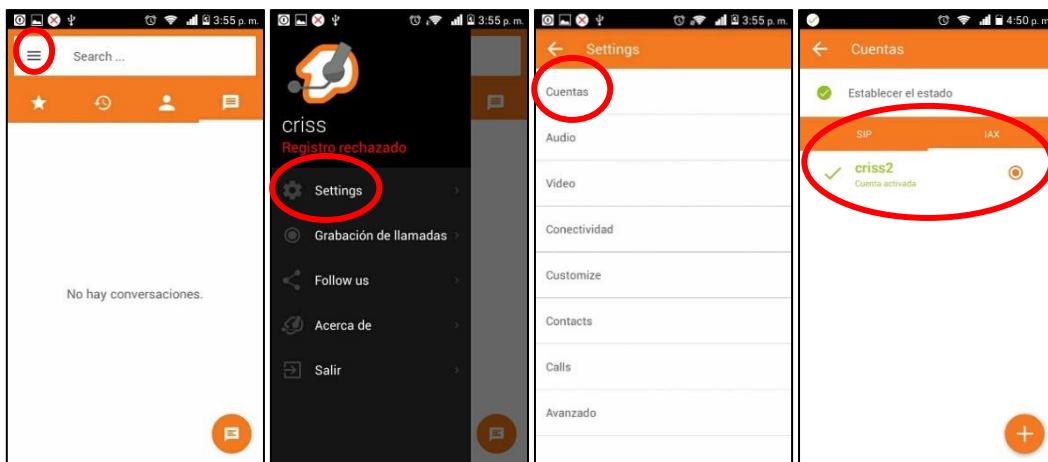
## Activación o desactivación del sistema con Softphone (**Zoiper-Remotamente**)

Paso 1.- Conectar el móvil a Internet (WiFi o Datos Móviles).

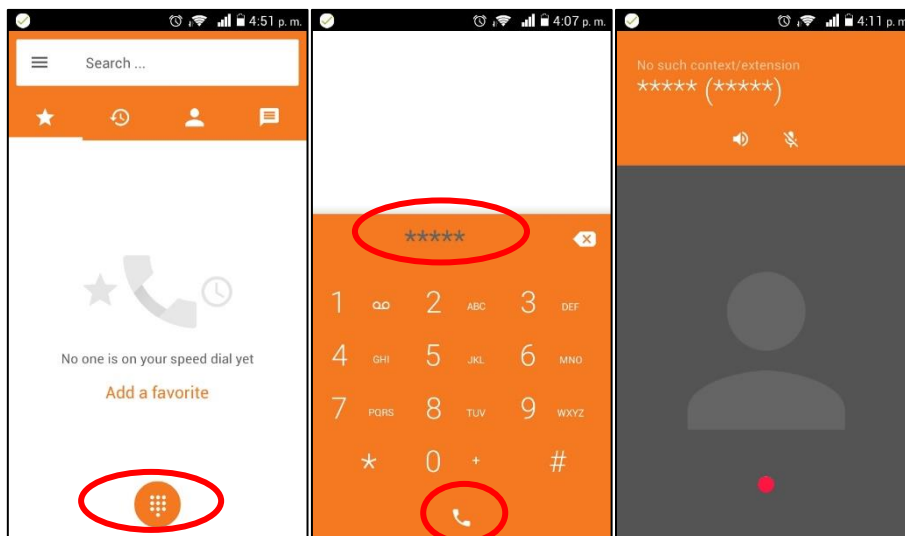


Paso 2.- Ingresar a Zoiper.

Paso 3.- Verificar que la aplicación este operativo y la cuenta IAX este seleccionada.



Paso 4.- Regresar a la pantalla de marcado y digitar la clave de activación o desactivación.



Nota: El sistema confirmará la activación o desactivación con un audio indicando el estado actual del sistema.

## 2.- COMO MONITOREAR LAS CÁMARAS.

🔗 Acceso a la visualización de cámaras desde la red local de la empresa.

1.- Selecciones un dispositivo conectado a la red de empresa (PC-Smartphone).

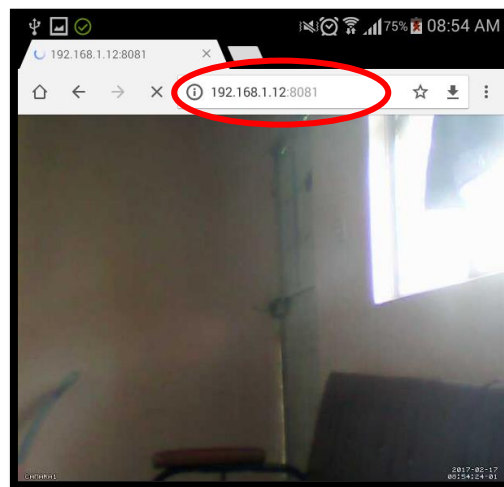
2.- Ingrese a un navegador web y digite lo siguiente: 192.168.1.12:9000.



🔗 Acceso a la visualización por cámara desde la red local de la empresa.

1.- Selecciones un dispositivo conectado a la red de empresa (PC-Smartphone)

2.- Ingrese a un navegador web y digite lo siguiente: 192.168.1.12:808X.



Nota: La X representa la cámara de 1 a 5. Ej. Cámara 1: 192.168.1.12:8081

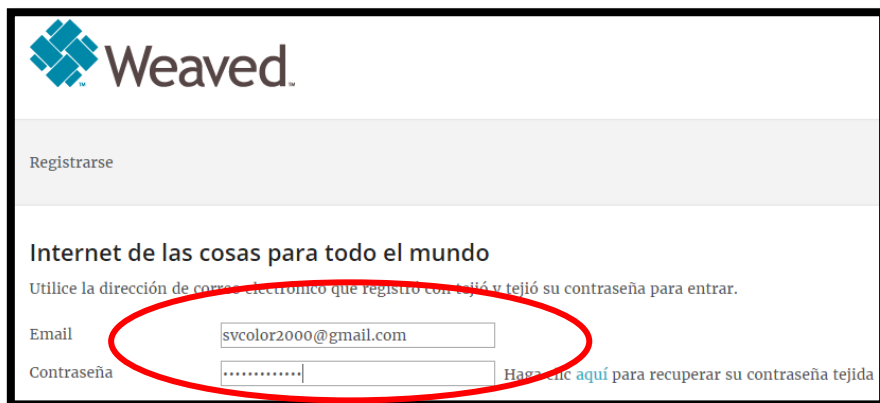
 Acceso a la visualización por cámara desde Internet.

1.- Seleccione un dispositivo conectado a Internet. (PC-Smartphone-Tableta)

2.- Desde la PC ingrese a un navegador web y digite lo siguiente:

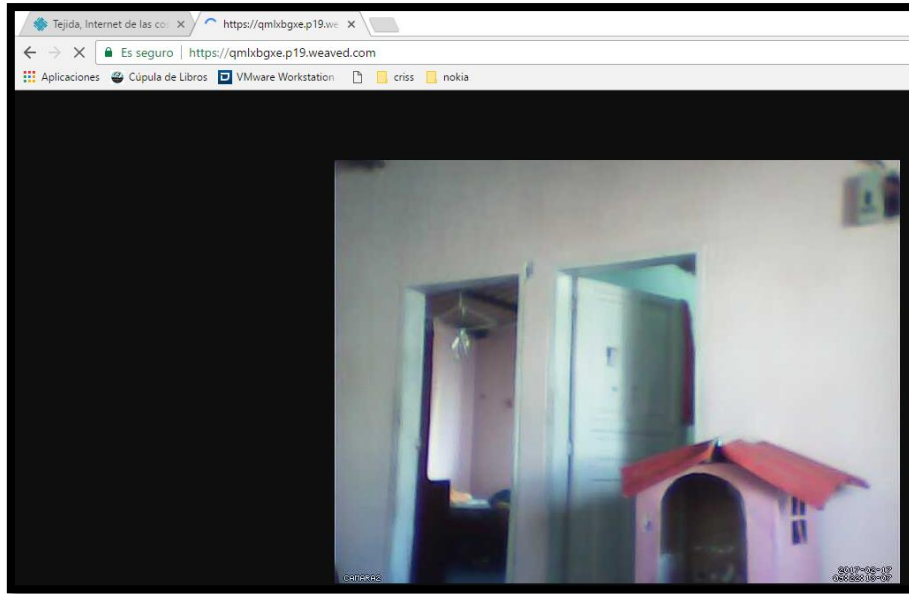
<https://developer.weaved.com/portal/login.php> .

3.- Ingrese el usuario y contraseña para entrar a la aplicación.

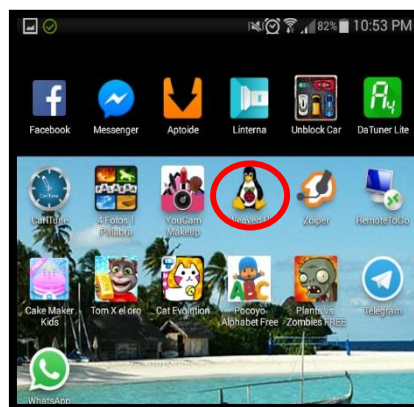


4.- Seleccione la cámara que desea visualizar.

