

UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA



**“DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA
INTEGRAL DE SEGURIDAD, CONTROLADO Y
MONITOREADO EN FORMA LOCAL Y REMOTA
MEDIANTE LAS REDES DE COMUNICACIÓN PARA LAS
AGENCIAS DE CAJA RURAL – LOS ANDES S.A.”**

TESIS

PRESENTADA POR:

LIMA ORTEGA EDGAR JOAQUIN

ESPILLICO CONDORI JOSE LUIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

PUNO - PERÚ

2015

UNIVERSIDAD NACIONAL DEL ALTIPLANO
FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA INTEGRAL DE
SEGURIDAD, CONTROLADO Y MONITOREADO EN FORMA LOCAL Y
REMOTA MEDIANTE LAS REDES DE COMUNICACIÓN PARA LAS
AGENCIAS DE CAJA RURAL – LOS ANDES S.A."

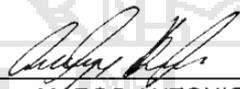
TESIS PRESENTADA POR:

EDGAR JOAQUIN LIMA ORTEGA
JOSE LUIS ESPILLICO CONDORI

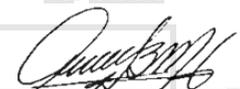
PARA OPTAR EL TÍTULO PROFESIONAL DE: INGENIERO
ELECTRÓNICO

APROBADA POR EL JURADO REVISOR CONFORMADO POR:

PRESIDENTE


Mg. Ing. MARCO ANTONIO QUISPE BARRA

PRIMER MIEMBRO


M. Sc. Ing. PEDRO BEJAR MUÑOZ

SEGUNDO MIEMBRO


Mg. Ing. KARLOS ALEXANDER CCANTUTA CHIRAPO

DIRECTOR DE TESIS


M. Sc. Ing. GAVINO JOSÉ FLORES CHIPANA

ASESOR DE TESIS


M. Sc. Ing. IVAN DELGADO HUAYTA

ASESOR DE TESIS


Ing. DIMAS ARTURO LOAYZA SALAS

Puno - Perú

2015

ÁREA: Telecomunicaciones

TEMA: Aplicaciones en telecomunicaciones

AGRADECIMIENTOS

Las personas que merecen nuestro agradecimiento son innumerables y solamente por razones de espacio no se encuentran mencionadas, aunque saben que son incluidas con singular afecto.

A los docentes de la Escuela Profesional de Ingeniería de Electrónica de la Universidad Nacional del Altiplano, por los conocimientos compartidos para nuestra formación académica y profesional. Especialmente para el Ing. Marco Antonio Quispe Barra por su guía, motivación y comentarios para la realización del presente trabajo.

Al Ing. Marco Antonio Quispe Barra, Ing. Pedro Bejar Muñoz, Ing. Karlos Alexander Ccantuta Chirapo, Ing. Gavino José Flores Chipana e Ing. Ivan Delgado Huayta, los mismos que contribuyeron en la revisión y mejora del presente trabajo de investigación.

A todas aquellas personas que aun sin saberlo contribuyeron a la realización de este trabajo, a aquellos que sin conocernos fueron guías en nuestro trabajo y pusieron los cimientos para su realización.

DEDICATORIA

Con todo mi cariño y mi amor para las personas que hicieron todo en la vida para que yo pudiera lograr mis sueños, por motivarme y darme la mano cuando sentía que el camino se terminaba, a ustedes por siempre mi corazón y mi agradecimiento.

Papá y Mamá

Posiblemente en estos momentos no entiendas mis palabras, pero para cuando seas capaz, quiero que te des cuenta de lo que significas para mí. Eres la razón de que me levante cada día, esforzarme por el presente y el mañana, eres mi principal motivación.

Como en todos mis logros, en este has estado presente.

Muchas gracias, Hija.

Les doy gracias por ser parte de mi vida y aunque cada uno es diferente al otro, todos somos uno solo.

Edgar Joaquin.

DEDICATORIA

A quienes más que una luz,
son el sendero que guía mis
pasos hacia una vida
mejor..... mi familia.

A quien en todo momento me
brindó su apoyo incondicional
para la culminación del presente
trabajo.

A mis amigos... por ser las piezas
del rompecabezas que
complementaron la realización de
mis sueños.

José Luis

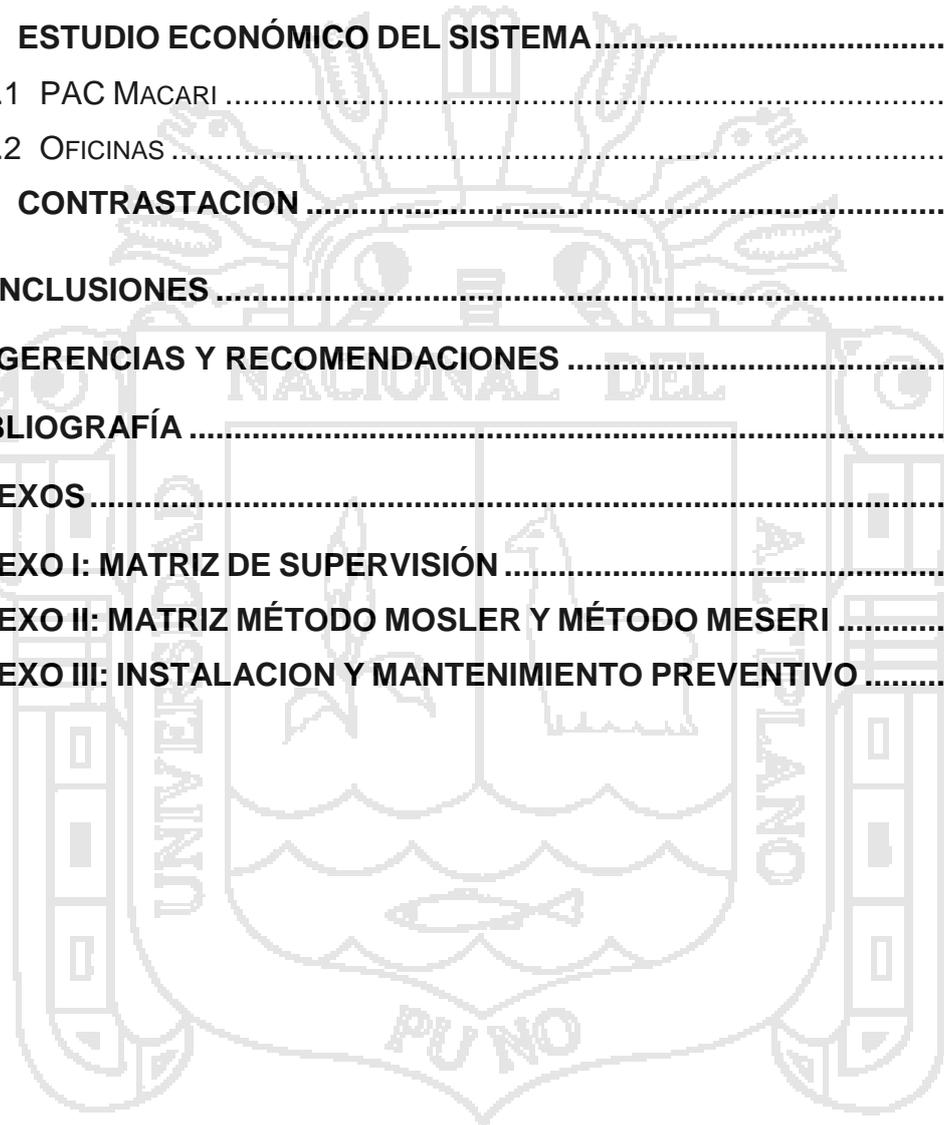
INDICE

RESUMEN	13
ABSTRACT	14
INTRODUCCIÓN	15
CAPITULO I.....	17
1 PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACION	18
1.1 DESCRIPCIÓN DEL PROBLEMA.....	18
1.1.1 FORMULACIÓN DEL PROBLEMA	18
1.1.2 SISTEMATIZACIÓN DEL PROBLEMA	18
1.2 JUSTIFICACION DEL PROBLEMA.....	19
1.3 OBJETIVOS DE LA INVESTIGACION.....	20
1.3.1 OBJETIVO GENERAL.....	20
1.3.2 OBJETIVOS ESPECÍFICOS	20
CAPITULO II.....	22
2 MARCO TEORICO	23
2.1 ANTECEDENTES DE LA INVESTIGACION	23
2.2 SUSTENTO TEORICO	24
2.2.1 SEGURIDAD BANCARIA.....	24
2.2.1.1 Tipos de Seguridad.....	25
2.2.1.2 Catálogo de Riesgos	26
2.2.1.3 Documentación en Seguridad Bancaria	28
2.2.2 PLANES DE EMERGENCIA	30
2.2.2.1 Base Legal:.....	30
2.2.3 PLAN DE SEGURIDAD CONTRA ACTOS ANTISOCIALES	31
2.2.3.1 Análisis y Evaluación De Riesgos.....	31
2.2.3.2 Medios de Protección	34
2.2.3.3 Manual de Procedimientos	36
2.2.4 PLAN DE SEGURIDAD PARA TRANSPORTE DE VALORES.....	36
2.2.4.1 Análisis y Evaluación De Riesgos.....	37
2.2.4.2 Medios de Protección	38
2.2.4.3 Manuales de Procedimientos.....	40

2.2.5 SISTEMAS DE PROTECCIÓN ACTIVA	40
2.2.5.1 Circuito Cerrado de Televisión.....	40
2.2.5.1.1 Formatos de Video	43
2.2.5.1.2 Componentes de un sistema de CCTV	47
2.2.5.1.3 Características de las Cámaras	48
2.2.5.1.3.1 Lentes	51
2.2.5.1.4 Medio de Transmisión	53
2.2.5.1.4.1 Medios Analógicos.....	54
2.2.5.1.4.2 Medios Inalámbricos	57
2.2.5.1.5 Video Grabadores Digitales	58
2.2.5.1.6 Monitoreo	59
2.2.5.2 Sistema de Control de Acceso.....	60
2.2.5.3 Sistema Central de Alarma.....	63
2.2.5.3.1 Tipos de Centrales de Alarma.....	64
2.2.5.3.2 Principales características de la Central de Alarmas.....	66
2.2.5.3.3 Partes Básicas de una Central de Alarma.....	71
2.2.5.3.3.1 Panel de Control	71
2.2.5.3.3.2 Teclado	72
2.2.5.3.3.3 Sirena	73
2.2.5.3.3.4 Sensores interiores de movimiento.....	73
2.2.5.3.3.5 Sensores Magnéticos	74
2.2.5.3.3.6 Detector de Humo.....	75
2.2.5.3.3.7 Botones de Pánico.....	76
2.3 GLOSARIO DE TERMINOS BASICOS	76
2.4 HIPOTESIS DE LA INVESTIGACION	77
2.4.1 HIPÓTESIS ESPECÍFICA	77
2.5 OPERACIONALIZACION DE VARIABLES	77
2.5.1 VARIABLES DEPENDIENTES.....	77
2.5.2 VARIABLES INDEPENDIENTES	78
CAPITULO III.....	79
3 DISEÑO METODOLÓGICO DE LA INVESTIGACIÓN	80
3.1 TIPO Y DISEÑO DE INVESTIGACIÓN	80
3.2 POBLACIÓN Y MUESTRA DE LA INVESTIGACIÓN	80

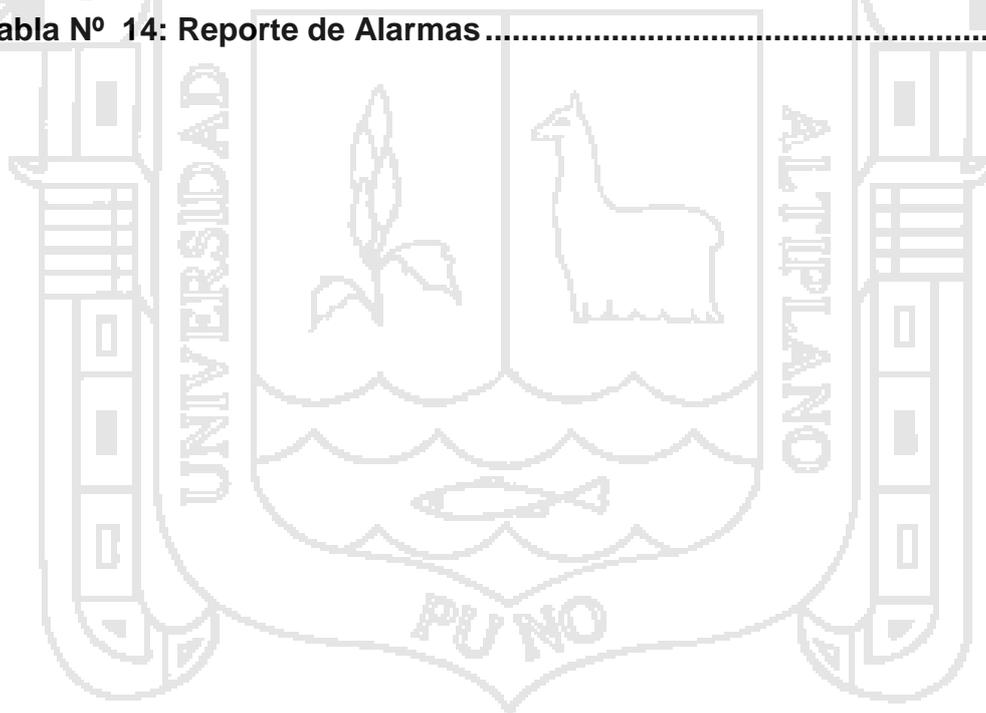
3.2.1 POBLACIÓN	80
3.2.2 MUESTRA.....	82
3.3 UBICACIÓN Y DESCRIPCIÓN DE LA POBLACIÓN.....	82
3.4 MATERIAL EXPERIMENTAL.....	82
3.5 TÉCNICAS E INSTRUMENTOS PARA RECOLECTAR INFORMACIÓN	83
3.6 TÉCNICAS PARA EL PROCESAMIENTO Y ANÁLISIS DE DATOS.....	84
3.7 PROCEDIMIENTO DEL EXPERIMENTO	84
3.8 PLAN DE TRATAMIENTO DE DATOS.....	85
3.9 PRUEBA DE LA HIPÓTESIS	86
3.9.1 HIPÓTESIS ESPECIFICA 01	86
3.9.2 HIPÓTESIS ESPECIFICA 02.....	86
3.9.3 HIPÓTESIS GENERAL.....	87
CAPITULO IV	88
4 ANÁLISIS, E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN.....	89
4.1 ESCENARIO INICIAL.....	89
4.1.1 OFICINA ILAVE	89
4.1.2 OFICINA COATA	91
4.1.3 PAC MACARI	91
4.2 REQUISITOS DEL SISTEMA DE SEGURIDAD.....	91
4.2.1 REQUISITOS MÍNIMOS.....	92
4.2.2 APLICACIÓN BANCARIA.....	94
4.3 SISTEMA DE SEGURIDAD IMPLEMENTADO.....	96
4.3.1 SISTEMA DE SEGURIDAD EN OFICINAS	96
4.3.1.1 Central de alarma	96
4.3.1.1.1 Características de una Central de Alarma.....	98
4.3.1.2 Circuito cerrado de televisión.....	102
4.3.2 SISTEMA DE SEGURIDAD EN PAC	103
4.3.2.1 Distribución del sistema de alarma	103
4.3.2.2 Distribución del CCTV	105
4.4 DISPOSITIVOS ELECTRONICOS UTILIZADOS.....	105
4.4.1 PANEL CENTRAL BOSCH.....	105
4.4.2 TARJETAS EXPANSORAS	107

4.4.3	SENSOR DE MOVIMIENTO	108
4.4.4	DETECTOR DE HUMO	109
4.4.5	SENSORES DE RUPTURA DE VIDRIOS.....	110
4.4.6	RECEPTOR PASARELA DE COMUNICACIONES	111
4.5	MEDIOS DE COMUNICACIÓN	112
4.5.1	COMUNICACIÓN POR RED TELEFÓNICA CONMUTADA (RTC).....	112
4.5.2	COMUNICACIÓN POR RED O CELULAR	114
4.6	ESTUDIO ECONÓMICO DEL SISTEMA.....	116
4.6.1	PAC MACARI	116
4.6.2	OFICINAS	117
4.7	CONTRASTACION	118
	CONCLUSIONES	138
	SUGERENCIAS Y RECOMENDACIONES	139
	BIBLIOGRAFÍA	140
	ANEXOS	141
	ANEXO I: MATRIZ DE SUPERVISIÓN	142
	ANEXO II: MATRIZ MÉTODO MOSLER Y MÉTODO MESERI	143
	ANEXO III: INSTALACION Y MANTENIMIENTO PREVENTIVO	146



ÍNDICE DE TABLAS

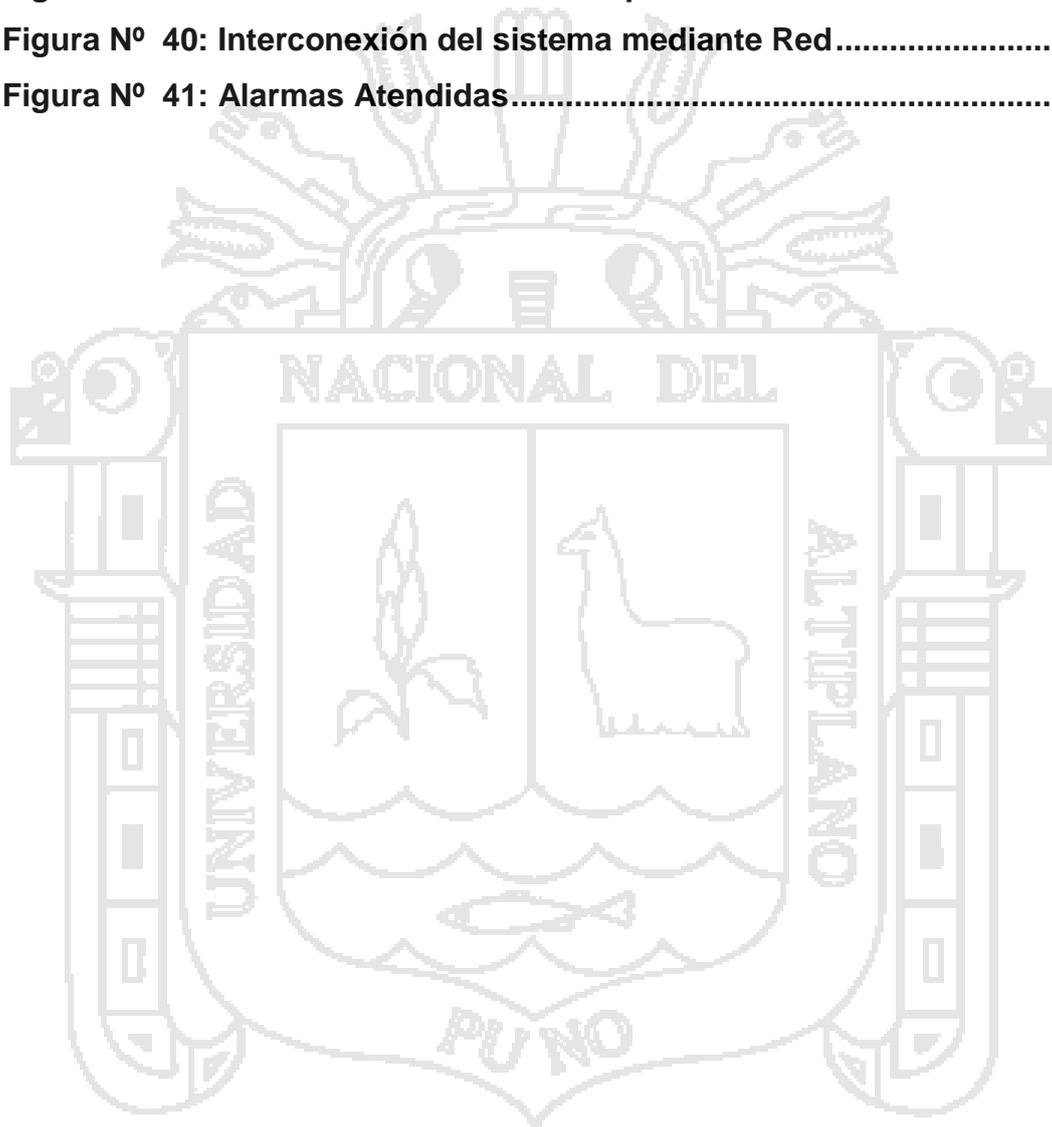
Tabla N° 1: Clasificación de los medios de protección	35
Tabla N° 2: Resolución de Cámaras Analógicas	50
Tabla N° 3: Determinación del Zoom	53
Tabla N° 4: Cuadro de Variables	78
Tabla N° 5: Dirección de Oficinas	81
Tabla N° 6: Puntos de Atención al Cliente	81
Tabla N° 7: Muestra Escogida	82
Tabla N° 8: Características de los paneles Bosch	106
Tabla N° 9: Costos del sistema de alarma en PAC	117
Tabla N° 10: Costo del Sistema de alarma en Oficinas	118
Tabla N° 11: Apertura y Cierre de la Oficina llave	122
Tabla N° 12: Apertura y Cierre de la Oficina Coata	124
Tabla N° 13: Apertura y Cierre de Bóveda	131
Tabla N° 14: Reporte de Alarmas	137



INDICE DE FIGURAS

Figura N° 1: Pirámide de Seguridad Integral	27
Figura N° 2: Resumen Plan Integral de Seguridad	29
Figura N° 3: Plan contra actos Antisociales	31
Figura N° 4: Plan de seguridad transporte de Valores.....	37
Figura N° 5: Esquema de un CCTV	41
Figura N° 6: Interconexión de un CCTV	42
Figura N° 7: Imagen formato PAL	45
Figura N° 8: Formato de Cámaras.....	50
Figura N° 9: Cobertura de los Lentes	51
Figura N° 10: Constitución del cable coaxial	55
Figura N° 11: Distancia Vs numeración del cable	56
Figura N° 12: Video Balun	56
Figura N° 13: CCTV inalámbrico	58
Figura N° 14: DVR LSVISION de 16 canales.....	59
Figura N° 15: Tarjeta RFID	61
Figura N° 16: Control Biométrico.....	63
Figura N° 17: Panel central Bosch.....	71
Figura N° 18: Teclado Bosch.....	72
Figura N° 19: Sensor de movimiento.....	74
Figura N° 20: Sensor magnético para puertas.....	75
Figura N° 21: Detector de Humo	75
Figura N° 22: Esquema central de alarma.....	97
Figura N° 23: Panel de Control Bosch.....	97
Figura N° 24: Circuito Tamper.....	99
Figura N° 25: Zona Cableada.....	99
Figura N° 26: Zona Multiplexada	100
Figura N° 27: Circuito balanceo de Línea.....	101
Figura N° 28: Funcionamiento de Alarma en PAC	103
Figura N° 29: Ubicación de dispositivos	104
Figura N° 30: Dispositivos de Seguridad en Ventanilla	104
Figura N° 31: Ubicación de las Cámaras.....	105
Figura N° 32: Panel de Alarma Oficina llave	106

Figura N° 33: Descripción del Panel.....	107
Figura N° 34: Conexión tarjetas expansoras	108
Figura N° 35: Cobertura de un sensor PIR.....	109
Figura N° 36: Características del sensor de ruptura.....	110
Figura N° 37: Ángulos de funcionamiento	110
Figura N° 38: Posición del sensor de ruptura.....	111
Figura N° 39: Interconexión del Sistema por RTC.....	113
Figura N° 40: Interconexión del sistema mediante Red.....	116
Figura N° 41: Alarmas Atendidas.....	132



RESUMEN

El Proyecto consiste es un sistema nuevo, que utiliza tecnología de última generación, técnicas de electrónica acordes a los conocimientos adquiridos en la carrera universitaria e ideas innovadoras que convierten al sistema de seguridad en un sistema autónomo, que integra diferentes elementos para que trabajen conjuntamente con las redes de comunicación públicas. La primera parte del proyecto consistió en la revisión de la documentación básica necesaria para poder comprender el funcionamiento de este tipo de sistemas, se realizó un estudio de los aspectos geográficos y ambientales a considerar y de la normativa pertinente. Considerando que el ámbito de trabajo de la empresa es el sector Rural, y el factor tecnológico es una limitante muy seria. Por último, se plantea un diseño aplicando los automatismos que permita la máxima eficiencia en el aprovechamiento de los medios geográficos y ambientales para los respectivos sistemas de alarmas.

Palabras Claves: Seguridad, Sensores, Planes de Emergencia, Central receptora de Alarmas y Circuito Cerrado de Televisión

ABSTRACT

The project involves a new system, which uses the latest technology, electronic techniques in line with the knowledge acquired in the university career and innovative ideas that make the security system in an autonomous system that integrates different elements to work together with public communication networks. The first part of the project involved reviewing the basic documentation needed to understand how such systems, a study of geographical and environmental aspects to consider and relevant legislation is made. Whereas the scope of work of the company is the rural sector and the technological factor is a serious limitation. Finally, we propose a design automation application that allows maximum efficiency in the use of geographical and environmental media for the respective alarm systems.

Keywords: Safety, Sensors, Emergency plans, Central alarm receiver, Closed circuit television

INTRODUCCIÓN

En los últimos años se ha observado el crecimiento de la necesidad de seguridad en todas las personas en su vida diaria, en sus lugares de trabajo, por parte de empresas de todo tipo, industrias, Bancos, Financieras etc., esto debido a la gran cantidad de robos, accidentes, incendios, incidentes fortuitos, negligencias cometidas por personas al momento de realizar una actividad, entre otros.

Como antecedentes de este proyecto se ha investigado como manejan el efectivo los diferentes Bancos del sistema financiero del país, y se tiene que desde sus inicios y hasta la actualidad aún se mantiene el manejo tradicional, el cual consiste en la dualidad física (dos personas) para la apertura de la caja fuerte.

Esta tesis promueve el uso de tecnología para diseñar y desarrollar interfaces que se encargaran de automatizar el proceso de apertura física y electrónica de las agencias, teniendo en cuenta además los lineamientos de seguridad con los que debe cumplir el proceso.

Tomando como base todos los conocimientos de Electrónica y Control con las nuevas tecnologías en sistemas de seguridad electrónica, se desarrolla un sistema innovador que funcione casi de forma independiente, que garantice al máximo la seguridad de la empresa Caja Rural - Los Andes S.A. y sea muy versátil en su manejo.

En el Capítulo I, se describe en forma general el planteamiento del problema, donde se hace hincapié que el principal problema es la inseguridad a nivel Nacional como Internacional, es donde nacen los objetivos para la realización de esta tesis, la cual busca en gran manera dar solución a los problemas de inseguridad que existen en la actualidad.

En el Capítulo II, se da una amplia visión de temas de seguridad en los que respecta a entidades bancarias y/o financieras, dando a conocer la documentación necesaria, para poder llevar o realizan un plan de seguridad adecuado a cada agencia realizando sus planes de emergencia, planes de contingencia contra actos antisociales, plan de contingencia en caso de asalto o robos, y plan de acción en caso de desastres naturales.

En el Capítulo III, se aborda el diseño de metodología de la investigación donde se describe que tipo de investigación se usó para el desarrollo de la respectiva tesis, se detalla la ubicación y población implicada en esta investigación.

Capitulo IV, se da a conocer el diseño de Ingeniería que se realizó para los fines de este proyecto, materiales utilizados para las distintas Agencias y/o Oficinas de Caja Rural - Los Andes S.A., métodos por los cuales se corroboran los resultados obtenidos



1 PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACION

1.1 DESCRIPCIÓN DEL PROBLEMA

El problema que se vive actualmente es la inseguridad, siendo una de las principales preocupaciones más importantes a nivel nacional e internacional, por consecuencia el incremento de atentados, bandas organizadas, robos y asaltos, Es de conocimiento público y de interés mundial, todo lo referido a la Seguridad, tanto personal como colectiva en todos los sectores: Residencial, Industrial, Empresarial, Bancos, etc.

1.1.1 FORMULACIÓN DEL PROBLEMA

¿Qué incidencia tiene la implementación de un sistema integral de seguridad con alarmas autónomas y CCTV (Circuito Cerrado de Televisión) para la vigilancia de las agencias de caja Rural Los Andes S.A.?

1.1.2 SISTEMATIZACIÓN DEL PROBLEMA

La implementación de un sistema de seguridad electrónica integrado en los sectores antes referidos es imprescindible, para así poder garantizar la disminución de problemas tales como robos, pérdida de bienes, accidentes y eventualidades en las actividades realizadas por las personas ajenas a la institución y el personal de empresa, así como la optimización del manejo de los recursos humanos en empresas, por ejemplo, protección de la vida de las personas. La propiedad Pública y Privada así como la búsqueda de una organización eficiente en el manejo de una empresa.

Puesto que el área de trabajo de la Caja Rural - Los Andes S.A. es el sector Rural, se nos presenta muchas limitantes tecnológicas y de comunicación en ciertas zonas la cual se busca solucionar adecuando tecnologías conocidas o nuevas para así poder brindar la adecuada seguridad física y electrónica a las respectivas agencias de Caja Rural - Los Andes S.A.

1.2 JUSTIFICACION DEL PROBLEMA

Frente al desmesurado crecimiento de la delincuencia en nuestro medio, la gran mayoría de empresas, instituciones, sitios públicos e inclusive hogares están optando por la adquisición de un sistema de seguridad, para que de alguna manera disminuya el riesgo de sufrir algún hecho delictivo.

La implementación de un sistema de seguridad en una institución como lo es Caja Rural - Los Andes S.A., presentará varios beneficios para esta, puesto que se llevará un mejor control del ingreso y salida del personal de la institución, dando a estos mayores niveles de comodidad, seguridad, ahorro de tiempo y de energía.

La importancia del estudio de la implementación del Sistema de Seguridad, será el diseño del sistema en sí, dimensionando el sistema específicamente en las nuevas Oficinas o Agencias, previa identificación de las zonas sensibles de Caja Rural - Los Andes S.A. como por ejemplo puertas de acceso a las Agencias, Acceso a bóvedas, etc. Utilizando una red de datos o Servidor, se podrá centralizar toda la información, sin dejar de lado la infraestructura existente instalada como son las cámaras de vigilancia y alarmas.

El desarrollo de este proyecto es de gran relevancia ya que promueve la investigación y elaboración de proyectos orientados hacia la seguridad en este

caso orientada a la seguridad bancaria, así mismo busca despertar el interés de los estudiantes por la aplicación de teorías vanguardistas orientadas a la Seguridad, ampliamente usadas en otros campos de la ciencia, lo cual representa un avance en materia tecnológica primeramente para la Universidad y por ende para el País.