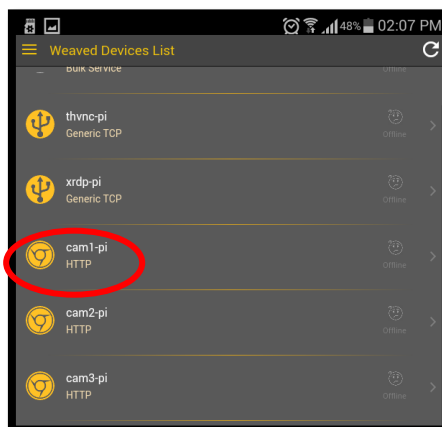
Nombre	Tipo	Estado	
cam1-pi	HTTP	en línea	Compartir   ajustes
CAM2-pi	HTTP	en línea	Compartir   ajustes
cam3-pi	HTTP	en línea	Compartir   ajustes
cam4-pi	HTTP	en línea	Compartir   ajustes
scweb-pi	HTTP	en línea	Compartir   ajustes
thvnc-pi	TCP genérico	en línea	Compartir   ajustes
VNC-pi	VNC	en línea	Compartir   ajustes
webcontrolsc-pi	HTTP	en línea	Compartir   ajustes
xrdp-pi	TCP genérico	en línea	Compartir   ajustes



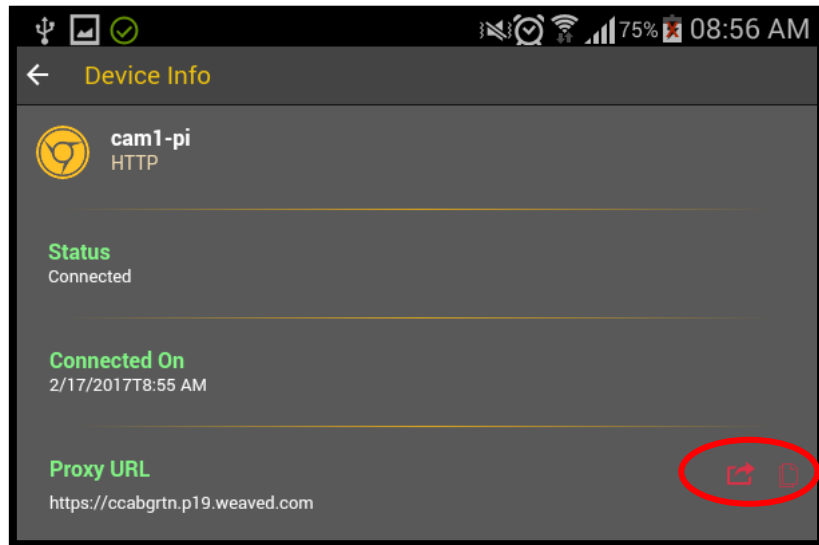
6.- Desde un Smartphone: Ingresa a la aplicación Weaved pi.



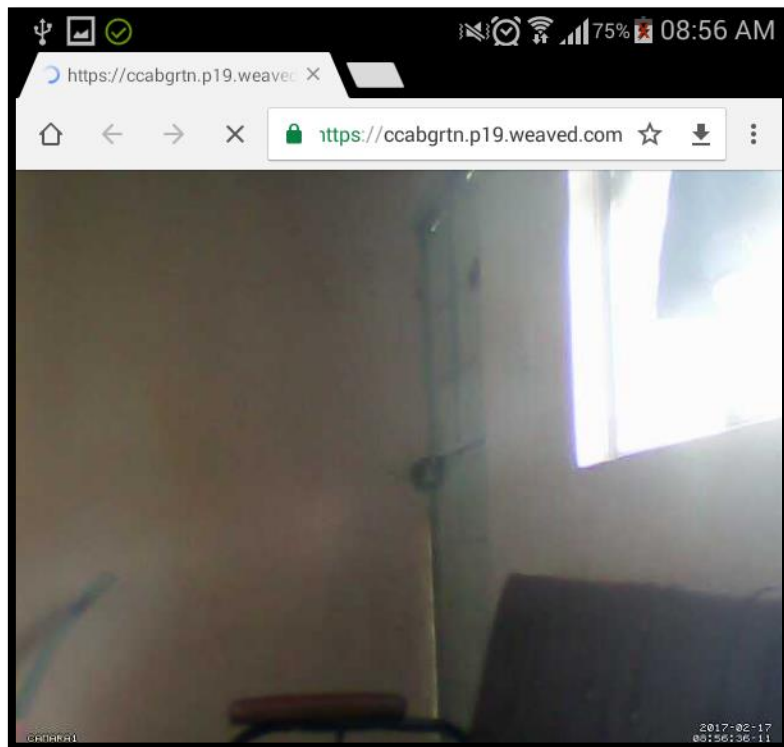
7.- Seleccione la cámara que desea visualizar.



8.- Espere que se genere el link y pulse en el icono de conexión.



9.- Automáticamente se abre en un navegador web la visualización.



### 3.- COMO MANEJAR LAS ALERTAS DEL SISTEMA.

🚦 Aviso de intrusión por alerta de llamada telefónica al móvil.

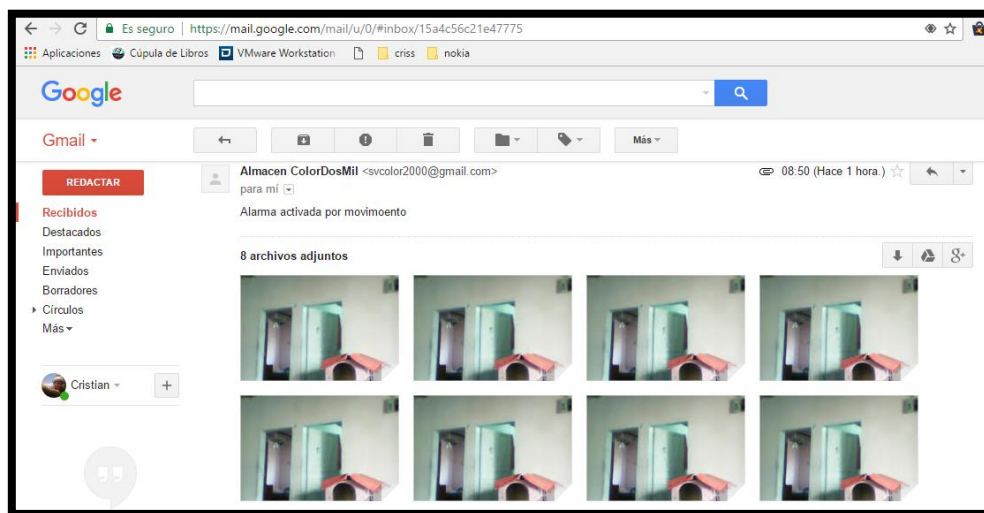
Opción 1.- Digite 1 para reiniciar el sistema.

Opción 2.- Digite 2 para desactivar el sistema.

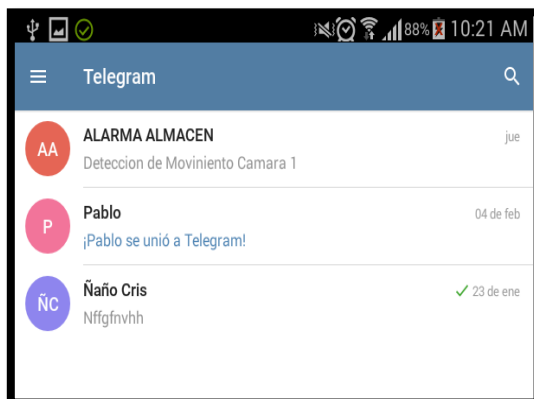
Opción 3.- Digite 3 para reactivar sirena.

Opción 4.- Digite 4 para silenciar la sirena.

🚦 Aviso de intrusión por alerta de correo electrónico.



🚦 Aviso de intrusión por alerta de mensaje en Telegram.



## **ANEXO 3.- GUÍA DE MANTENIMIENTO PARA EL SISTEMA**

- 1.- Como cuidar su equipo.
- 2.- Administración de archivos grabados.

### **1.- CÓMO CUIDAR DE SU EQUIPO**

#### **MONITOR**

Mantener la pantalla del monitor limpia pasándole un paño para evitar que el polvo cause sobrecalentamientos o dificulte la visualización del video transmitido por las cámaras.

#### **CÁMARAS**

Quitar el polvo y la suciedad que se acumule en el lente de la cámara y del cristal, esto afecta la capacidad de la visión. Se debe tener cuidado al limpiar para no desenfocar la cámara del área a monitorear. Use un paño de microfibras para limpiar regularmente las cámaras o cuando el vídeo transmitido se vea nublado o poco claro.

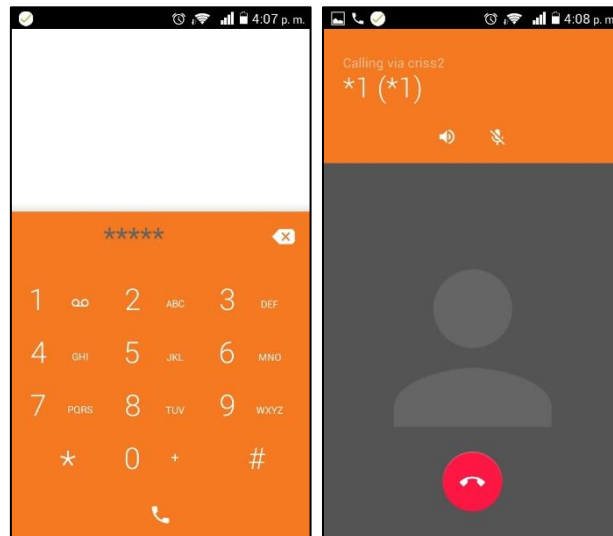
#### **EQUIPOS**

Ubicar el computador de placa reducida, el HUB USB, teléfono móvil y disco de almacenamiento en un rack, revisar periódicamente la presencia de polvo o humedad, revisar también las conexiones para evitar fallos en el sistema.

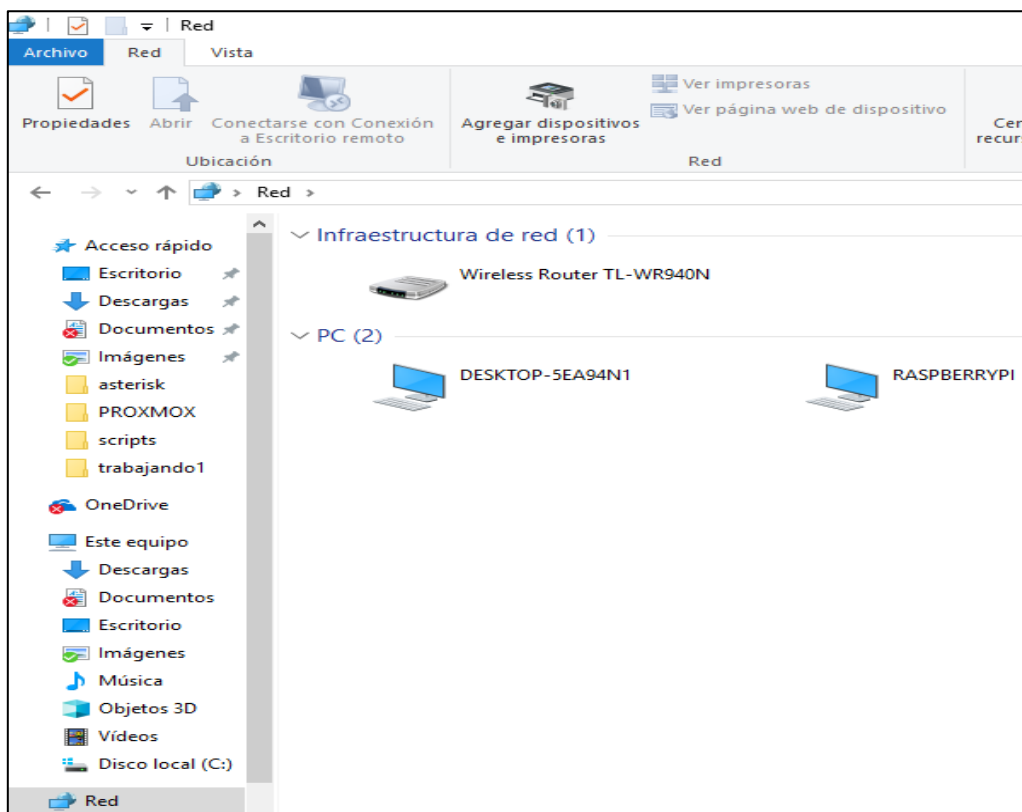
### **2.-ADMINISTRACIÓN DE ARCHIVOS GRABADOS.**

Conforme avanza el tiempo, el disco de almacenamiento se llenará con archivos grabados. Si hay archivos que desea guardar, trasládelos a su computadora para almacenarlos y verlos posteriormente. Para evitar que el sistema se sature se debe generar espacio para el almacenamiento de archivos ya sea borrando parcialmente o totalmente los archivos anteriores después de respaldar la información necesaria. Este procedimiento se debe realizar cada 4 o 6 semanas.

1.- Si el modo de Alarma y Monitoreo está activado, con la aplicación Zoiper ponga el sistema en modo de Solo Monitoreo ingresando el código y realizando la llamada.

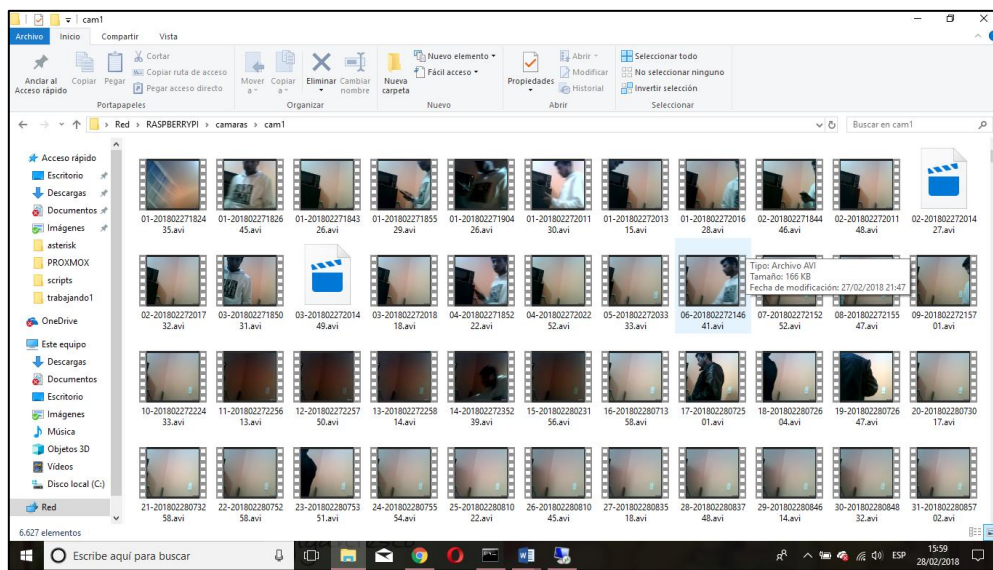
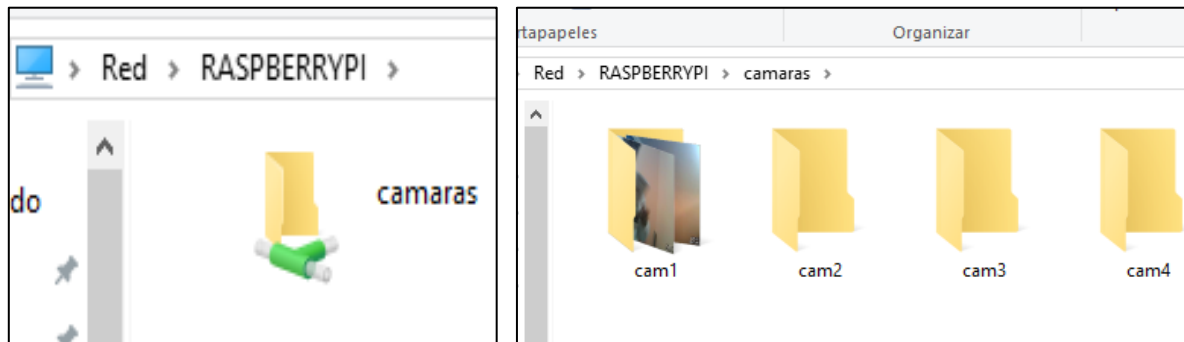


2.- Desde un computador conectado a la red de la empresa diríjase a red dentro se mostrara el disco de almacenamiento del sistema el cual esta compartido, se mostrara con el nombre RASPBERRYPI para ingresar ingrese el usuario y contraseña del sistema.

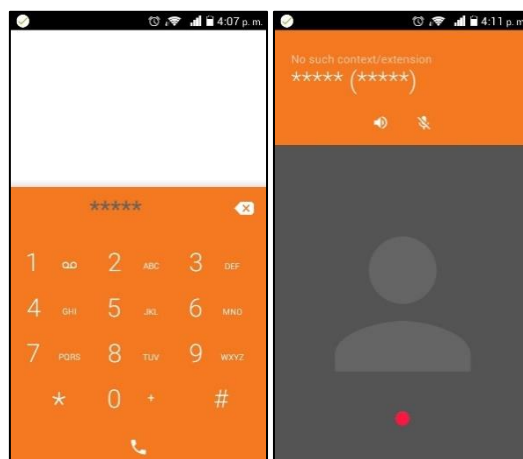




3.- Entre en directorio compartido y respalde los archivos necesarios.



4.- Con la aplicación Zoiper ingrese el código XXXX para borrar los archivos del disco del sistema y generar espacio para continuar grabando. Con la aplicación Zoiper ingrese el código XXXX para reiniciar el sistema.



## **ANEXO 4.- GUÍA DE ADICIÓN DE DISPOSITIVOS (CÁMARAS)**

- 1.- Consideraciones.
- 2.- Adición de cámaras.

### **1.- CONSIDERACIONES**

#### **DISTANCIA**

Si la distancia en la que se desea ubicar la cámara supera los 5 metros adquirir cable USB activo, de lo contrario se conecta directamente en el HUB USB.

#### **ENFOQUE**

Ubicar la cámara en un lugar donde se aproveche la máxima visión del área a monitorear, el enfoque se debe realizar manualmente.