Para la Universidad Nacional del Altiplano, concretamente la Escuela Profesional de Ingeniería Electrónica, el proyecto sirve de base para la investigación de nuevas tecnologías, las cuales se pueden continuar desarrollando a futuro y de esta forma ser pioneros en proyectos de implementación y gestión de dispositivos para el área Seguridad.

1.3 OBJETIVOS DE LA INVESTIGACION

Se plantearon los siguientes objetivos a cumplir:

1.3.1 Objetivo General

Proporcionar una solución en el planeamiento de un sistema integral aplicado a la seguridad en las distintas agencias de Caja Rural - Los Andes S.A., utilizando las redes de comunicación.

1.3.2 Objetivos Específicos

- Diseñar de la seguridad de bóveda, con un control dual.
- Obtener una respuesta en tiempo real, de parte del sistema de alarmas y cámaras de la ocurrencia de un evento, es decir lograr disminuir el tiempo de respuesta de los Sistemas de Seguridad.

- Interconectar la red de Agencias de Caja Rural – Los Andes S.A., y así optimizar y crear el Centro de Monitoreo de Alarmas e incidencias.





2 MARCO TEORICO

2.1 ANTECEDENTES DE LA INVESTIGACION

La segunda guerra mundial trajo consigo un acelerado crecimiento de la protección privada debido en parte a la insistencia de los organismos militares, preocupados en proteger las instalaciones que manufacturaban productos bélicos, incluso fue frecuente que personal militar, fuera asignado a cuidar plantas y fabricas estratégicas, por lo que la demanda de contratar personal privado para patrullaje y vigilancia aumenta cada vez.

No es hasta la época de los 60's cuando la seguridad adquirió el realce técnico que hoy tiene y que se enfoca principalmente a sustituir cada vez más al elemento humano a través de equipos electrónicos y procedimientos.

Con este breve resumen histórico se destaca la invaluable e indudable aportación que los guardias han hecho en la evolución del campo de la seguridad, pero también es necesario detenernos a reflexionar que hoy en día no son la solución de todos los problemas que se tienen que enfrentar, más bien, deben considerarse solo como un elemento de la Seguridad Integral que toda organización necesita poseer.

No se cuestiona la importancia que tiene el sistema financiero en el que convergen experiencia, profesionalidad y medios, pero también una diversidad de riesgos, y en algunas ocasiones poca consideración hacia las inversiones en materia de seguridad.

Seguridad es lo que para la mayoría de las personas, representa este tipo de entidades. Cuando un cliente ofrece su dinero o sus bienes a una entidad bancaria para su custodia, espera de ella los máximos valores de seguridad.

Tanto es así que el asalto a bancos es uno de los delitos que mayor repercusión tiene sobre la opinión pública.

La seguridad que representan las entidades financieras está sustentada tanto en tecnologías de seguridad, software y hardware, así como políticas y procedimientos internos.

Por otro lado, en el libro de GOMEZ Manuel, Seguridad en entidades bancarias, E.T. Estudios Técnicos, España 1998. Nos da a conocer una amplia teoría sobre seguridad bancaria en la cual expone entre otras cosas: la mapización de riesgo; análisis de riesgo desde tres puntos de vista (agente causante-sujeto receptor-ámbito o entorno); clasificación general del catálogo de riesgos bancarios; aplicación del Método Mósler para el análisis y evaluación de riesgos bancarios; sistemas de protección e integración y tele gestión aplicados a los bancos; métodos de planificación; planteamiento de las seguridades de prevención y protección en las entidades bancarias; y planes de seguridad. Las cuales son muy importantes para comprender teóricamente sobre Seguridad Bancaria.

2.2 SUSTENTO TEORICO

2.2.1 SEGURIDAD BANCARIA

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

Así, en un siniestro, en principio lo detectará, luego lo señalará, para posteriormente iniciar las acciones encaminadas a disminuir o extinguir los

efectos (Accionando mecanismos de extinción, comunicación con central receptora de alarmas, conectando cameras de video grabación, etc.)

Los sistemas de seguridad pueden ser variables según las necesidades del local a proteger y del presupuesto disponible para ello. En el mercado existe un gran abanico de componentes (centrales, detectores, etc.) con características técnicas y calidades distintas, que hacen que no se pueda tipificar a la hora de la realización de diseños de los sistemas de seguridad.

2.2.1.1 Tipos de Seguridad

En el ámbito de Seguridad Bancaria abarca una serie de seguridades entre las que destaca:

- **SEGURIDAD BÁSICA:** Constituida principalmente por los planteamientos arquitectónicos (cerramientos y elementos constructivos), los medios de protección física y mecánica (blindajes, cajas fuertes, cerraduras, cámaras acorazadas, etc.) y los medios de prevención y protección activa o electrónica (sistemas de detección, control, registro, etc.)
- **SEGURIDAD OPERATIVA Y FUNCIONAL:** Constituida por los procesos administrativos y de control de riesgos, informaciones y datos confidenciales, formación y capacitación del personal, control de accesos y circulación de personas, control de las instalaciones de gestión y seguridad.

- **SEGURIDAD INFORMÁTICA:** Constituida por los sistemas de protección de la información, control de las comunicaciones, transmisión de datos, control y protección de los procesos operativos.
- **SEGURIDAD ESPECIAL:** Constituida por los sistemas y operativos especiales correspondientes para la protección de personas, de informaciones y valores específicos, así como por los dispositivos necesarios ante situaciones de riesgo o amenaza no habituales (agresiones terroristas, amenaza de bomba, catástrofes, etc.)

Lo cual es muy acertado ya que la Seguridad Bancaria es muy compleja todas las sub partes que existen en sistemas de seguridad que abarca: Seguridad física, seguridad electrónica, seguridad de la información e informática, seguridad y salud en el trabajo, seguridad transporte de valores, etc.

2.2.1.2 Catálogo de Riesgos

Todo esto obedece a que las Instituciones Financieras tienen un catálogo de Riesgos constituidos por los siguientes:

- **Riesgos Naturales:** Inundaciones, tormentas eléctricas, seísmos, etc.
- **Riesgos Tecnológicos:** Si se tiene la facilidad para interconectarse.
- **Riesgos Técnicos:** Diseño y fabricación, construcción o montaje, conservación, control de mantenimiento, averías de instalación, etc.
- **Riesgos Antisociales:** Robo, atraco, hurto, secuestro, sabotaje, fraude, estafa, vandalismo, amenaza de bomba, incendio provocado, falsificación de cheques o moneda, terrorismo etc.

- **Riesgos Sociales y Laborales:** Accidentes de trabajo, golpes, caídas, explosión fortuita, etc.

Ante este contexto, las entidades Bancarias y Financieras deben contar con un Plan de Seguridad para gestionar el catálogo de riesgos arriba expuesto que aquejan a la actividad financiera. Dicho plan contiene varios planes en los cuales en términos generales se realiza la identificación, análisis y evaluación de los riesgos que atentan contra la actividad bancaria, así como la determinación de los recursos a utilizar para proteger a la institución, y finalmente se establece manuales y procedimientos. Toda esta información es necesario agrupar en un solo documento para establecer el Plan Integral de Seguridad.

El Plan Integral de Seguridad es el documento por el que se rigen todos los planes de seguridad de una empresa, organismo o instalación. Tiene por objeto coordinar los esfuerzos, asignar responsabilidades y cometidos, así como determinar los recursos humanos y materiales necesarios para la elaboración, desarrollo e implantación de los diversos planes de seguridad, a fin de hacer frente a los riesgos y amenazas que afecten a las diferentes áreas que conforman una entidad bancaria.



Figura N° 1: Pirámide de Seguridad Integral
Fuente: Seguridad Bancaria
Elaborado: Por José Reyes

2.2.1.3 Documentación en Seguridad Bancaria

Podemos establecer que el Plan Integral de Seguridad Bancaria está compuesto por diferentes documentos para su respectiva gestión y estos están gobernados por los siguientes planes de Seguridad y estas a su vez se resumen en la figura N° 2.

- a) **Plan de Seguridad Contra Actos Antisociales:** Es un documento elaborado con la finalidad de establecer las medidas de intervención y reacción, para la protección de las personas y bienes contra los riesgos antisociales.
- b) **Plan de Prevención de Riesgos Laborales:** Es un documento en el cual recoge las “medidas y el desarrollo de las actividades necesarias para la prevención de riesgos derivados del trabajo”, logrando así promover la Seguridad y Salud de los trabajadores.
- c) **Plan de Mantenimiento:** Es un documento que establece las actividades de mantenimiento de los equipos y sistemas de seguridad implementados, con la finalidad de garantizar el funcionamiento y operatividad de los mismos en todo momento, para que puedan cumplir su función preventiva y protectora al 100%.
- d) **Plan de Protección AVP:** Es un documento que establece responsabilidades y cometidos al personal de seguridad así como también los medios a utilizar con la finalidad de proteger y salvaguardar la integridad y vida de personas muy importantes de las entidades bancarias.

- e) **Plan de Emergencia:** Es un documento que determina los recursos para la prevención y protección contra incendios, robos y asaltos, así como también las responsabilidades y procedimientos para la evacuación y la intervención inmediata frente a siniestros o desastres naturales.
- f) **Plan de Protección de la Información:** Es un documento en el cual establece las acciones y medidas a tomar para conservar la integridad, confidencialidad y disponibilidad de la información que maneja la institución.

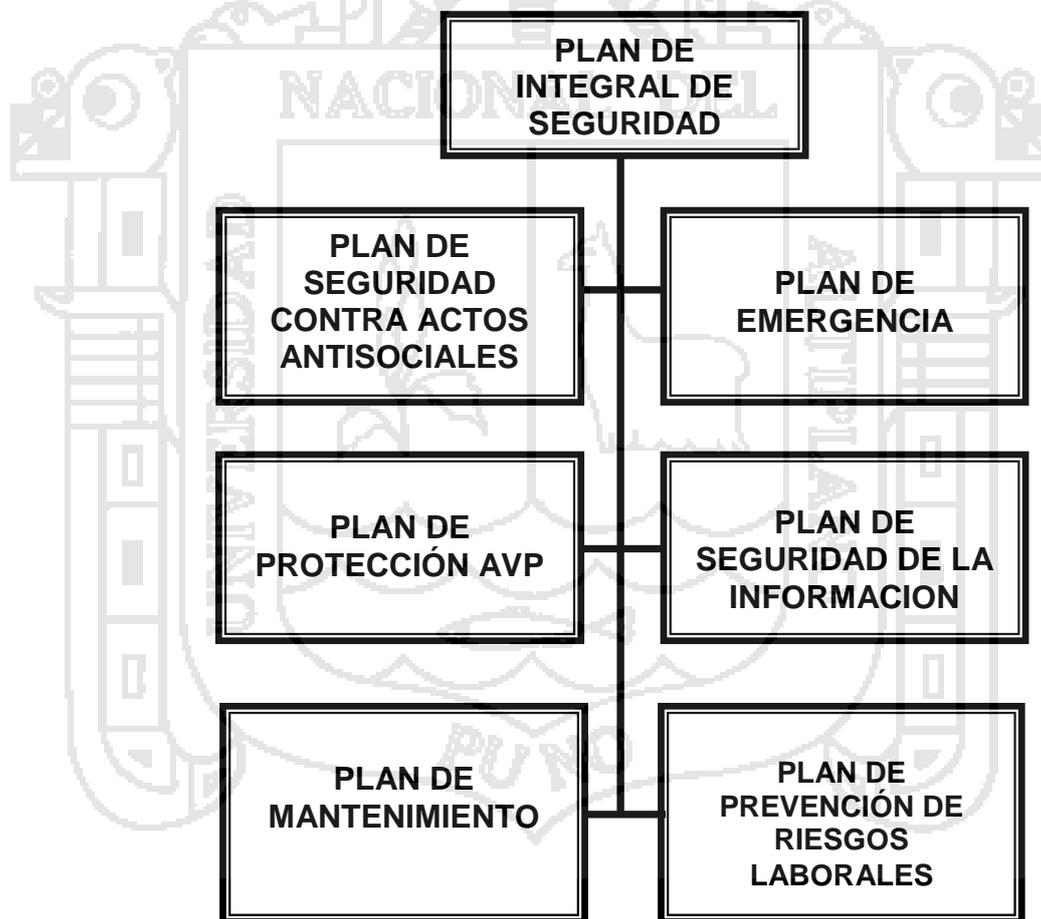


Figura Nº 2: Resumen Plan Integral de Seguridad
Fuente: Seguridad Bancaria - José Reyes
Elaborado: Por los Investigadores

2.2.2 PLANES DE EMERGENCIA

El objetivo fundamental de los planes de Emergencia elaborados para Caja Rural - Los Andes S.A., están basados el cumplimiento de los siguientes criterios:

- Evaluar, analizar y prevenir los riesgos en nuestro establecimiento.
- Evitar o mitigar las lesiones que las emergencias puedan ocasionar a nuestro personal y a terceros.
- Capacitar permanentemente a todo nuestro personal en prevención de riesgos y entrenamientos en acciones de respuestas ante situaciones de emergencias.
- Contar con los procedimientos a seguir durante las operaciones de respuestas a la contingencia.

2.2.2.1 Base Legal:

- Decreto Legislativo N° 735 – Ley del Sistema de Defensa Civil.
- D.S. N° 066-2007-PCM Reglamento de Inspecciones Técnicas en Seguridad de Defensa Civil.
- Ley N° 28976, Ley Marco de Licencia de Funcionamiento.
- Ley N° 29783, Ley de Seguridad y Salud en el Trabajo.
- Circular SBS N° G-139 “Gestión de la Continuidad del Negocio”.
- Circular SBS N° G-164 “Reporte de eventos de interrupción significativa de operaciones”.

2.2.3 PLAN DE SEGURIDAD CONTRA ACTOS ANTISOCIALES

Para desarrollar el Plan de Seguridad Contra Actos Antisociales se establece que dicho plan debe contener los siguientes epígrafes: Análisis de Riesgos y Amenazas; Medios de Protección; y Manual de Procedimientos. A esta estructura como se puede ver en la Figura N° 3, le aumentamos el epígrafe de objetivo y en la parte de los medios de protección nos basamos en el establecimiento de la seguridad integral, ante lo cual en dicho epígrafe constara los recursos humanos, técnicos y organizativos. Adicional se contempla el costo de implementación de los medios de protección.

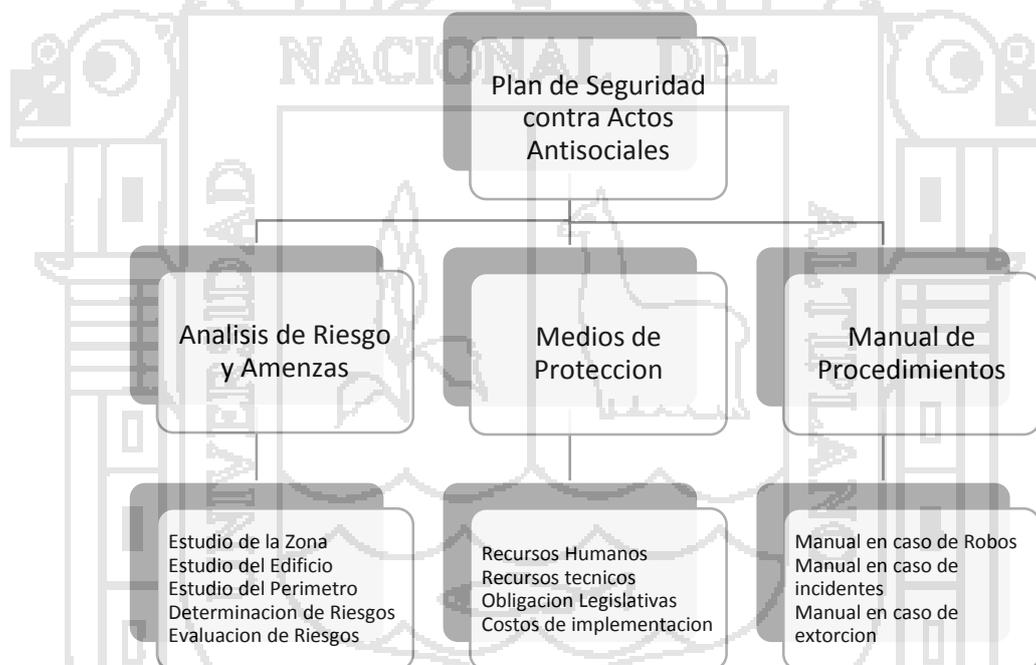


Figura N° 3: Plan contra actos Antisociales
Fuente: Seguridad Bancaria - José Reyes
Elaborado: Por los Investigadores

2.2.3.1 Análisis y Evaluación De Riesgos

En este epígrafe se da a conocer el catálogo de riesgos que atenta contra la institución financiera, determinando los riesgos reales y potenciales a

través del estudio del entorno, instalación, perímetros, etc., que den a resaltar las amenazas y vulnerabilidades para determinar los riesgos y evaluarlos.

El análisis de cualquier caso de seguridad y sean cuales fueren sus dimensiones o complejidad surge, inevitablemente, la necesidad de afrontar el estudio de unos factores como elementos básicos cuyo desarrollo concreto nos conducirá siempre a una solución eficiente. Este estudio resulta ser una ardua tarea que requiere el desarrollo de diversos análisis parciales, interrelacionados donde las conclusiones de una parte del trabajo constituyen las premisas del siguiente apartado. En consecuencia, resulta imprescindible la aplicación de una metodología o procedimiento de análisis que garantice la solución total del problema y el rigor profesional del estudio, ya que la ausencia frecuente de ese estudio de seguridad, su elaboración incompleta o la falta de un método que sistematice el trabajo se traduce, generalmente, en la aplicación de soluciones erróneas o defectuosas.

Ante esto, el estudio se inicia con una tarea previa, denominada trabajo de campo, que consiste en la recopilación ordenada y sistemática de cuanta información pueda ser necesaria para los análisis posteriores.

Entre los principales son:

- **Análisis del entorno:** Analiza las condiciones socioeconómicas del entorno donde está situado el edificio o agencia bancaria. Destacando: entorno sociocultural, nivel de delincuencia, y emplazamiento urbano, en la periferia o en pequeñas poblaciones.

Emplazamiento del local sede de la agencia bancaria o edificio singular: se describe el conjunto arquitectónico en donde está emplazado el edificio o agencia bancaria destacando: características específicas del

edificio; número de edificios o locales que le son colindantes; año de edificaciones y remodelaciones; superficie de los locales; canalizaciones generales de telefonía, agua, conducciones eléctricas, alcantarillado; superficies colindantes subterráneas, sótanos, garajes, aparcamientos, metropolitano, y grado de seguridad de los elementos constructivos.

- **Catálogo de riesgos antisociales:** Se realiza la descripción cualitativa y cuantitativa de los riesgos de carácter antisocial que afecta a cada uno de los locales, detallando desde los métodos de falsificación hasta el análisis de la casuística de los procedimientos utilizados en los diferentes atracos y robos por butrón realizados en los últimos años.

Cabe indicar que cualquier metodología de seguridad puede ser válida siempre y cuando asegure el tratamiento minucioso y coordinado del objeto, las amenazas, el espacio y el tiempo, así como una respuesta de los medios que resuelva todas las vulnerabilidades existentes.

Con estos estudios se tiene la información necesaria para realizar el análisis y evaluación de riesgos aplicando un método para la respectiva valoración y ponderación de los factores de riesgo detectados, para lo cual existen varios métodos de valoración, entre ellos está el METODO MOSLER que es el más adecuado utilizar ya que el método tiene una gran ventaja y es que este califica con objetividad, por tal motivo no hay que temer a sobre pasarse ya que los resultados de estas, casi siempre resultan bajas, en comparación con la apreciación aparente de los riesgos. Con esto elimina los aspectos negativos del método. Adicional con la ayuda de la utilización de sub criterios ayuda para un mejor análisis y evaluación de los riesgos.

El método Mósler tiene como objeto la identificación, análisis y evaluación de los factores que pueden influir en la manifestación y materialización de un riesgo, con la finalidad de calcular la clase y dimensión del riesgo para su tratamiento. Este método es secuencial ya que el desarrollo de sus fases se fundamenta en los datos y resultados de las fases precedentes. Son cuatro fases en las que se desarrolla este método:

1. Definición del riesgo.
2. Análisis del riesgo.
3. Evaluación del riesgo.
4. Cálculo de la clase de riesgo

2.2.3.2 Medios de Protección

Una vez realizado el análisis y evaluación de riesgos es pertinente establecer los recursos o medios de seguridad a utilizar para minimizar los riesgos. Para lo cual se debe establecer un sistema de seguridad integral.

La seguridad integral está constituida por tres tipos de medios que deben aunarse como partes integrantes de un todo.

- Medios Humanos: constituidos por el personal de seguridad, tanto Pública, Institucional y/o Privada.
- Medios Técnicos: pasivos o físicos; activos o electrónicos.
- Medios Organizativos: planes, normas, estrategias.

Estos tres recursos deben ser manejados conjuntamente, para alcanzar una sinergia entre estos elementos, para tener como resultado un Sistema de

Seguridad eficiente y eficaz al servicio de las personas y bienes que engloban las entidades bancarias.

En base a esto los recursos o medios de seguridad a utilizar en las instituciones financieras son:

- **Recursos Humanos:** Conforman todas las personas que trabajan en el área de seguridad bajo relación de dependencia y/o servicios prestados (Jefe de Seguridad, Supervisores, Guardias, etc.)
- **Recursos Técnicos:** Está conformado por los sistemas y tecnologías de seguridad, los cuales se dividen en:
 - **Sistemas de protección pasiva:** Son aquellos materiales, equipos y sistemas de seguridad de carácter físico o mecánico que se emplean, desde un punto de vista pasivo, para la prevención y protección ante los riesgos en las entidades bancarias.
 - **Sistemas de protección activa:** Son aquellos equipos y sistemas de seguridad de carácter electrónico e informático que se emplean específicamente, desde un punto de vista activo, para la prevención y la protección ante los riesgos y amenazas que configuran el catálogo de aplicación a las entidades bancarias.

SISTEMAS DE PROTECCIÓN PASIVA	SISTEMAS DE PROTECCION ACTIVA
Bóveda	Control de Acceso
Puerta de Bóveda	Sistema de Alarma
Caja fuerte	Sistema de CCTV
Archivadores de seguridad	
Blindaje	

Tabla N° 1: Clasificación de los medios de protección
Fuente: Seguridad Bancaria - José Reyes
Elaborado: Por los investigadores

2.2.3.3 Manual de Procedimientos

Aquí se detalla las actuaciones ante agresiones antisociales entre las más importantes y por su frecuencia en la actividad bancaria se debe establecer las actuaciones en caso de: asalto, robo, amenaza de bomba, secuestro y extorción. Definiendo las actuaciones y responsabilidades en el antes durante y después de cada agresión antisocial.

2.2.4 PLAN DE SEGURIDAD PARA TRANSPORTE DE VALORES

El transporte de valores es un servicio que consiste en trasladar de un lugar a otro los valores consignados, para lo cual quien realiza dicho servicio asume la responsabilidad de custodia y traslado de dichos valores. Es decir, quien presta el servicio asume los riesgos y amenazas que aquejan a esta actividad, para lo cual se debe desarrollar un plan de seguridad de transporte de valores para garantizar un servicio ordenado, seguro y confiable.

El servicio del transporte de valores es de alto riesgo, ya que los delincuentes han volcado su mirada, en los últimos tiempos, a esta actividad debido a varios factores, entre los principales tenemos:

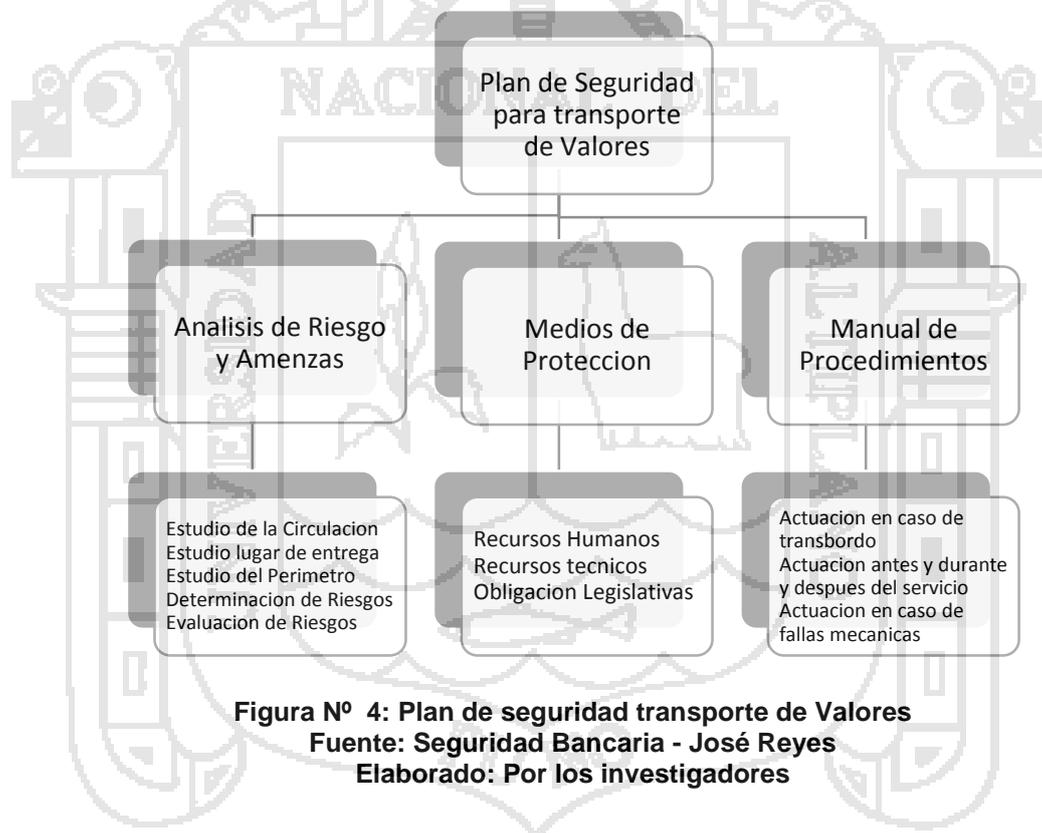
- El botín a conseguir es elevado.
- Pueden escoger el lugar y el momento adecuado para realizar el asalto.
- Facilidad de observación sin acarrear sospechas y planeamiento anticipado.
- Sorpresa en la acción, sin riesgo de accionar un sistema de alarmas.

En los últimos años se han dado varios casos de asaltos a los vehículos blindados, dejando en algunos casos como saldo la pérdida de vidas humanas. Con lo cual se evidencia el riesgo elevado que abarca realizar la actividad del

transporte de valores, ante esto es importante desarrollar un plan de seguridad para el transporte de valores.

Para desarrollar un Plan de Seguridad para Transporte de Valores tomaremos como referencia la estructura para elaborar un Plan de Seguridad Contra Actos Antisociales y la adaptaremos para el transporte de valores considerando los tres epígrafes que contempla el plan:

- 1) Análisis de Riesgos y Amenazas.
- 2) Medios de Protección.
- 3) Manuales de Procedimientos.



2.2.4.1 Análisis y Evaluación De Riesgos

En este epígrafe se da a conocer el catálogo de riesgos que atenta contra el transporte de valores, determinando los riesgos reales y potenciales a través del estudio de:

- Perímetro: considera si es urbana, rural, etc.
- Circulación: considera si hay alta, baja, etc., circulación vehicular y peatonal.
- Acceso vehicular: considera el tipo de acceso que existe en el lugar donde se realizara el servicio (vías asfaltadas, pavimentadas, dañadas, parqueadero, etc.)
- Vigilancia: Considera si en el lugar existe vigilantes y/o policías cercanos.
- Iluminación: Considera la claridad por donde circula el vehículo, donde se estaciona y por donde recorre el custodio.
- Acceso custodio: considera la distancia que tiene que recorrer el custodio desde que se baja del blindado hasta el sitio donde se realiza la entrega recepción y si el trayecto es a vista del público, restringido, etc.
- Peligrosidad: Considera la peligrosidad del sector tomando en cuenta los hechos presentados de inseguridad.

Para desarrollar el análisis y evaluación de riesgos se puede utilizar varios métodos existentes, la ventaja de utilizar sub criterios con el fin de cuantificar más objetivamente, y a través de los sub criterios se pueden plasmar los factores de riesgo.

2.2.4.2 Medios de Protección

Una vez realizado el análisis y evaluación de riesgos es pertinente establecer los recursos o medios de seguridad a utilizar para minimizar los riesgos.

a) Recurso Humano

El personal mínimo que realiza el transporte de valores es:

- Vigilante de Seguridad Conductor: entre sus funciones esta conducir y velar por el buen funcionamiento del vehículo blindado tanto a nivel mecánico como los dispositivos de seguridad.
- Vigilante de Seguridad Porteador: tiene como principal función la entrega y recepción de valores, verificando que la documentación y valijas estén correctos.
- Vigilante de Seguridad de protección: su principal función es proteger al vigilante porteador en sus desplazamientos de operación así como también al blindado.

b) Recurso Técnico:

Los principales recursos técnicos en el transporte de valores son: vehículo blindado y su equipamiento, armamento y medios de protección del personal como chalecos y cascos antibalas, máscaras anti gases, etc.

El vehículo blindado, está dividido en tres compartimientos. El compartimiento delantero es en el cual va únicamente el conductor. En el central van los vigilantes de seguridad, y en el posterior es destinado para transportar los valores.

Cada compartimiento está separado por una mampara blindada, y las puertas del segundo compartimiento con la tercera serán escluidas para que no puedan abrir mientras la puerta del tercer compartimiento, que da a la parte de carga de valores, este cerrada. Adicional para la apertura de la puerta de zona de carga de valores estará dotada de una cerradura temporizada.

2.2.4.3 Manuales de Procedimientos

En este epígrafe se detalla las actuaciones antes, durante y después del servicio de transporte de valores, así como también ante agresiones antisociales y casos emergentes, entre los más importantes y por su frecuencia en la actividad de transporte de valores se debe establecer las actuaciones en caso de: asalto, accidente de tránsito, daño mecánico, transbordo.

Hay una medida que es común para las tres fases, que es sumamente importante, y que es la observación atenta y permanente a todo lo que sucede. Así, se observara para saber si alguien nos vigila y hace esperas al vehículo blindado a las salidas, en el recorrido o a la entrada en la base, en las cargas y descargas, etc., tomando nota de matrículas y personas sospechosas.

2.2.5 SISTEMAS DE PROTECCIÓN ACTIVA

2.2.5.1 Circuito Cerrado de Televisión

Un circuito cerrado de televisión (CCTV) se diferencia con los medios de difusión de video pública porque todos sus componentes están enlazados y se enfoca en un número limitado de espectadores. El circuito puede estar compuesto, por una o más cámaras de vigilancia conectadas a uno o más monitores o televisores, que reproducen las imágenes capturadas por las cámaras. Aunque, para mejorar el sistema, se suelen conectar directamente o enlazar por red otros componentes como controladores especializados y computadoras.