### **2.-ADICIÓN DE CÁMARAS.**

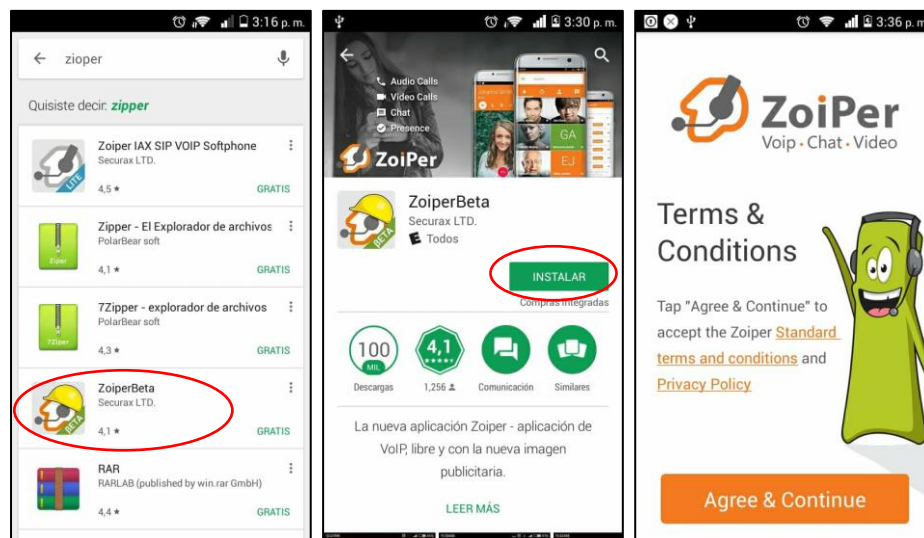
- 1.- Diríjase al gabinete donde se encuentra el equipo del sistema de video vigilancia, verifique que en el HUB USB existan puertos disponibles.
- 2.- Instalar la cámara físicamente en el área a monitorear.
- 3.-Conecte el cable USB al puerto del HUB USB.
- 4.- Reinicie el modo de Solo Monitoreo utilizando la aplicación Zoiper y el código.
- 5.- Enfocar la cámara para cubrir el área deseada, luego fijarla en la posición final.

## ANEXO 5.- GUÍA DE USO Y REGISTRO DE USUARIO EN EL SOFTPHONE.

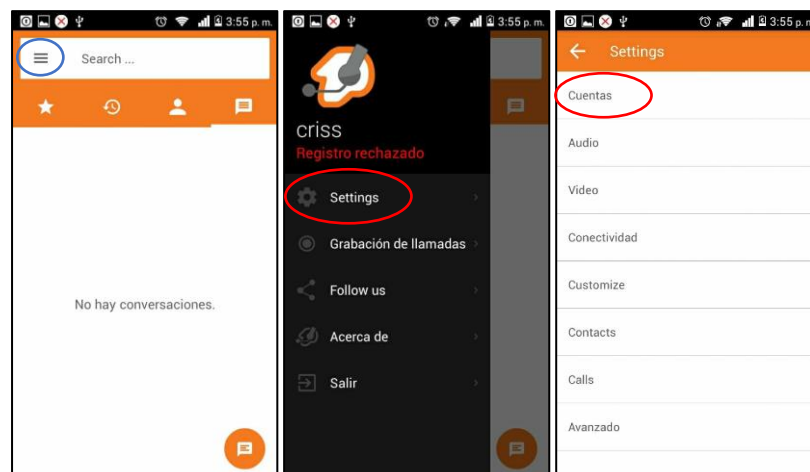
### 1.- CONFIGURACIÓN PARA APLICACIÓN ZOIPER EN ANDROID.

Verificar que la conexión a internet del teléfono este activa por Wi-Fi o datos.

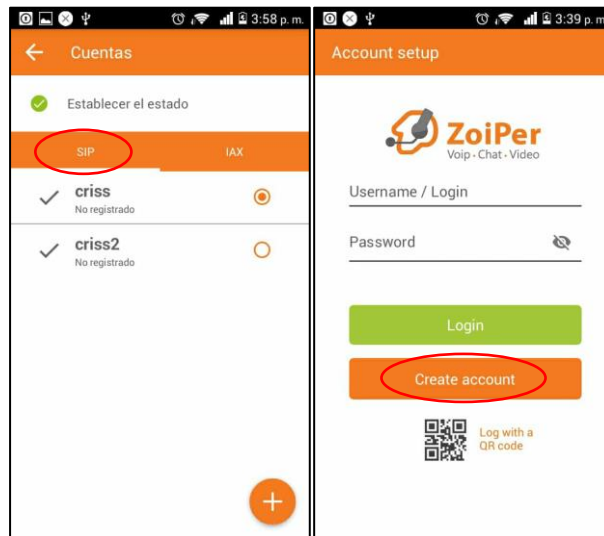
Para descargar la aplicación “ZOIPER” se debe ingresar a la tienda de aplicaciones Play Store o App Store y realizar la búsqueda de la aplicación abajo indicada (versión gratuita), e instalársela.



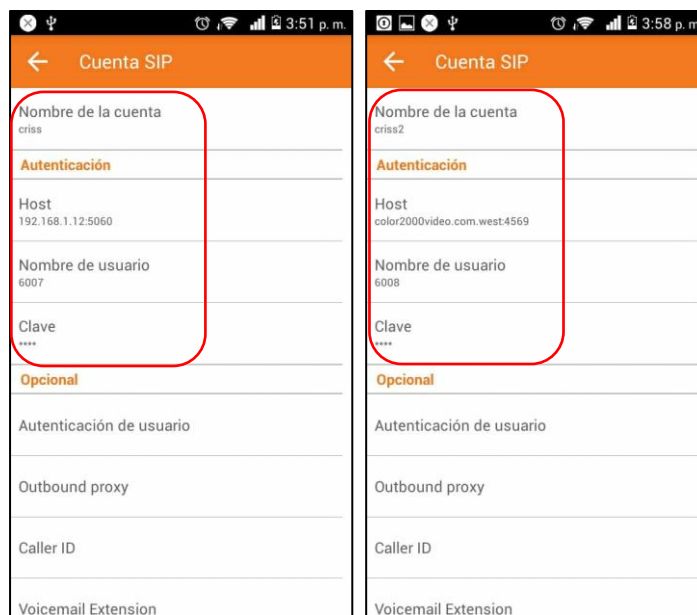
Una vez instalada; ir la esquina superior izquierda y abrir el menú y seleccionar configuraciones, luego en cuentas y en SIP.



Para adicionar nuestra cuenta; debemos seleccionar SIP o IAX, luego elegir crear cuenta



En el espacio de Nombre de cuenta, Host, Nombre de usuario y Clave ingrese los datos proporcionado por el administrador. Guarde la configuración.



## ANEXO 6.- CÓDIGO HTML DE LA PÁGINA WEB DE VISUALIZACIÓN.

### SERVIDOR LAMP

Para conseguir un entorno Web, desde donde se podrá interactuar con las cámaras y controlar la activación del modo de alarma.

Se necesita instalar un Servidor LAMP (Linux, Apache, Mysql, PHP).

#### 1.- Actualizar el sistema operativo y los repositorios:

```
sudo apt-get update
sudo apt-get upgrade
```

#### 2.-Instalar el servicio de Apache2:

```
sudo apt-get install apache2
```

#### 3.-Instalar php5:

```
sudo apt-get install php5
```

#### 4.-Instalar php mysql:

```
sudo apt-get install php5-mysql
```

#### 5.-Instalar mysql:

```
sudo apt-get install mysql-server *****(colocar la contraseña)*****
```

#### 6.-Instalar phpmyadmin:

```
sudo apt-get install phpmyadmin
****Colocar la contraseña de mysql-server para el usuario root de phpmyadmin****
```

#### 7.-Base de Datos:

Se creó una base de datos con el fin de alojar un inicio de sesión seguro, para la Web que se realizó.

La base de datos se creará con phpmyadmin junto a Mysql anteriormente instalados. Entrar a través de un navegador en la dirección IP, del servidor que en este caso es 192.168.1.12:8080/phpmyadmin.

**Nos aparecerá la siguiente pantalla:**

Ahora se debe introducir el usuario y contraseña que se haya puesto en la instalación.  
Aparecerá esta ventana:  
Aquí ir a la pestaña Base de datos:

Se creará una Base de Datos, poner el nombre, la base de datos creada aparecerá a la izquierda, se pone el nombre de la tabla a crear, se llamará usuarios, y el número de columnas 3, que serán id\_usuario, nombre\_usuario y contraseña.

## 8.-Servidor Apache

Para poder interactuar con las conexiones que se tengan hechas en la raspberry pi desde la Web, se necesitará hacer llamadas a los Script que contengan el modo en el que queremos que actúen.