El sistema de video-vigilancia funciona a través de la instalación de un conjunto de cámaras ubicadas en lugares estratégicos y empleando un

dispositivo de grabación de imágenes, es posible disponer de un sistema de CCTV de las zonas comunes de la edificación cuya complejidad varía en función del número de cámaras a instalar. Los sistemas actuales de gestión de seguridad han evolucionado hacia el telecontrol. Las soluciones de telecontrol actuales se estructuran en cuatro elementos básicos: las cámaras, el servidor de captura, almacenamiento y transmisión, la red de comunicación y el equipo receptor y de control. Estos conceptos se describen a continuación.



Figura Nº 5: Esquema de un CCTV
Fuente: Diseño e Instalación de Sistemas de CCTV
Elaborado: Por José María Merchán

Las cámaras no varían en exceso de las empleadas tradicionalmente (fijas o motorizadas), excepto en que reducen su tamaño y potencia. En blanco y negro o en color, pueden ubicarse en interiores, escaleras, rellanos, sótanos y exteriores como fachadas, calles contiguas, y son absolutamente orientables desde el equipo de control. Su función es captar las imágenes y transmitir las al servidor de captura.

Una vez almacenadas las imágenes, éstas son transmitidas como datos hacia un receptor ubicado todo lo lejos que se desee, pues es posible emplear

cualquier tipo de red de comunicación. La telefonía básica PSTN y la red vía ADSL con protocolos TCP/IP, son las redes más empleadas por su relación prestaciones-precio. Sin embargo pueden utilizarse con una inversión algo más elevada enlaces por fibra óptica, microondas e incluso satélite como se muestra en la figura N° 6.

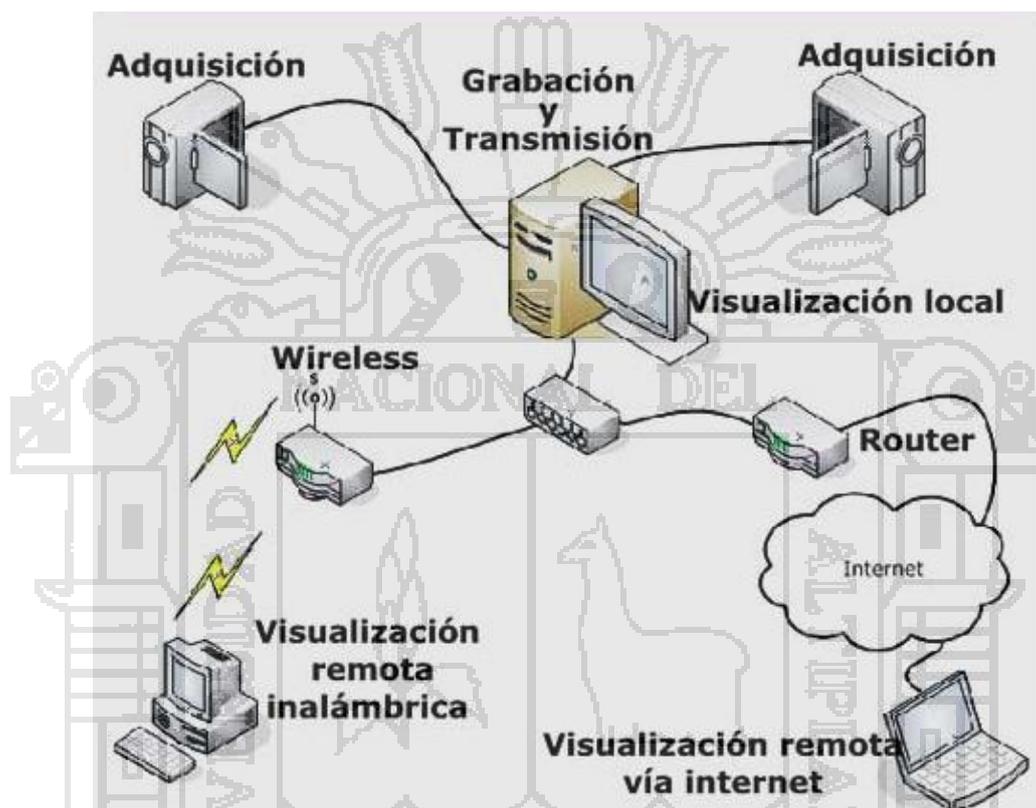


Figura N° 6: Interconexión de un CCTV
Fuente: Diseño e Instalación de Sistemas de CCTV
Elaborado: Por José María Merchán

El último eslabón de la cadena lo conforma el equipo receptor. Éste se compone de un ordenador personal y de un Router o equipo de adaptación a la red de comunicaciones que haya sido elegida. A través de éste el encargado de monitoreo podrá visualizar en tiempo real, aspecto destacable del sistema, lo que suceda en las instalaciones donde se encuentra el equipo. Y todo ello mediante un software adecuado y un navegador web como el Internet Explorer, y un sistema de claves que una vez introducidas, permiten tener una visión global de todas las cámaras o de una sola, orientarlas, hacer zoom en una de ellas o

poner en reposo el equipo hasta que un sensor ubicado en las mismas detecte algún tipo de movimiento.

2.2.5.1.1 Formatos de Video

La señal de vídeo está formada por un número de líneas agrupadas en varios cuadros y estos a la vez divididos en dos campos que portan la información de luz y color de la imagen. El número de líneas, de cuadros y la forma de portar la información del color depende del estándar de televisión concreto. La amplitud de la señal de vídeo es de 1Vpp (1 voltio de pico a pico) estando la parte de la señal que porta la información de la imagen por encima de 0V y la de sincronismos por debajo el nivel de 0V. La parte positiva puede llegar hasta 0,7V para el nivel de blanco, correspondiendo a 0V el negro y los sincronismos son pulsos que llegan hasta -0,3V.

La señal de vídeo consta de la luminancia (que es el componente de la señal de vídeo que contiene las informaciones de la luz o brillo), la crominancia (es el componente de la señal de vídeo que contiene las informaciones del color) y de los sincronismos (indican donde comienza y acaba cada línea de las que se compone la imagen de video). La amplitud se sitúa entre los -0,3 V del nivel inferior del sincronismo hasta los 0,7 V que corresponde al blanco. La frecuencia de los pulsos de sincronismo depende del sistema de televisión: en América (con excepción de Argentina y Uruguay, que siguen la norma europea) se usa frecuencia de línea (número de líneas) de 525 líneas por cuadro (y 60 campos por segundo), mientras que en Europa se utilizan 625 líneas por cuadro (312,5 por cada uno de los dos campos en la exploración entrelazada), a una frecuencia de 15.625 Hz, y 50 campos por segundo, (25 cuadros).

El ancho de banda de la señal de luminancia suele ser del orden de 5 MHz, pero depende del sistema empleado. La crominancia es una señal modulada en cuadratura (es decir en amplitud y en fase). A la portadora se la denomina “subportadora de color” y es una frecuencia próxima a la parte alta de la banda; evidentemente, esta frecuencia tiene relación con el resto de frecuencias fundamentales de la señal de vídeo que están referenciadas a la frecuencia de campo que toma como base (frecuencia de la red de suministro eléctrico), 50 Hz en Europa y 60 Hz en muchas partes de América.

En lo referente al color, en todos los estándares se modula una portadora con la información del color. En NTSC y PAL lo que se hace es una modulación en amplitud para la saturación, y en fase para el tinte, lo que se llama «modulación en cuadratura». El sistema PAL alterna la fase de la portadora 180° en cada línea, para compensar distorsiones de la transmisión. El sistema SECAM modula cada componente del color en las respectivas líneas.

- a. **Formato PAL:** El formato PAL/SECAM (Phase Alternating Line/Sequential Colour with Memory), permite la codificación de videos en 625 filas de las cuales sólo se muestran 576 porque las restantes se utilizan para sincronización, a una frecuencia de 25 imágenes por segundo con un formato 4:3, es decir, con una proporción 4/3 de ancho/altura.

No obstante, a 25 imágenes por segundo, muchas personas perciben cierta intermitencia en la imagen. Por lo tanto, como no es posible enviar más información debido a las limitaciones del ancho de banda, las imágenes se entrelazan, es decir, se envían las filas pares en primer lugar y

después las filas impares. El término "campo" indica la "media imagen" formada por las filas pares o las filas impares. La transmisión completa que comprende los dos campos se llama pantalla entrelazada. Cuando no hay entrelazado, se utiliza el término pantalla progresiva.

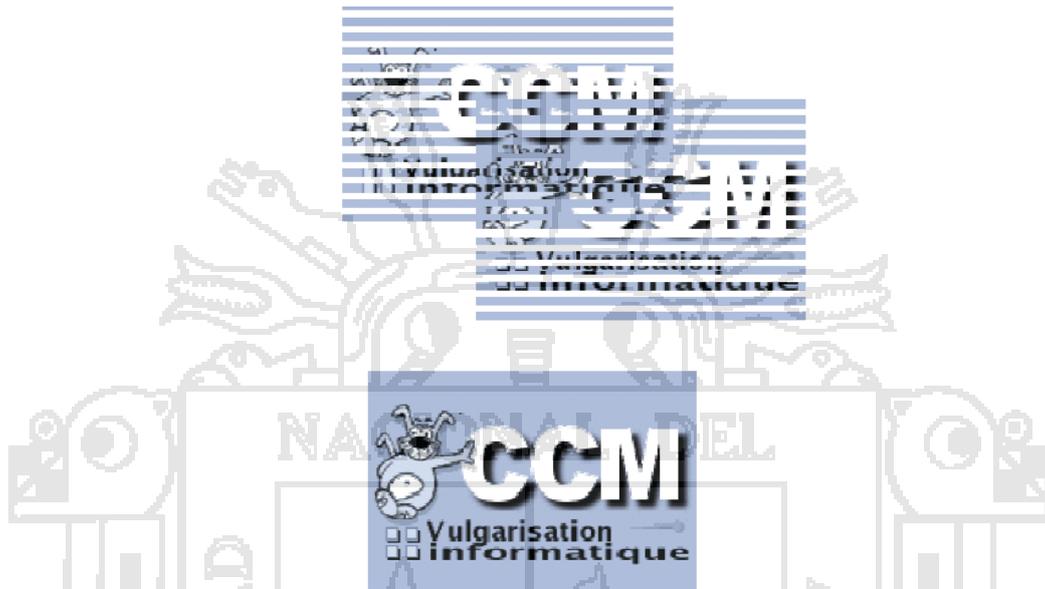


Figura N° 7: Imagen formato PAL
Fuente: Diseño e Instalación de Sistemas de CCTV
Elaborado: Por José María Merchán

Gracias a este procedimiento llamado "entrelazado", un televisor PAL/SECAM muestra 50 campos por segundo (es decir, a una frecuencia de 50 Hz), lo que significa 2 x 25 imágenes en dos segundos.

- b. Formato NTSC:** La norma NTSC (National Television Standards Committee), utiliza un sistema de 525 filas entrelazadas a 30 imágenes por segundo (es decir, a una frecuencia de 60 Hz). Como en el caso de la norma PAL/SECAM, el 8% de las filas se utiliza para sincronizar el receptor. De esta manera, dado que la norma NTSC muestra un formato de imagen de 4:3, la resolución que se muestra en realidad es de 640 x 480 líneas. La fluidez de un video se caracteriza por el número de imágenes por segundo (frecuencia

de cuadros), expresado en FPS (cuadros por segundo). El estándar PAL/SECAM especifica 25 FPS, mientras que el NTSC especifica 29,97 FPS.

- c. Video digital:** El video digital consiste en mostrar una sucesión de imágenes digitales a una frecuencia determinada, especificando así el número de bytes mostrados o transferidos por unidad de tiempo. De esta manera, la frecuencia necesaria para mostrar un video (en bytes por segundo) equivale al tamaño de la imagen multiplicado por el número de imágenes por segundo. Entre los formatos de video digital utilizados están el JPEG y el MPEG.

El formato JPEG es un algoritmo diseñado para comprimir imágenes fijas con 24 bits de profundidad o en escala de grises. La compresión es con pérdida de calidad, por lo tanto al descomprimir la imagen no es la misma; igualmente (dependiendo del grado de compresión) la calidad es aceptable. Está especialmente diseñado para comprimir fotografías, pues en gráficos, la pérdida de calidad se hace evidente. Los ficheros que utilizan esta compresión llevan la extensión .jpe o .jpg.

El formato MPEG utiliza algoritmos que comprimen la información en pequeños paquetes a una alta tasa de compresión almacenando solamente los cambios de un frame al siguiente, en vez de almacenar el frame entero. La información del video se codifica entonces usando una técnica llamada Discrete Cosine Transform (DCT)

2.2.5.1.2 Componentes de un sistema de CCTV

El C.C.T.V. permite realizar identificaciones durante o después del suceso que está visualizando. Por eso es muy importante definir qué función van a cumplir y donde serán colocadas las cámaras.

Las características principales de las cámaras son: la sensibilidad en relación a la cantidad real de luz visible o infrarroja necesaria para producir una imagen de calidad, la resolución en relación a la calidad de imagen y las características especiales de cada cámara para ajustarse a distintos medios.

Para diseñar un CCTV se deben tomar en cuenta los siguientes pasos:

- 1) Determinar el propósito del sistema de C.C.T.V.
- 2) Definir las áreas que cada cámara visualizará.
- 3) Elegir la cámara cuyas características se adapten de mejor manera al medio.
- 4) Determinar donde se localizará el monitor o monitores para visualizar el sistema.
- 5) Determinar el mejor método para transmitir la señal de vídeo de la cámara al monitor.
- 6) Determinar el área de ubicación del control.

Un sistema de video vigilancia se utiliza para la detección de sospechosos, la seguridad del personal, monitorear y llevar un registro de lo ocurrido, procesos industriales, prevención de algún robo, etc.

Dependiendo de la calidad y sofisticación del sistema se pueden tener un gran número de elementos que lo componen, pero en general los principales son los siguientes:

- a. Cámaras.
- b. Medio de Comunicación.
- c. Grabador.
- d. Monitoreo.

2.2.5.1.3 Características de las Cámaras

Las cámaras son el medio con el cual se capturara las imágenes, estas deben ser ubicadas de acuerdo al área que se requiere tomar, se tiene que tener en cuenta las condiciones climatológicas del lugar, luz en el área, el lugar en el que se colocara.

Las cámaras de una manera simple se pueden clasificar de la siguiente manera:

- **Cámaras Móviles:** Son cámaras que permiten movimientos del lente ya sea de forma manual o programada así enfocara diferente lugares, pueden tener movimientos derecha e izquierda dependiendo el modelo serán los grados que permita este movimiento hasta los 360° (Pan), es el movimiento arriba abajo, también depende el modelo de cámara los grados de libertad que tenga este movimiento y va hasta los 180° (Tilt) y también podremos acercar o alejar la imagen. (Maureen, 1995)
- **Cámaras Fijas:** Estas cámaras tendrán una toma única en la que se dejara enfocada la cámara, las hay ya con lentes incluidos fijos o con lentes que uno puede escoger de acuerdo al enfoque que se requiere tener. Las hay de domo, habitualmente para techos o plafón, y de bala habitualmente para exteriores.

- **Cámaras Analógicas:** Mediante esta tecnología se envía el video o imágenes de video capturas a través de cable RG-59 habitualmente.
- **Cámaras IP:** Esta tecnología de comunicación permite a las cámaras trabajar bajo el protocolo TCP/IP directamente desde la cámara, estas ya tienen la entrada Ethernet y una vez estando en red es posible darle salida a internet a la cámara directamente.
- **Cámaras Interiores:** Son cámaras que únicamente pueden ser instaladas en interiores, ya que no soportan condiciones de lluvia o sol.
- **Cámaras Exteriores:** Estas cámaras son para ser colocadas en exteriores, no les afecta la lluvia, el sol, el viento.
- **Cámaras IR:** son cámaras sensibles a la luz infrarroja esto es para poder tener imagen de noche con esta luz.

Dentro de las características de las Cámaras se puede mencionar las más resaltantes y estas son:

1. **CCD “Charged Coupled Device”:**

En español “dispositivo de carga acoplada” Este dispositivo sólido fotosensible es el encargado de recoger las imágenes en forma de luz, descomponiéndola en colores primarios Rojo, Verde y Azul para luego formar la imagen que será mostrada en el medio de visualización utilizado; posee alta sensibilidad de IR y bajo costo de producción.

2. **Formato de Cámaras:**

El formato de una cámara está determinado por el tamaño del CCD; por ejemplo una cámara de formato de CCD de 1/3 de pulgada, se refiere

a la medida en forma diagonal en el elemento sensor y dependiendo del tamaño de éste se define el formato de la cámara como se muestra en la Figura N° 8.

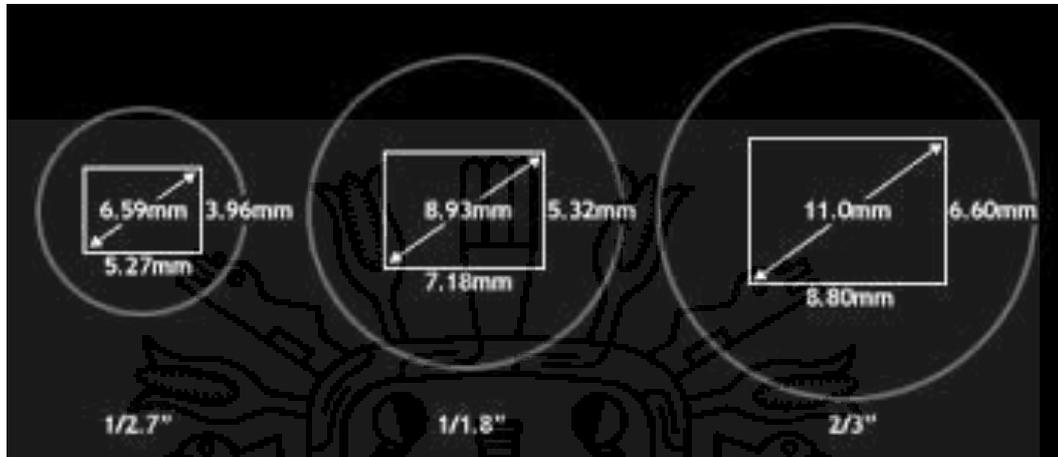


Figura N° 8: Formato de Cámaras
Fuente: Diseño e Instalación de Sistemas de CCTV
Elaborado: Por José María Merchán

3. Lux Rating:

Esta característica determina la cantidad mínima de luz que la cámara requiere para producir una señal de video con buena calidad. A menor Lux menor iluminación requerida. Esta medida viene dada en Lúmenes en las características de cada cámara.

4. Resolución:

Se refiere a la calidad de la imagen, en función de líneas de televisión y se detalla en la tabla N° 2.

Cámaras Analógicas	Resolución
QCIF	176 x 144
CIF	352 x 288
2CIF	704 x 288
DCIF	528 x 384
4CIF	704 x 576
D1	720 x 480

Tabla N° 2: Resolución de Cámaras Analógicas
Fuente: Diseño e Instalación de Sistemas de CCTV
Elaborado: Por los Investigadores

5. Auto iris incorporado:

Algunas cámaras de alta calidad usan el sensor de imagen CCD, para realizar un control automático del iris interno.

2.2.5.1.3.1 Lentes

Se requieren las distancias del objeto a la cámara así como lo alto y lo ancho de la toma que se requiere para poder definir el lente apropiado. Los hay fijos, con una sola medida de lente para enfocar y varifocales tendrá un rango de foco para poder ajustar así como el grado de apertura puede ir hasta los 180°

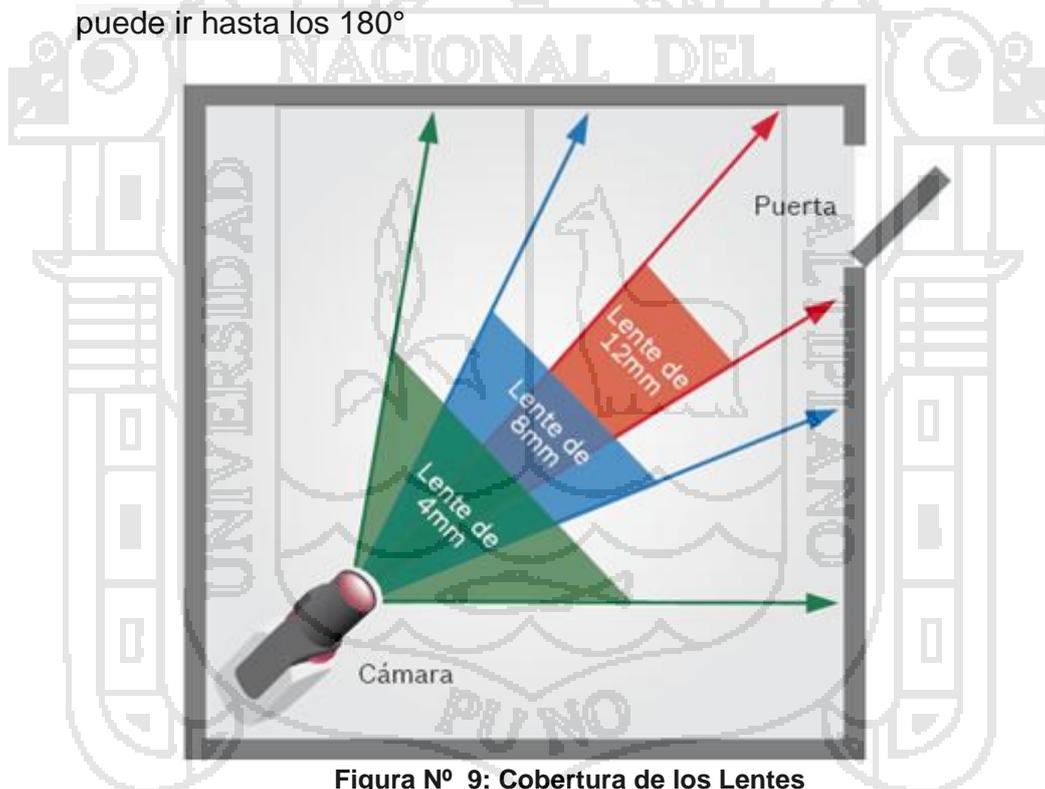


Figura N° 9: Cobertura de los Lentes
Fuente: Diseño e Instalación de Sistemas de CCTV
Elaborado: Por José María Merchán

Las características de los lentes de las cámaras son las siguientes:

- Longitud Focal.
- Foco o enfoque.
- Iris.

- Formato de lentes.

En función de estas características se selecciona el lente individualmente o todo el conjunto con el cuerpo funcional de la cámara.

1. Longitud Focal, Zoom in y Zoom out:

Es la distancia que existe entre el CCD de la cámara y el primer cristal del lente y dependiendo de la distancia se califican los lentes. Por ejemplo a menos milímetros más campo de visión (Zoom out). A más milímetros menos ángulo de visión pero más distancia (Zoom in).

2. Focus o enfoque:

Cuando se realiza el enfoque de una imagen, se requiere de un ajuste para obtener una señal clara entre la distancia de enfoque y la apertura del iris.

3. Iris:

El iris es un dispositivo mecánico controlado manualmente, o electrónicamente a través de la cámara o controlador directamente por el lente (Autoiris de Video), para controlar la cantidad de luz que entra al centro del CCD. Si los cambios de iluminación son muy bruscos, entonces éste se cierra para no dejar pasar tanta luz, sin comprometer la calidad de la imagen.

4. Formatos de los lentes:

Al igual que las cámaras los lentes también tienen formatos y éstos no son intercambiables tomando en cuenta que los lentes de formatos pequeños no se pueden instalar en cámaras de formatos grandes, porque se tendría una visión tipo tubo. De lo contrario los lentes de un formato mayor puestos en una cámara de formato menor tienen un efecto de zoom.

Existen lentes fijos y varifocales. Los primeros poseen una visión fija de 3.5mm y funcionan con todos los tipos de iris, mientras que los varifocales tienen un lente que da una longitud focal variable para la función de zoom manual o automático. La relación entre formato y longitud focal, para determinar el zoom de una cámara se indica en la Tabla N° 3.

Formato	Longitud del Foco Inicial	Longitud del Foco Final	Zoom Ratio
1/3"	6,5 mm; 6 mm	39 mm; 60 mm	6x; 10x
1/2"	8mm; 8mm	48 mm; 80 mm	6x; 10x
2/3"	11,5 mm; 10 mm; 9,5 mm	69 mm; 100 mm; 152 mm	6x; 10x; 16x
1"	16 mm	160 mm	10x

Tabla N° 3: Determinación del Zoom

Fuente: Diseño e Instalación de Sistemas de CCTV

Elaborado: Por los investigadores

2.2.5.1.4 Medio de Transmisión

El medio de transmisión constituye el soporte físico a través del cual emisor y receptor pueden comunicarse en un sistema de transmisión de datos. Distinguimos dos tipos de medios: guiados y no guiados. En ambos casos la transmisión se realiza por medio de ondas electromagnéticas. Los medios guiados conducen (guían) las ondas a través de un camino físico, ejemplos de estos medios son el cable coaxial, la fibra óptica y el par trenzado. Los medios no guiados proporcionan un soporte para que las ondas se transmitan, pero no las dirigen; como ejemplo de ellos tenemos el aire y el vacío. (Tomasi, 1996)

La naturaleza del medio junto con la de la señal que se transmite a través de él, constituyen los factores determinantes de las características y la calidad de la transmisión. En el caso de medios guiados es el propio

medio el que determina el que determina principalmente las limitaciones de la transmisión: velocidad de transmisión de los datos, ancho de banda que puede soportar y espaciado entre repetidores. Sin embargo, al utilizar medios no guiados resulta más determinante en la transmisión el espectro de frecuencia de la señal producida por la antena que el propio medio de transmisión.

La transmisión del video se puede realizar por diferentes medios tales como:

- Cable coaxial.
- Par trenzado. (UTP).
- Fibra óptica.
 - A través de la línea telefónica.
 - Inalámbricamente.
 - RED local (LAN) o INTERNET.

Dependiendo de la disponibilidad del material y de las conexiones dentro del lugar de instalación del sistema se selecciona el o los medios que mejor se adapten a los dispositivos y que permitan tener un trabajo más eficiente y confiable del sistema.

2.2.5.1.4.1 Medios Analógicos

Se cablea con RG-G9 y se poncha con BNC en los extremos, para distancias más largas se pueden utilizar transceptores hasta para kilómetro de distancia o en el mejor de los casos se puede utilizar fibra óptica para el cableado.

a) Cable de Video coaxial:

El cable coaxial, es el medio más utilizado y confiable para la transmisión de video en banda ancha. Tiene mejor blindaje que el de par trenzado, abarcando tramos más largos a velocidades mayores.

Un cable coaxial consiste en un alambre de cobre rígido como núcleo, rodeado por un material aislante, el mismo que está forrado con un conductor cilíndrico que con frecuencia es una malla fuertemente trenzada.

El conductor externo se cubre con una envoltura protectora de plástico. Su impedancia es de 75 ohms, con un voltio pico a pico en la transmisión.

El ancho de banda posible depende de la calidad y longitud del cable, y de la relación señal a ruido de la señal de datos. Los cables modernos tienen un ancho de banda de cerca de 1 GHz.

Su estructura se muestra en la Figura N° 10 y las distancias máximas de conexión en función del tipo de cable coaxial se muestran en la Figura N° 11.

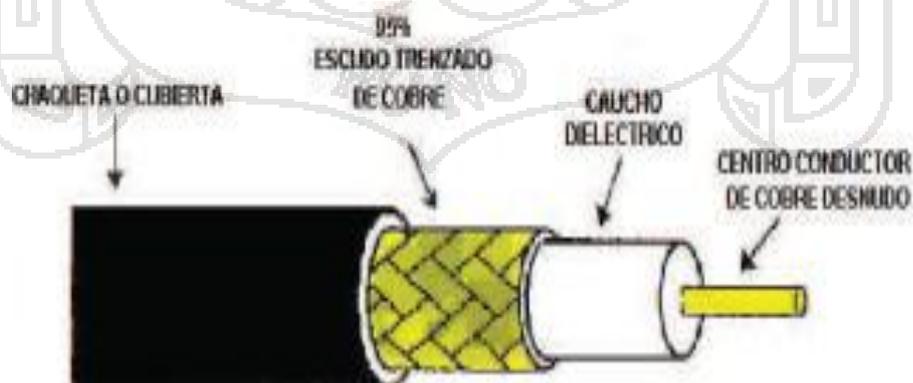


Figura N° 10: Constitución del cable coaxial
Fuente: Hoja de datos del Cable
Elaborado: Por CONDUMEX

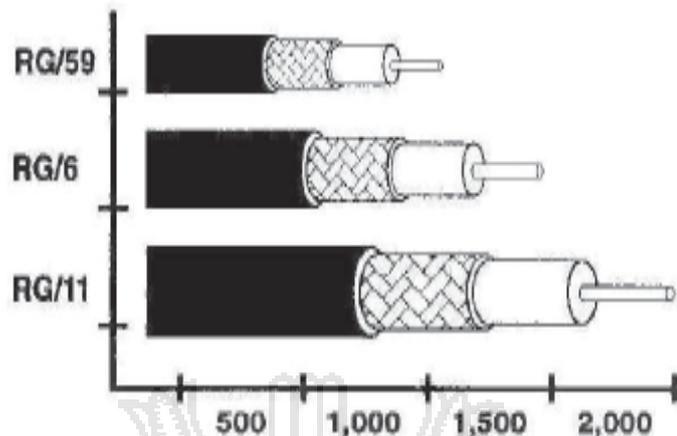


Figura N° 11: Distancia Vs numeración del cable
Fuente: Hoja de datos del Cable
Elaborado: Por CONDUMEX

b) Transmisión a través de cable Par Trenzado:

Se puede utilizar una red ya existente y solo conectarse en los nodos disponibles, lo que reduce los costos o planear una propia red de video se cablea con UTP.

Cuando la transmisión se la requiere entre largas distancias el cable coaxial no es adecuado, por lo que se utiliza el cable UTP mediante un acoplador de impedancia llamado Video Balun figura N° 12, el cual convierte la impedancia de 75 ohms del cable coaxial a 100 ohms que tiene el cable par trenzado y viceversa. El cable de par trenzado consiste en dos alambres aislados, por lo general de 1 mm de grueso, trenzados en forma helicoidal, ya que dos alambres paralelos constituyen una antena simple.



Figura N° 12: Video Balun
Fuente: Hoja de datos del dispositivo
Elaborado: Por UTC Fire & Security

El ancho de banda depende del grosor del cable y de la distancia que recorre; se pueden obtener transmisiones de varios megabits/seg, en distancias de pocos kilómetros. Hay varios tipos de cableado de par trenzado.