En primer lugar debemos dar los siguientes permisos al directorio de apache.

```
sudo chmod 775 /var/www/html
```

Añadimos al usuario de apache www-data al grupo pi.

```
sudo usermod -a -G www-data pi
```

Ahora debemos dar permisos de root al usuario www-data y además que no le pida contraseña, para que pueda ejecutar los Script.

```
sudo visudo
```

Añadimos una última línea:

```
www-data ALL=(root)NOPASSWD:ALL
```

Reiniciamos el servicio de apache2

```
sudo /etc/init.d/apache2 restart
```

### Código: index.html

```
<!DOCTYPE html>
<!-- Esta página contiene el contenido del inicio de sesión -->
<html>
<head>
  <meta charset="UTF-8">
  <title>Inicio de Sesión</title>
  <link rel="stylesheet" href="css/bootstrap.css">

  <!-- Las siguientes dos líneas se utiliza para que la página sea
multipantalla -->
  <meta name="viewport" content="width=device-width, initial-
scale=1.0">
  <link href="css/bootstrap.min.css" rel="stylesheet"
media="screen">
  <link rel="stylesheet" href="css/style.css">
  <script src="js/bootstrap.js"></script>
  <script src="js/bootstrap.min.js"></script>

</head>
<body>
<h1 align="center" style="color:#00ACC1">SISTEMA DE VIDEO
VIGILANCIA</h1>
<h2 align="center" style="color:#00ACC1"> ALMACEN COLOR 2000 </h2>
<!-- Se utilizará el método POST, para el envío de datos a una
página PHP, en este caso seguridad.php -->
  <div class="login-card">
    <h1>Inicio de Sesión</h1><br>
    <form method="POST" action="seguridad.php">
      <input type="text" name="user" placeholder="Usuario">
```

```

        <input type="password" name="pass" placeholder="Contraseña">
        <input type="submit" class="btn btn-success" value="Iniciar">
    </form>
</div>
</body>
</html>

```

### Código: seguridad.php

```

<?php
    // Recogemos con POST los datos de index.html y los guardamos en
    variables.
    $usuario = $_POST['user'];
    $contrasena = $_POST['pass'];
    // Conectamos con la base de datos, indicando donde está, el
    usuario y la contraseña principal
    $conexion = mysql_connect("localhost","root","avril184");
    // Conectamos con la Base de datos usuario, que es la que
    creamos y donde se ha introducido los datos.
    mysql_select_db("usuario",$conexion);
    // Hacemos una consulta a la base de datos, comprobando que
    coincide el usuario y la contraseña escrita.
    $sql = "SELECT id_usuario FROM usuarios WHERE nombre_usuario
= '$usuario' AND contrasena = '$contrasena' ";
    $comprobar = mysql_query($sql);
    // En caso de que exista, el id_usuario se guardará en una
    cookie, y se redireccionará al archivo principal
    if (mysql_num_rows($comprobar) > 0) {
        $id_usuario = mysql_result($comprobar,0);
        setcookie("misitio_userid","$id_usuario",time() + 3600);
        header("Location:inicio.php");
    }
    // En caso contrario, mostrar que el Usuario o Contraseña son
    incorrectos
    else {
        echo "<meta charset='UTF-8'>";
        echo "<h1 style='color:red'>Usuario o Contraseña
Incorrectos</h1>";
    }

?>

```

### Código: modo.php

```

<html>
    <head>
        <!-- Utilizamos los CSS de Bootstrap y JavaScript -->
        <title>ALMACEN COLOR 2000</title>
        <meta name="viewport" content="width=device-width, initial-
scale=1.0">
        <link href="css/bootstrap.min.css" rel="stylesheet"
media="screen">
        <link type="text/css" href="css/bootstrap.css" />
        <link rel="stylesheet" type="text/css"
href="css/estilos.css" />

```



```

<script src="js/jquery-1.10.1.min.js"></script>
<script src="js/bootstrap.js"></script>
<script src="js/bootstrap.min.js"></script>
<script src="js/npm.js"></script>

<!-- Este script facilita que podamos navegar por el menu
sin salir de la página -->
<script>
$(function(){
  var hash = window.location.hash;
  hash && $('ul.nav a[href="' + hash + '"]').tab('show');
  $('>nav-tabs a').click(function (e) {
    $(this).tab('show');
    var scrollmem = $('>body').scrollTop();
    window.location.hash = this.hash;
    $('>html,body').scrollTop(scrollmem);
  });
});
</script>

</head>
<body>

        <div class="page-header" align="center">
          <h1 class="text-danger" style="color:#00ACC1">
ALMACEN COLOR 2000 </h1>
        </div>
        <div class="tabbable">
          <ul class="nav nav-tabs">
            <li class="active"><a href="inicio.php"
datatoggle="tab"><span>INICIO</span></a></li>
            <br></br>
          </ul>

          <div class="tab-content">
            <!-- Estas lineas contienen el menú, para poder navegar
->

            <!-- Primera opción del menú -->
              <div class="tab-pane active" id="tab1">
<?php
  /* El while contiene la cookie del inicio de sesión, con esto
permitimos que si no se ha iniciado sesión
no se pueda interactuar con el servidor */

  if (isset($_COOKIE['misitio_userid'])) {
    /* Aquí se utiliza el método POST, con botones, en caso de que
se pulse el botón de encendercocina
se registrara una cookie, en el navegador y se actualizará
la página, para que se pueda cumplir la siguiente condición*/

    if (isset($_POST['encendersalon'])) {
      exec("sudo /usr/local/bin/modoalarma.sh start");
      echo "
<br>ttt<br>

```

```

        <div class='center-block' align='center'>
        <h1 align='center' style='color:green'>ALARMA
ACTIVADA</h1>
        <a><img src='on.JPG' width='200px' height='200px'></a>
        </div>";
        //header( "refresh:0;" );
        }

        // En caso de pulsar apagarsalon se elimina la cookie
        anterior, y se actualiza la página
        if (isset($_POST['apagarsalon'])) {
            exec("sudo /usr/local/bin/modoalarma.sh stop");
            echo "
                <br>rrr<br>
                <div class='center-block' align='center'>
                <h1 align='center' style='color:blue'>ALARMA
DESACTIVADA ---- MODO SOLO MONITOREO</h1>
                <a><img src='off.png' width='200px' height='200px'
></a>
                    </div>";
            // header( "refresh:0;" );
            }
        }

?>
        <!-- En estas líneas encontramos los diferentes botones -->
        <form action="" method="post">
            <br><br>
            <div class='center-block' align="center">

                <input type="submit" name="encendersalon" class="btn btn-
                success btn-lg" value="ACTIVAR" align="center" size="18">
                <input type="submit" name="apagarsalon"
                value="DESACTIVAR" class="btn btn-primary btn-lg" align="center">
                <br><br>
            </div>
            <br>
        </form>
        <div class='center-block' align="center">
            <a href="inicio.php" class='center-block' align="center"
            style='color:blue' size="18" ><span> INICIO CAMARAS </span></a>
        </div>
        </div>

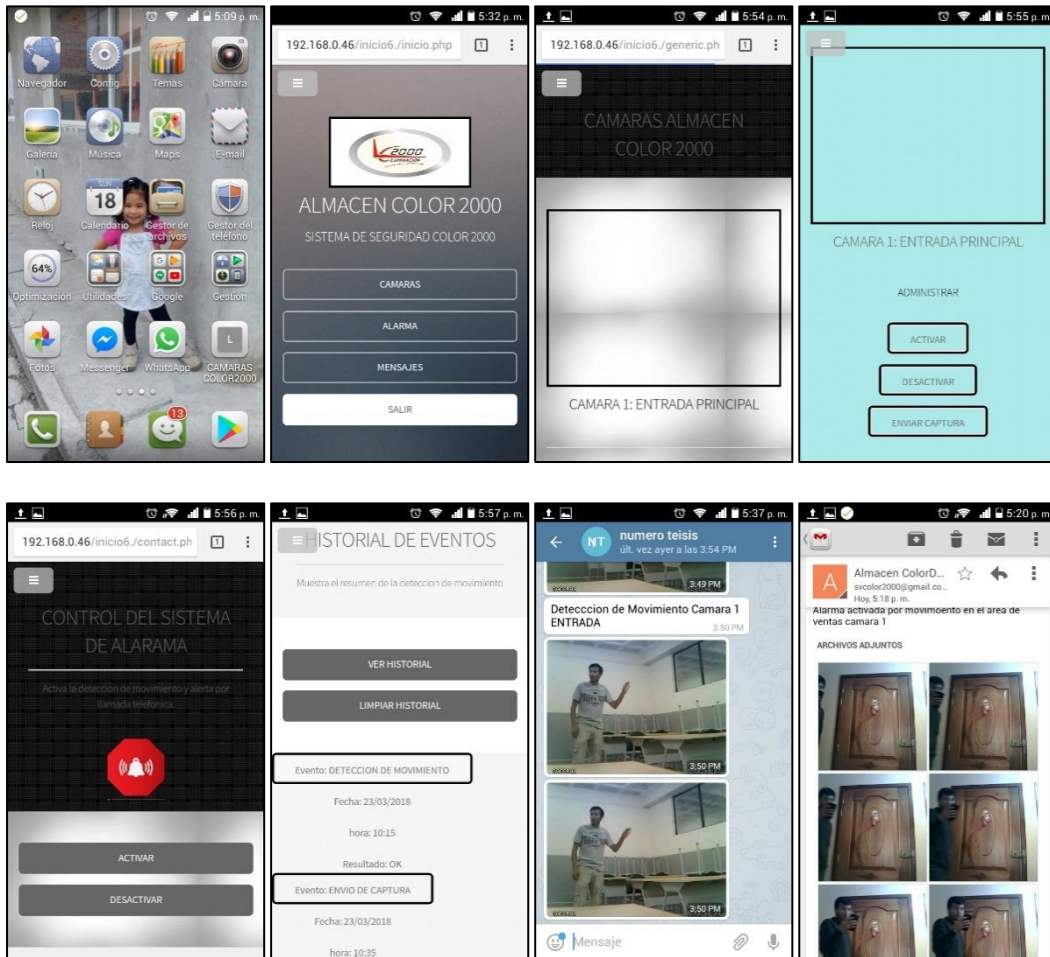
        <div class='center-block' align="center">
            <a href="MENSAJES.html" class='center-block' align="center"
            style='color:blue' size="18" ><span> MENSAJES </span></a>
        </div>

        <div class='center-block' align="center">
            <a href="index.html" class='center-block' align="center"
            style='color:blue' size="18" ><span> SALIR </span></a>
        </div>

```

```
</div>  
</div>  
  
</body>  
</html>
```

**Resultados:**



## ANEXO 7.- CARACTERÍSTICAS DE LAS CÁMARAS Y TELÉFONO MÓVIL USADOS EN EL SISTEMA.

- 1.- Características de la cámara PREMIUM 5MP WEBCAM IMEXX IME-41674.
- 2.- Características del teléfono móvil Nokia C3.

### 1.- CARACTERÍSTICAS DE LA CÁMARA PREMIUM 5MP WEBCAM IMEXX IME-41674.

Cámara Imexx IME-41674.



Línea: **Imexx**  
 Código de producto: IME-41674  
 Disponibilidad: **En stock**



**Suave**  
 Hasta 30 fps.



**Simple**  
 True plug and play.



**Versátil**  
 rotación omnidireccional.



**Voz**  
 incorporado en el micrófono digital.

### CARACTERÍSTICAS

- Sensor de imagen de 5.0 megapíxeles
- Sin conductor
- Se adapta a todos los monitores LCD y portátiles
- Botón de instantánea
- Micrófono digital incorporado: 56db
- Rotación Omni direccional
- Clip multifuncional
- Conecta y reproduce
- Velocidad de fotogramas de hasta 30 fps
- Distancia de enfoque: 30 mm ~ infinity (VGA)
- Formato de video: color verdadero de 24 bits
- Interfaz: compatible con USB 2.0 y USB 1.1
- Windows y Mac OS 7 Certified

## 2.- CARACTERÍSTICAS DEL TELÉFONO MÓVIL NOKIA C3.

Teléfono móvil Nokia c3.



### CARACTERÍSTICAS

<b>GENERAL</b>	<b>Anunciado</b>	2010, abril
	<b>Lanzamiento</b>	Disponible. Lanzamiento
	<b>Dimensiones</b>	115.5 x 58.1 x 13.6 mm, 63.2 cc
	<b>Peso</b>	114 g
<b>RED</b>	<b>2G</b>	GSM 850 / 900 / 1800 / 1900
	<b>3G</b>	
	<b>4G</b>	
	<b>Max. Velocidad</b>	
	<b>SIM</b>	Meni-SIM
<b>PANTALLA</b>	<b>Tipo</b>	TFT, 256K colores
	<b>Tamaño / Resolución</b>	320 x 240 pixels, 2.4 pulgadas (~167 ppi)
	<b>Táctil</b>	
<b>CÁMARA</b>	<b>Cámara principal</b>	2 MP, 1600 x 1200 pixels
	<b>Video Cámara Principal</b>	QCIF@15fps
	<b>Camara secundaria</b>	No
<b>CONECTIVIDAD</b>	<b>USB</b>	microUSB v2.0
	<b>Bluetooth</b>	v2.1, A2DP, EDR
	<b>WiFi</b>	Wi-Fi 802.11 b/g
	<b>Auriculares Jack 3.5</b>	Sí
<b>ALMACENAMIENTO</b>	<b>Memoria Interna</b>	55 MB, 64 MB RAM, 128 MB ROM
	<b>Ranura de memoria</b>	microSD, hasta 8 GB, 2 GB enclused
<b>MULTIMEDIA / INTERNET</b>	<b>Mensajería</b>	SMS, MMS, Email, Push Email, IM
	<b>Radio FM</b>	Stereo FM radio con RDS
<b>SISTEMA</b>	<b>Sistema operativo</b>	
	<b>Sensores</b>	
	<b>Procesador</b>	
	<b>GPS</b>	No
<b>AUTONOMÍA</b>	<b>Batería</b>	Li-Ion 1320 mAh (BL-5J)
	<b>Autonomía en espera</b>	Hasta 800 h
	<b>Autonomía en conversación</b>	Hasta 7 h
	<b>Autonomía en música</b>	
<b>EXTRAS</b>	<b>Extras</b>	<ul style="list-style-type: none"> <li>- Social network entegration</li> <li>- MP4/AVI/H.264/WMV player</li> <li>- MP3/WAV/WMA/eAAC+ player</li> <li>- Voice comando/marcación</li> <li>- Organizador</li> <li>- Entrada de texto predictivo</li> </ul>

## **ANEXO 8.- MANUAL DE PRUEBAS DE FUNCIONAMIENTO**

Este manual tiene la finalidad de comprobar las funcionalidades del sistema así como los métodos de accesos para administración del mismo.

### **Métodos de acceso para administración y configuración del sistema de video vigilancia.**

El acceso al sistema se puede realizar local y remotamente:

Localmente utilizando una laptop, computador de escritorio, Tablet o Smartphone los que deben estar conectados a la red de cableada o inalámbrica de la empresa, dicho de otra forma a la red LAN. Para el acceso local al sistema mediante Tablet o Smartphone se requiere de una aplicación como lo es Remote ToGo.

Remotamente utilizando una laptop, computador de escritorio, Tablet o Smartphone los que deben estar conectados a Internet o contar con el servicio de datos móviles. Para el acceso Remoto al sistema mediante Laptop o computador de escritorio es necesario ingresar a la página de Weaved para internet de las cosas <https://developer.weaved.com/portal/login.php> con el usuario y contraseña correspondientes para luego acceder normalmente por conexión a escritorio remoto. Para el acceso con Tablet o Smartphone se requiere de dos aplicaciones como lo son Weaved pi y Remote ToGo.

## 1.- Verificación de la función de acceso local y remoto a al sistema.

Métodos de acceso al sistema de video vigilancia			Resultados y observaciones
Acceso local al sistema	Laptop/PC	Mediante escritorio remoto	
	Tablet	Mediante aplicación Remote ToGo	
	Smartphone	Mediante aplicación Remote ToGo	
Acceso remoto al sistema	Laptop/PC	Mediante aplicación Weaved pi y Escritorio remoto	
	Tablet	Mediante aplicación Weaved pi y aplicación Remote ToGo	
	Smartphone	Mediante aplicación Weaved pi y aplicación Remote ToGo	

**Modos de funcionamiento del sistema de video vigilancia:**

El sistema de video vigilancia tiene dos modos de funcionamiento el modo de Solo Monitoreo y el modo Alarma y Monitoreo.

**Modo de Solo Monitoreo:** En este modo de funcionamiento del sistema se visualiza el video transmitido por las camaras, la presentación de la página web de monitoreo con las cámaras transmitiendo. Se visualiza la transmisión individual de cada cámara utilizando las aplicaciones para visualización local y remota.

## 2.- Verificación de la visualización de las cámaras del sistema de video vigilancia.

Visualización de las cámaras del sistema de video vigilancia			Resultados y observaciones
Visualización de las cámaras desde la red local	Laptop/PC	Mediante Navegador Web (Dirección IP de La Página/Cámara de monitoreo + Puerto)	
	Tablet	Mediante Navegador Web  Aplicación Weaved pi	
	Smartphone	Mediante Navegador Web  Aplicación Weaved pi	
Visualización de las cámaras desde Internet	Laptop/PC	Mediante Navegador Web (Dirección Url: ingresar a la página de Weaved para internet de las cosas <a href="https://developer.weaved.com/portal/login.php">https://developer.weaved.com/portal/login.php</a> con el usuario y contraseña)	
	Tablet	Aplicación Weaved pi	
	Smartphone	Aplicación Weaved pi	

**Modo de Alarma y Monitoreo:** El sistema de alarma cumple una función complementaria al sistema de video vigilancia en su modo de Solo Monitoreo, el sistema funcionara con normalidad con todas las características del primer modo, pero además este modo de funcionamiento hará que las cámaras actúen en forma de sensores de movimiento, independientemente de su función de capturar imágenes y video.



En la gestión de eventos (Detección de Intrusos en las áreas monitoreadas) intervienen los softwares: Asterisk para realizar una llamada de alerta al móvil del gerente y gestionar la sirena mediante un IVR (Respuesta interactiva de voz ), Mutt para enviar un correo con imágenes correspondientes al sitio de la intrusión con la etiqueta de la cámara que detecto el evento y Telegram para el envío de mensajes instantáneos a la cuenta del gerente con la etiqueta de la cámara q detecto la intrusión.

### 3.- Verificación de la detección de movimiento y control de eventos.

Métodos de control para el sistema de video vigilancia		Resultados	
Detección de una intrusión y gestión de eventos por los softwares (Alarma).	Software de gestión de reproducción de audio mpg123.	<b>Activación de sirena de Alarma</b> mediante reproducción: (sonido de sirena por altavoces )	
	Software de gestión de mensajes instantáneos Telegram.	<b>Envío de mensaje a cuenta del gerente</b> mediante detección de movimiento: (etiqueta de cada cámara )	
	Software de gestión de correo electrónico Mutt.	<b>Envío de mensaje a correo de la empresa</b> con imágenes de la detección de movimiento (etiqueta de cada cámara )	
	Software de gestión de llamadas (Asterisk) y módulo Gateway de voz hacia la red GSM (Chan Mobile) <b>IVR</b>	<b>Opción 1.-</b> Digite 1 para reiniciar el sistema.	
		<b>Opción 2.-</b> Digite 2 para cambiar a modo solo monitoreo.	
		<b>Opción 3.-</b> Digite 3 para activar sirena inmediatamente.	
		<b>Opción 4.-</b> Digite 4 para silenciar la sirena.	