El ancho de banda depende del grosor del cable y de la distancia que recorre; se pueden obtener transmisiones de varios megabits/seg, en distancias de pocos kilómetros. Hay varios tipos de cableado de par trenzado.

El cable UTP categoría 3, consiste en dos alambres aislados que se trenzan de manera delicada. Cuatro de estos pares se agrupan por lo regular en una envoltura de plástico para su protección. El ancho de banda de este cable es de 16 MHz/100m.

El cable UTP categoría 5, es similar al de categoría 3, pero con más vueltas por centímetro, lo que produce una menor diafonía y una señal de mejor calidad a distancias más largas. El ancho de banda de este cable es de 100 MHz/100m. Este cable es adecuado para transmisiones de video análogo y para transmisión de datos en redes informáticas.

Las siguientes son las categorías 6 y 7, que pueden manejar señales con anchos de banda de 250 y 600 MHz, respectivamente.

2.2.5.1.4.2 Medios Inalámbricos

Estas bandas cubren aproximadamente desde 55 a 550 Mhz. Son también omnidireccionales, pero a diferencia de las anteriores la ionosfera es transparente a ellas. Su alcance máximo es de un centenar de kilómetros, y las velocidades que permite del orden de los 9600 bps. Su aplicación suele estar

relacionada con los radioaficionados y con equipos de comunicación militares, también la televisión y los aviones (Couch, 1995).

Habitualmente son cámaras muy lejanas con antenas dedicadas para su transmisión. Son cámaras ya con la especificación de este tipo de transmisión y solo son configuradas dentro del alcance de la red con acceso Wifi.

Este tipo de conexión inalámbrica resulta muy óptima, el gran inconveniente que presenta este tipo de tecnología es el costo de las cámaras, aplicándose este tipo de conexión en el sector industrial.



Figura N° 13: CCTV inalámbrico
Fuente: Hoja de equipos de Seguricentro
Elaborado: Por Seguricentro

2.2.5.1.5 Video Grabadores Digitales

Estos equipos se los utiliza cuando se diseña un circuito cerrado de televisión y para seleccionarlo se debe tomar en cuenta los siguientes aspectos:

- El número de cámaras del sistema.
- La capacidad de integración con otros sistemas, como alarmas.
- El número de monitores.
- Las funciones de monitorización en vivo.
- Capacidad de comunicaciones en distintos protocolos y redes.

- Cámaras estacionarias o móviles.

Estas videograbadoras pueden alcanzar un tiempo de grabación de hasta 1000 días debido a la tecnología de compresión de video, utilizando un disco duro de enorme capacidad de grabación. Posee además capacidad de grabación de eventos de alarma por movimiento y por acción de dispositivos mecánicos conectados a las entradas de alarma.

En la mayoría de las videograbadoras de estas características se tiene la función de control de domos (cámaras con características especiales) en el mismo equipo (algunas soportan diferentes marcas y protocolos). Además en un circuito cerrado de televisión se pueden utilizar las unidades de movimiento conocidas como pantilt, que son unos motores donde se montan las cámaras y se las puede mover hacia la izquierda, derecha, arriba y abajo, todo esto a través de los controladores que están en el centro de control, o se puede utilizar cámaras tipo PTZ (pan, tilt, zoom).



Figura N° 14: DVR LSVISION de 16 canales
Fuente: Hoja de Equipos de LSVISION
Elaborado: Por LSVISION

2.2.5.1.6 Monitoreo

El efecto más importante para una adquisición de un sistema CCTV es obtener mejor supervisión y control de los clientes y los empleados en una empresa. Un buen sistema CCTV permite al personal de seguridad monitorear

un área extensa con pocas personas y hacer más efectiva la vigilancia del área por cubrir. Con sistemas inteligentes se pueden configurar reacciones diferentes (e-mail, sirenas, llamadas automáticas a teléfonos o celulares, iluminación, etc.) según el área, horario e incidente en cuestión (Calderón, 1990).

- **Monitoreo Local:**

Podemos colocar Monitores convencionales, desde televisores y pantallas para PC lo que no es del todo recomendable pero si económico, o monitores profesionales que pueden estar prendidos 24hrs al día esto para poder estar visualizado lo que ocurre en las cámara el tipo de monitor y la cantidad lo define el tipo de grabador que se esté utilizando también se pueden hacer arreglos específicos de monitores utilizando distribuidores de video o matriciales.

- **Monitoreo Remoto:**

Una vez que nuestro grabador sea posible configurar con salida a internet, podemos tener una página en la cual podamos visualizar las cámaras y gracias a que el internet está al alcance en cualquier parte del mundo tener así nosotros acceso en donde quiera que estemos. Podemos monitoreas en nuestros celulares, siempre y cuando esté disponible el software dependiendo de las características de nuestro grabador, y las características de nuestros teléfonos celulares, en una PDA, en un iPod touch o iPhone, laptop, notebook, etc. (Couch, 1995).

2.2.5.2 Sistema de Control de Acceso

Los sistemas de control en los accesos, tanto en Agencias, como Bóvedas cualquiera sea la actividad que realizan, es un elemento importante en un moderno sistema de seguridad. Para la conformación de un buen control de

acceso, existen cerraduras electromagnéticas controladas mediante lectoras de tarjetas inteligentes RFID y de banda magnética que requieren la introducción de diversas claves secretas, a través de mando a distancia por infrarrojo como alternativa a una llave de seguridad, e incluso accesos a través de módulos de pared que exigen pasar la banda magnética de una tarjeta, reconocer el código programado en tarjetas ICC, introducir un código mediante un teclado y reconocimiento de huella digital, palma de la mano e iris de los ojos (Guada, 2006).

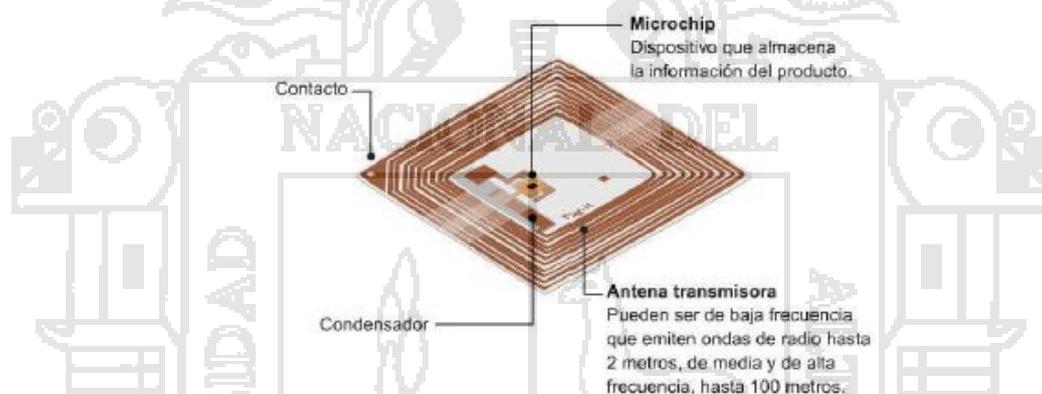


Figura Nº 15: Tarjeta RFID

Fuente: Diseño e Implementación de un Sistema de Control de Acceso

Elaborado: Por Justo Saavedra

Básicamente en una empresa se establecen jerarquías para los trabajadores de la misma en función de las cuales se permite o no el ingreso a determinada dependencia. Para llevar a cabo un control de acceso eficiente se debe seleccionar el nivel de seguridad que se requiere para así hacer uso del dispositivo más adecuado para llevar a cabo la tarea. De esta manera se establecen los siguientes niveles de acceso:

a. NIP (Número de Identificación personal):

Es el sistema de control de acceso más básico, que se basa en asignar un código numérico a las personas que tienen acceso a áreas restringidas. Esta tecnología es de comprobada eficiencia al relacionar códigos con los derechos

definidos para cada uno de los usuarios; sin embargo su nivel de seguridad es bajo, ya que cualquier persona que tenga conocimiento del código podrá tener acceso al área restringida.

b. Proximidad:

A este nivel de acceso se lo conoce como sistema de no-contacto, el cual se basa en transmisores (tarjetas o tags) y receptores que actúan de forma inalámbrica para el intercambio de datos. Al presentar la tarjeta a cierta distancia, el sistema de recepción puede leer el código de la misma y enviarlo al centro de control para su validación, y otorgar o no el acceso al área restringida. La tecnología de proximidad está probada como una de las más eficientes, y es aplicada tanto para acceso de personas como de vehículos.

c. Sistemas Biométricos:

Los sistemas biométricos son de un mayor nivel de seguridad, pues se basan en identificadores únicos del individuo para permitir el acceso. Existen sistemas de reconocimiento facial, de venas, de iris, de huella digital, etc. Esta última es una tecnología más probada y por ende de menor costo.

Los Lectores de Huella Digital por ejemplo, sólo permitirán el acceso a la persona cuya huella digital fue dada de alta en el sistema; aquí no existe el problema de robo de claves o de tarjetas. La tecnología actual y los avanzados algoritmos de búsqueda permiten identificar una huella de entre cientos, verificadas en menos de 2 segundos.

El control de acceso brinda una mayor seguridad cuando se trata de mantener una administración eficiente y funcional de áreas importantes, incluso para mantener un registro de entradas y salidas.



Figura N° 16: Control Biométrico
Fuente: Hoja de equipos de Seguricentro
Elaborado: Por Seguricentro

2.2.5.3 Sistema Central de Alarma

Una central de alarma es un elemento de seguridad que no realiza ninguna acción para evitar o controlar una situación anormal, lo que hace es advertir de ella como una función disuasoria frente a posibles problemas como: la intrusión de personas, el inicio de incendios, el desbordamiento de un tanque o cualquier situación que sea anormal para el usuario.

La alarma de intrusión más básica es un circuito eléctrico simple colocado en una puerta de entrada. Los sistemas de alarma de intrusión modernos poseen una Caja de Control, la cual se conecta a uno o más circuitos de alarma, pero también cuenta con su propia fuente de poder en la mayoría de los casos alimentada desde un dispositivo UPS.

Monitorea los circuitos y activa la alarma cuando éstos son cerrados o abiertos. Pero una vez que la alarma es activada, la caja de control no la desactivará hasta que alguien introduzca un código de seguridad en el teclado.

2.2.5.3.1 Tipos de Centrales de Alarma

Hay tres tipos de centrales según su aplicación y número de detectores que debe alimentar. Son: Central exterior, central interior y central selectora de zona (Calderón, 1990).

- **Central exterior**

Las centrales exteriores son las más simples y sencillas; van colocadas en el exterior de los lugares a vigilar. Los sensores que se usan van conectados a ella y en la misma caja de la central están ubicados una sirena y un foco intermitente.

La carcasa está convenientemente tratada contra la corrosión y actos vandálicos, pero su utilización cada vez es menor, siendo su aplicación más usual en pequeñas viviendas y establecimientos.

Su utilización es cada vez menor, ya que no da más posibilidades que las de exteriorizar por medios acústicos y ópticos la activación del estado de la alarma. En general, son propensas a ser ignoradas y el ruido que provocan es más motivo de rechazo que de situación de alarma.

- **Central interior**

La central interior se ubica dentro del inmueble a proteger y tiene la posibilidad de controlar numerosos puntos de detección tanto para robo como para incendio.

Varían según el tamaño y se usan una u otra central existente en el mercado, según el número de detectores, alarmas y circuitos conexos que hay que instalar.

Existe un circuito de retardo al que van conectados aquellos sensores colocados en lugares de acceso, con el fin de que dé tiempo a desactivar la alarma, antes de que suene.

La central, lógicamente, se conecta o desconecta con cerraduras de seguridad, estando protegidas de ataques exteriores. Las cerraduras pueden ser con llaves normales, electrónicas o con clave de acceso.

Es una central mucho más compleja y fiable que la central exterior, ya que nos proporciona ciertas posibilidades muy importantes:

- a. Comunicación con la central receptora de alarmas.
- b. Programación de tiempos: salida y entrada de zonas.
- c. Instalación con líneas balanceadas.
- d. Aviso de situación de atraco.
- e. Circuito támara.

La central interior está constituida por una placa de circuito impreso en la que está montado un circuito electrónico.

El circuito electrónico está compuesto, esencialmente a su vez, de tres partes:

- Fuente de alimentación.
- Microprocesador y memoria.
- Marcador telefónico.

La placa para protegerla de posibles accidentes ocasionales y de manipulaciones malintencionadas, se instalará dentro de una caja metálica, en un lugar escondido y del inmueble a proteger.

- **Central selectora de Zonas**

La central selectora de zonas es eminentemente igual a la anterior ya que da las mismas posibilidades, pero se diferencia en que ofrece la posibilidad de diferenciar los detectores según zonas. Esto permite a un vigilante saber en cuál de las zonas se ha producido la alarma, e incluso saber el detector exacto que se ha activado, hecho que nos permite actuar con más seguridad en nuestras actuaciones.

Es una central muy robusta que entre otras, puede ofrecernos las siguientes posibilidades:

- Comunicación con la central receptora de alarmas.
- Programación por zonas. (Todas ellas distintas).
- Circuito de protección támpor, general o por zonas.
- Conexión a zonas multiplexadas.
- Conexión de varios teclados.

2.2.5.3.2 Principales características de la Central de Alarmas.

- **CONEXIÓN Y DESCONEXIÓN**

La central de alarmas dispone de mecanismos para controlar el acceso a las zonas protegidas, y efectuar su conexión y desconexión. Esta puede ser de distintos tipos:

- 1) Llave de seguridad.
- 2) Tarjeta codificada.
- 3) Teclado.

- CIRCUITOS DE DETECCIÓN

Circuito retardado

En este circuito se conectarán los detectores que detecten al usuario del sistema al conectar la alarma y salir del inmueble, o bien para entrar y desconectar, sin que en ninguno de los dos casos se dispare la alarma.

Este circuito solo funcionará con el sistema conectado.

Circuito instantáneo.

Aquí se conectarán todos los detectores que no sean activados por el usuario al poner en marcha o desconectar el sistema.

En el momento que el detector o detectores conectados a este circuito “detecten” alguna anomalía, el sistema se accionará inmediatamente, activando los sistemas de aviso instalados.

Este circuito sólo funcionará con el sistema conectado.

Circuito támara

Este circuito tiene la finalidad de garantizar que no se produzca sabotaje o manipulación alguna en el sistema, durante la desconexión del mismo, como por ejemplo, arrancar una sirena, abrir un volumétrico, etc. , haciendo dispara la alarma cuando esto ocurra.

Por lo tanto este circuito está permanentemente en vigilancia, aunque la alarma este desactivada.

- Zona cableada

Circuito cerrado donde se han instalado y conexionado en serie los detectores.

Se diversifican en zonas para en el momento de su activación, saber el lugar exacto de su ubicación.

No conviene instalar muchos detectores por zona, ya que cuando se active uno de ellos, solo sabremos la zona activada. Sólo se suelen conectar como máximo unos tres detectores por zona.

- Zona multiplexada

Instalando en cada detector un pequeño módulo codificador, que introduce un código que sólo identificará la central de alarmas, permite instalar todos los detectores en una sola zona cableada, pero con la peculiaridad de que cuando sea activado algún detector, la central identificará al detector exacto activado.

Este sistema permite simplificar de forma considerable la instalación, a una sola tirada de dos cables, abaratando consecuentemente los costes de instalación.

- Balanceo de línea.

Es un sistema de protección para la instalación de detectores realizada.