### Método de control local y remoto para el sistema de video vigilancia.

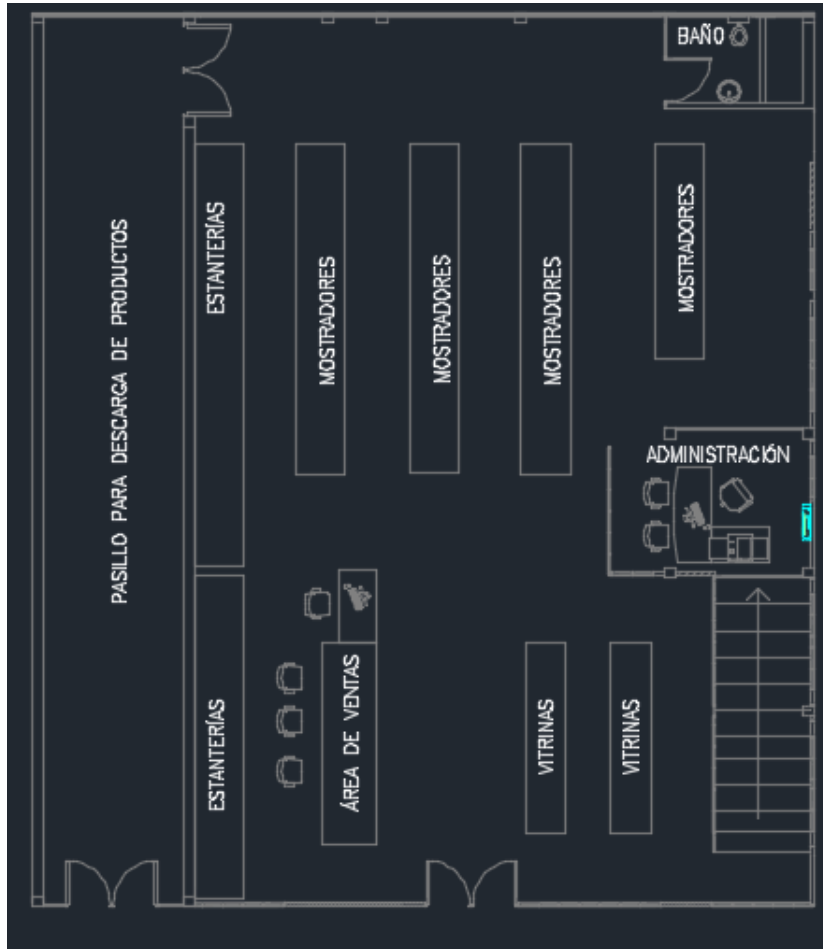
Funcionamiento:

Este sistema necesita un método de control para su activación y desactivación, el cual será gestionado por el software Asterisk mediante un plan de marcado en un formato específico gestionando de forma local con una cuenta SIP y remotamente con una cuenta IAX.

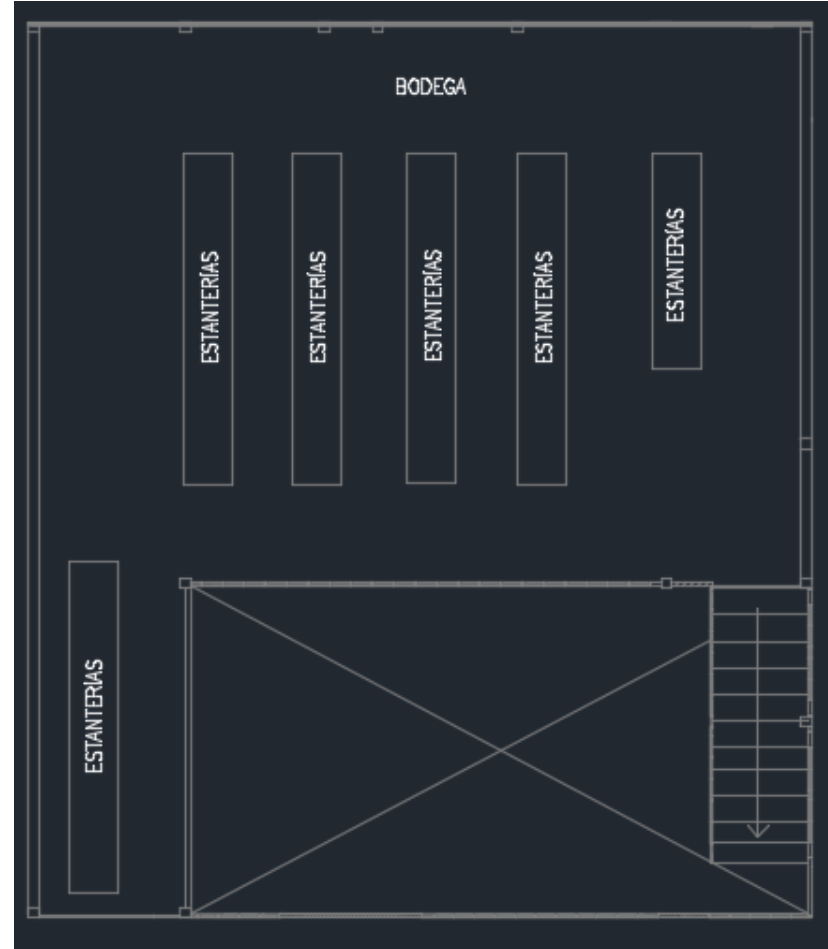
#### 4.- Métodos de control para el sistema de video vigilancia.

Métodos de control para el sistema de video vigilancia		Resultados
Control a nivel local para el sistema	Software de gestión Asterisk  Aplicación <b>Zoioper</b> <b>Cuenta SIP</b>	<b>Activación sistema de Alarma</b> mediante marcación: (Código de Activación )
		<b>Desactivación de sistema de Alarma</b> mediante marcación: (Código de Desactivación )
		<b>Activación y Desactivación de la Sirena</b> mediante marcación: (Código de Activación y Desactivación )
Control a nivel remoto para el sistema	Software de gestión Asterisk  Aplicación <b>Zoioper</b> <b>Cuenta IAX</b>	<b>Activación sistema de Alarma</b> mediante marcación: (Código de Activación )
		<b>Desactivación de sistema de Alarma</b> mediante marcación: (Código de Desactivación )
		<b>Activación y Desactivación de la Sirena</b> mediante marcación: (Código de Activación y Desactivación )

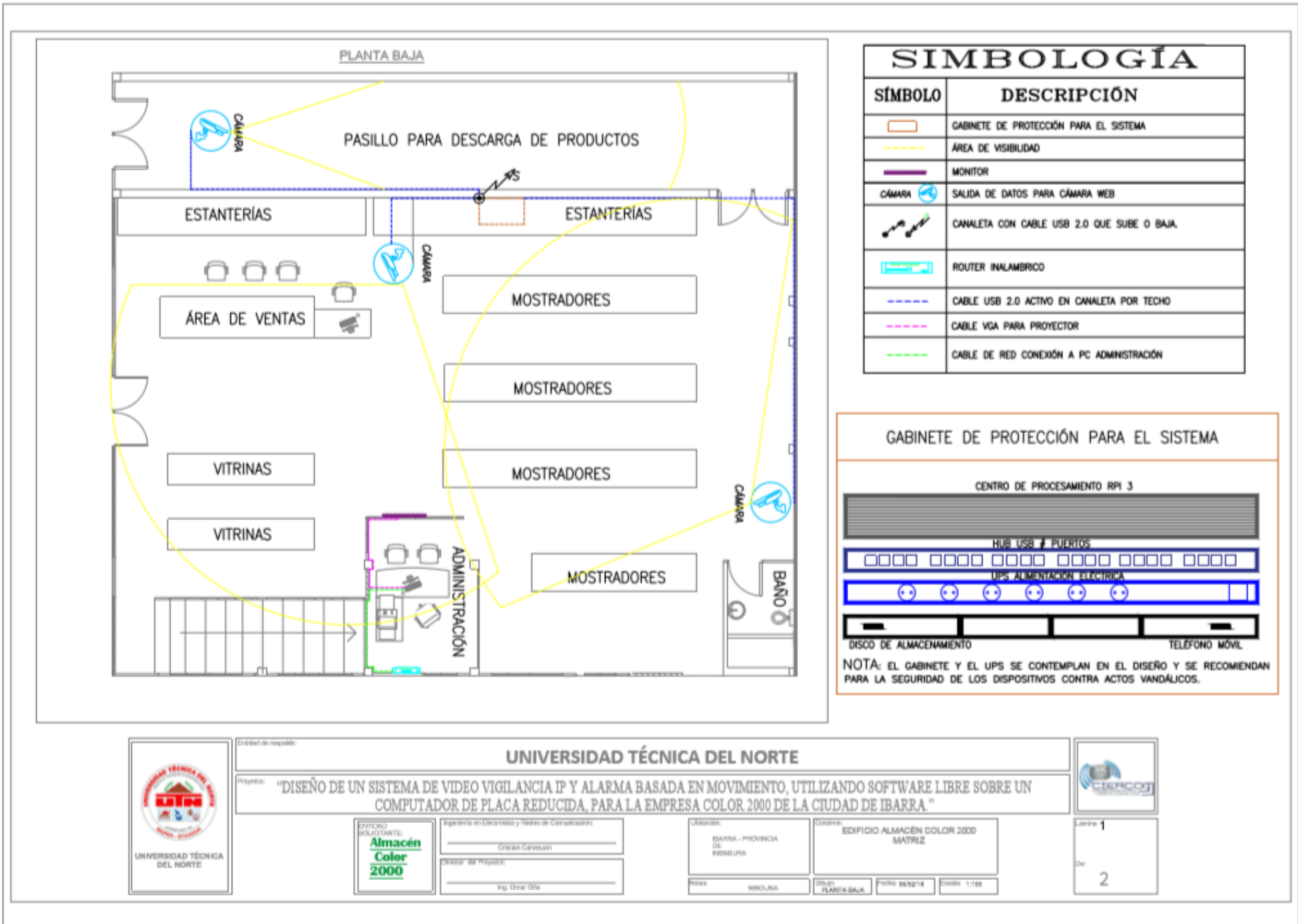
**ANEXO 9.- PLANOS DE INFRAESTRUCTURA Y DISEÑO DEL SISTEMA**



Planta baja

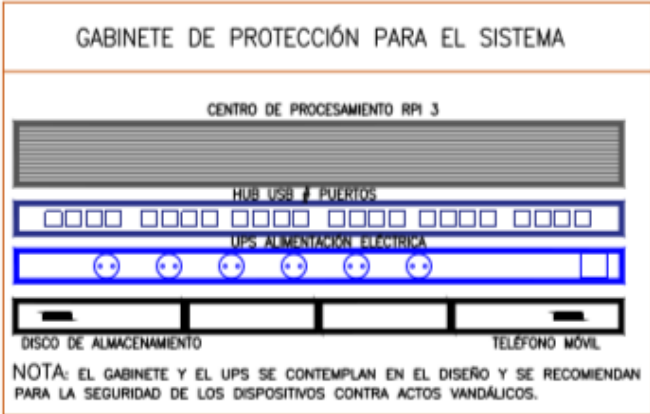


Primera planta



### SIMBOLOGÍA

SÍMBOLO	DESCRIPCIÓN
	GABINETE DE PROTECCIÓN PARA EL SISTEMA
	ÁREA DE VISIBILIDAD
	MONITOR
	SALIDA DE DATOS PARA CÁMARA WEB
	CANAleta CON CABLE USB 2.0 QUE SUBE O BAJA.
	ROUTER INALÁMBRICO
	CABLE USB 2.0 ACTIVO EN CANALETA POR TECHO
	CABLE VGA PARA PROYECTOR
	CABLE DE RED CONEXIÓN A PC ADMINISTRACIÓN



**UNIVERSIDAD TÉCNICA DEL NORTE**

Proyecto: "DISEÑO DE UN SISTEMA DE VIDEO VIGILANCIA IP Y ALARMA BASADA EN MOVIMIENTO, UTILIZANDO SOFTWARE LIBRE SOBRE UN COMPUTADOR DE PLACA REDUCIDA, PARA LA EMPRESA COLOR 2000 DE LA CIUDAD DE IBARRA."



ESTUDIO SOLICITANTE:  
**Almacén Color 2000**

Gerencia en telecomunicaciones y Redes de Comunicación

Orlando Carrasquin

Director del Proyecto:

Ing. Oscar Oña

Ubicación:  
IBARRA - PROVINCIA DE MORONA

Código:  
EDIFICIO ALMACÉN COLOR 2000 MATRIZ

Fecha:  
MORONA

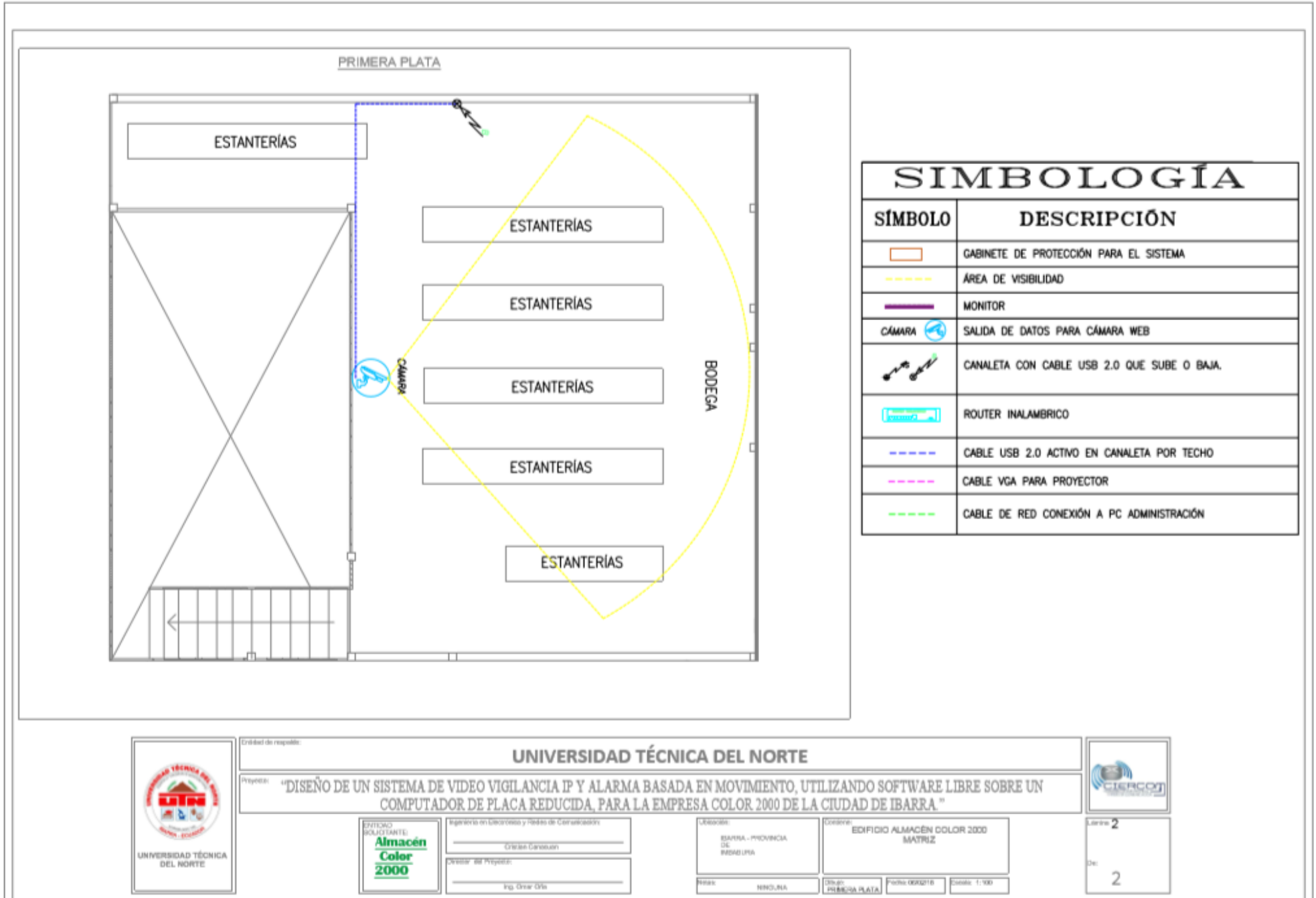
Diseño:  
PLANTA BAJA

Fecha:  
06/02/18

Escala:  
1:100

Lamina **1**

De **2**



Entidad de respaldo: **UNIVERSIDAD TÉCNICA DEL NORTE**

Proyecto: "DISEÑO DE UN SISTEMA DE VIDEO VIGILANCIA IP Y ALARMA BASADA EN MOVIMIENTO, UTILIZANDO SOFTWARE LIBRE SOBRE UN COMPUTADOR DE PLACA REDUCIDA, PARA LA EMPRESA COLOR 2000 DE LA CIUDAD DE IBARRA."



ENTIDAD SOLICITANTE:  
**Almacén Color 2000**

Ingeniería en Laboratorios y Redes de Comunicaciones

Origen Consultor: \_\_\_\_\_

Director del Proyecto: \_\_\_\_\_

Ing. Omar Oro \_\_\_\_\_

Ubicación: IBARRA - PROVINCIA DEL PASTAZA

Código: EDIFICIO ALMACÉN COLOR 2000 MATRIZ

Fecha: \_\_\_\_\_

Escala: 1:100

# ALMACÉN COLOR 2000

## CERTIFICO:

Que he recibido el producto final que consiste en la implementación del diseño de un sistema de video vigilancia y alarma, el cual forma parte del proyecto de titulación: **DISEÑO DE UN SISTEMA DE VIDEO VIGILANCIA IP Y ALARMA BASADA EN MOVIMIENTO, UTILIZANDO SOFTWARE LIBRE SOBRE UN COMPUTADOR DE PLACA REDUCIDA, PARA LA EMPRESA COLOR 2000 DE LA CIUDAD DE IBARRA**, del señor Cristian Germán Canacuan Ipiales.

Es todo cuanto se puede certificar; faculto al interesado hacer uso del presente en lo fines que estime conveniente, excepto en trámites judiciales.

Atentamente:



Ing. Alicia de Carmen Ramos Páez

GERENTE. ALMACÉN COLOR 2000

Ibarra, 22 de febrero del 2018