Consiste en colocar al final de las zonas cableadas una resistencia con un valor óhmico predeterminado y suministrado por el fabricante de la central, en serie con los detectores, cerrando el circuito.

En el momento que por causas de manipulación externa, se modifica el valor óhmico de la instalación (cortocircuito en el cableado o

en los detectores), la central detecta la modificación del mismo y hace activar la central.

Es un sistema en la práctica insaboteable, ya que un posible intruso no puede saber el valor de la resistencia para intentar cortar la tirada de detectores, colocando otra de igual valor, y aunque lo supiera, en el momento del cambio, como tendría que cortar por breves momentos la línea (aunque sólo fuera décimas de segundo), se activaría la alarma. Si intenta colocar otra resistencia en paralelo, se modificaría el valor general de la línea, con lo que igualmente es activada la central.

La central nos da posibilidad de conmutar zonas balanceadas o <NC>, no balanceado, para realizar las instalaciones que más nos interesen.

- Programación por tiempos.

Nos permite programar los tiempos de activación de las zonas. Pueden programarse zonas de activación instantánea, en las que por necesidad de paso del usuario para entrar o para desactivar o activar la alarma, les sea necesario un tiempo determinado.

Este tiempo puede variar desde varios segundos a varios minutos, dependiendo de las características de la instalación de la alarma.

- Aviso de situación de atraco y desconexión por coacción.

En instalaciones con riesgo de atraco, se suelen instalar centrales, que no sólo posibilitan la activación manual de atraco que dan aviso a la central receptora de alarmas (C.R.A.) al instante, sino que además prevén situaciones intermedias como de <preaviso de alarma>.

El preaviso de alarma consiste en la activación de un “**código**” de pre alarma, por causas que pueden ser la de presencia de individuos sospechosos, **situaciones** sospechosas, etc. Esto se hace por medio de un pulsador manual y pone en marcha en la central receptora un mecanismo de defensa acordado según el local vigilado.

Los “avisos o pre-avisos” de alarma, solo se producen en la C.R.A. ya que de activar sirenas, pueden poner en serio peligro la integridad física de los usuarios.

Igualmente nos permite la posibilidad de desactivar la Pre-alarma con un código paralelo de desactivación (que es diferente al código normal), que indica a la central receptora la existencia de un atraco con su consecuente emergencia para realizar la protección posible al usuario. Este último concepto es lo que se llama <desconexión por coacción>.

- Conexión con central receptora de alarmas.

Por medio de un circuito electrónico, marca automáticamente el número de teléfono programado de la central receptora de alarma para su comunicación con ella.

La conexión que efectúe la central puede variar desde la comunicación de existencia de alarma, a otras como las de <situación de atraco>.

Los sistemas comunican cualquier incidencia a la central receptora, activación y desactivación de la central, activación de zonas o de detectores, etc.

Igualmente se puede utilizar la conexión telefónica desde la central receptora al sistema concreto, para realizar cualquier variación deseada

en la programación de la central de alarmas, o para pedirle datos como el estado actual, incidencias producidas, etc.

Por ello podemos decir que es un sistema bidireccional.

2.2.5.3.3 Partes Básicas de una Central de Alarma

Los elementos básicos que forman parte de una Central de Alarma son los siguientes:

2.2.5.3.3.1 Panel de Control

Es la unidad central de procesamiento de la información del sistema. En ella se albergan la placa base, la fuente y la memoria central. Esta parte del sistema es la que recibe las diferentes señales que los diferentes sensores pueden emitir, y actúa en consecuencia, disparando la alarma, comunicándose con la central por medio de un módem, por línea telefónica o internet.

Se alimenta a través de corriente alterna y de una batería de respaldo, que en caso de corte de la energía, le proporcionaría una autonomía al sistema de entre 12 horas y 3 días (dependiendo de la capacidad de la batería).



Figura N° 17: Panel central Bosch
Fuente: Foto Tomada el 05/01/2015
Elaborado: Por los Investigadores

Es el cerebro de la instalación está en estado de vigilancia continuamente, recibiendo información constantemente de los circuitos detectores que componen el sistema, accionando los dispositivos de aviso (sirenas, conexiones a la C.R.A. si la hubiera), en el momento que sea activado cualquier detector o alguna anomalía en el mismo (intentos de vulneración del sistema de seguridad).

En la parte exterior de la carcasa, se dispone de una serie de pilotos indicadores que dan información del estado del sistema (funcionamiento de los detectores, alimentación, etc.).

En el interior dispone de una batería auto recargable por medio de la tensión de red, en previsión de posibles cortes de suministro eléctrico.

2.2.5.3.3.2 Teclado

Se trata de un teclado alfa numérico. Su función principal es la de permitir a los usuarios autorizados (usualmente mediante códigos pre-establecidos) armar (activar) y desarmar (desactivar) el sistema. Además de esta función básica, el teclado puede tener botones de funciones como: Emergencia Médica, Intrusión, Fuego, etc. El teclado es el medio más común mediante el cual se configura el panel de control.



Figura N° 18: Teclado Bosch
Fuente: Foto Tomada el 04/01/2015
Elaborado: Por los Investigadores

2.2.5.3.3.3 Sirena

Es el dispositivo audible básico del sistema, el cual suena cuando se detecta una intrusión específica avisándole al intruso que ha sido detectado. Para elementos de alarma como Botones de pánico, cuando se activan por lo general la sirena no suena. Tiene autonomía propia (puede funcionar aún si se le corta el suministro de corriente alterna o si se pierde la comunicación con la central procesadora) colocada dentro de un gabinete protector (de metal, policarbonato, etc.). Puede tener además diferentes sistemas luminosos que funcionan en conjunto con la disuasión sonora.

2.2.5.3.3.4 Sensores interiores de movimiento

Los sensores electrónicos son dispositivos de reducido tamaño y alimentados por baterías, o fuente de alimentación a baja tensión (6v. a 12v.) que detectan con un campo de actuación variable (varios metros), la presencia humana u otros elementos extraños.

Las variaciones eléctricas enviadas por los sensores son recogidas por la unidad de control, que una vez convenientemente tratadas dan lugar a la activación de los sistemas de señalización: ópticos, acústicos, etc.

En este sentido existen: sensores infrarrojos, de microondas o fotoeléctricos que detectan cambios de temperatura y movimiento. Si estos sensores detectan movimiento estando el sistema conectado, dispararán la alarma. Existen detectores regulados para no detectar mascotas, tales como perros y gatos.

Los sensores de movimiento utilizan luces infrarrojas para detectar los cambios de calor, como por ejemplo cuando una persona se mueve a través de una habitación, esta luz lo detecta con la ayuda del sensor infrarrojo. Si una persona se mueve del rango del sensor de movimiento, se activa la alarma. Los sensores infrarrojos son más baratos que los sensores de microondas y los sensores ultrasónicos. Los sensores infrarrojos generalmente son más pequeños y muy confiables (Marcelo, 2002).



Figura N° 19: Sensor de movimiento
Fuente: Foto Tomada el 04/01/2015
Elaborado: Por los Investigadores

2.2.5.3.3.5 Sensores Magnéticos

Los sensores de proximidad magnéticos son caracterizados por la posibilidad de distancias grandes de la conmutación, disponible de los sensores con dimensiones pequeñas. Detectan los objetos magnéticos (imanes generalmente permanentes) que se utilizan para accionar el proceso de la conmutación. Los campos magnéticos pueden pasar a través de muchos materiales no magnéticos, el proceso de la conmutación se puede también accionar sin la necesidad de la exposición directa al objeto. Usando los conductores magnéticos (ej. hierro), el campo magnético se puede transmitir

sobre mayores distancias para, por ejemplo, poder llevarse la señal de áreas de alta temperatura.

Son sensores que forman un circuito cerrado mediante un imán y un contacto de relé muy sensible a campos magnéticos pequeños que al separarse cambia el estado de N.C. o N.O y viceversa enviando una señal de alarma.



Figura N° 20: Sensor magnético para puertas
Fuente: Foto Tomada el 14/12/2014
Elaborado: Por los Investigadores

2.2.5.3.3.6 Detector de Humo

Son dispositivos que detectan un conato de incendio, mediante sensores de calor o de humo, que utilizan sistemas capacitivos, cuya capacitancia varía por la presencia de humo en el lugar que se encuentran instalados. Si el detector de humo se activa, el panel de control notificará a la estación central de monitoreo una alarma de incendio.



Figura N° 21: Detector de Humo
Fuente: Foto Tomada el 14/12/2014
Elaborado: Por los Investigadores

2.2.5.3.3.7 Botones de Pánico

Son de acción manual y deben estar localizados en lugares estratégicos fuera de la vista de posibles intrusos. Al presionar los botones se enviará una señal a la central de monitoreo solicitando ayuda que generalmente es de tipo silenciosa aunque se puede hacer que suene la sirena en el lugar.

2.3 GLOSARIO DE TERMINOS BASICOS

- **INCIDENTE:** Hecho Acontecido en las instalaciones de Caja Rural Los Andes S.A.
- **BACKUP CELULAR:** Dispositivo electrónico usado para la interconexión del sistema de alarmas de Caja los Andes S.A.
- **PULSADOR FIJO:** Dispositivo que se encuentra en ventanilla, jefe de oficina, su uso es restringido solo por el personal autorizado o de turno.
- **CIERRE DE OFICINA:** Cuando se activa por completo el Sistema de Alarmas en la Agencia u Oficina.
- **PULSADOR INALAMBRICO:** De uso exclusivo del personal de vigilancia y este se usa en última instancia.
- **ESTROBO:** Dispositivo que emite luz blanca y sonido al haber detectado el panel de alarma incidente de fuego en algún lugar de la agencia u oficina.
- **SALA DE COMUNICACIONES:** Lugar donde se encuentran Ubicados e instalados todo el sistema de seguridad, y servidores, es de acceso restringido.

- **CENTRAL DE MONITOREO:** Lugar donde llegan todos los reportes de alarmas de las diferentes alarmas o incidentes generados en toda la red de Agencias de Caja los Andes S.A.
- **RESTABLECIMIENTO DE PULSADOR:** Retornar a la posición original del pulsador fijo que se encuentra en ventanilla y jefe de Oficina, para que no siga generando falsa alarma.

2.4 HIPOTESIS DE LA INVESTIGACION

El implementar un Sistema Integral de Seguridad Bancaria ayuda a proteger y cuidar los bienes físicos de la entidad financiera, haciendo uso de cámaras CCTV, Central de Alarmas, haciendo uso de sensores y mejorando en cada una de estas en determinadas agencias, así mismo promoverá el mejoramiento de atención al cliente.

2.4.1 Hipótesis Específica

- Haciendo uso de un control dual remoto y/o biométrico, teniendo en cuenta los factores tecnológicos.
- Reducir el tiempo de retardo de los sensores, haciendo que las señales sean de menos peso y de fácil manejo.

2.5 OPERACIONALIZACION DE VARIABLES

2.5.1 Variables Dependientes

- Las agencias de Caja Rural – Los Andes S.A.

2.5.2 Variables Independientes

- Sistema de Seguridad Integral.

Variable de Estudio	Variable	Medida
Dependiente	Agencias de Caja rural Los Andes S.A.	3
Independiente	Sistema Integral de Seguridad	2

Tabla N° 4: Cuadro de Variables
Fuente: Operacionalización de Variables
Elaborado: Por los Investigadores





3 DISEÑO METODOLÓGICO DE LA INVESTIGACIÓN

3.1 Tipo y diseño de Investigación

La presente investigación, responde a la modalidad de investigación aplicada, porque se utiliza conocimientos y teorías adquiridas a lo largo de la formación universitaria, además de desarrollar un estudio y levantamiento de información in situ para determinar si la investigación puede ser útilmente aplicada con o sin mayor refinamiento para los propósitos definidos contrastando las hipótesis planteadas.

La presente Investigación tiene un enfoque Cualitativo, porque influye directamente en la sociedad con el que se pretende solucionar el problema de inseguridad.

3.2 Población y Muestra de la Investigación

3.2.1 Población

La empresa Caja Rural – Los Andes S.A., consta con un total de 21 Oficinas o Agencias, estando éstas distribuidas alrededor del país. Los departamentos en los que se encuentra son: Puno, Arequipa, Ayacucho, Cusco.

Se considera población a la cantidad total de Agencias o Oficinas, que tiene la empresa. Y estas se resumen en la tabla N° 5.

N°	Oficina	Dirección	Departamento
1	Back Office	Jr. Junín N° 129	Puno
2	Puno	Jr. Santiago Giraldo N° 262	Puno
3	Acora	Av. Panamericana N° 320	Puno
4	Ilave	Jr. 28 de Julio N° 218	Puno
5	Yunguyo	Jr. Cusco N° 330	Puno
6	Desaguadero	Av. Panamericana N° 355	Puno
7	Coata	Jr. Puno MZ "D" Lote 2 S/N	Puno
8	Juliaca - Pedro Vilcapaza	Av. Huancané N° 244-246	Puno
9	Juliaca - San Roman	Jr. San Roman N°150	Puno
10	Taraco	Jr. 28 de Julio	Puno
11	Huancané	Jr. 19 de setiembre N° 101	Puno
12	Ayaviri	Jr. 25 de Diciembre N° 645	Puno
13	Azangaro	Jr. 28 de Julio N° 265	Puno
14	Macusani	Jr. 28 de Julio N° 104	Puno
15	Sicuaní	Av. Centenario N° 238	Cusco
16	Espinar	Jr. Cusco N° 401-C	Cusco
17	Chivay	Mz. D, LOTE N° 09	Arequipa
18	Aplao	Av. Principal Lote 3A, Mz C2	Arequipa
19	Ayacucho	Jr. 9 de Diciembre N° 427	Ayacucho
20	Huanta	Jr. Miguel Untiveros N° 532	Ayacucho
21	Pampa Cangallo	Mz. "U" LOTE "1-A"	Ayacucho

Tabla N° 5: Dirección de Oficinas
Fuente: Ficha RUC de la empresa
Elaborado: Por los Investigadores

También se considera como población a los distintos puntos de atención que tiene la empresa donde se realizan operación básicas, pero también necesitan un servicio mínimo de seguridad, estos puntos pequeños de atención no llegan al rango de Oficina y/o Agencia.

Los puntos de atención al cliente (PAC's) están ubicados en toda la región de Puno y se resumen en la tabla N° 6.

N°	Pac's	Dirección
1	Mañazo	Plaza de Armas S/N
2	Muñani	Lote N° 18, Mz "K"
3	J.D.CH	Jr.Guillermo S/N
4	Nuñoa	Jr. Puno y Jr. Arica
5	Macari	Jr. Riquelme N° 103

Tabla N° 6: Puntos de Atención al Cliente
Fuente: Relación de Pac's de la empresa
Elaborado: Por los Investigadores

3.2.2 Muestra

El tamaño de la muestra se obtiene por la técnica de muestreo por conveniencia basada en un criterio estratégico.

Para la muestra la técnica que se utilizará es: “Muestreo por acceso más fácil”, por que consiste en seleccionar aquellos en los que se puede realizar el estudio en forma rápida y la que brinde mayor variedad a la hora de obtener datos.

De esta manera la muestra seleccionada son 3, entre Oficinas y PACs, las cuales se detallan en la siguiente tabla.

	Lugar	Dirección
Oficinas	Ilave	Jr. 28 de Julio N° 218
	Coata	Jr. Puno MZ "D" Lote 2 S/N
PAC	Macari	Jr. Riquelme N° 103

Tabla N° 7: Muestra Escogida
Fuente: Población y muestra de la Investigación
Elaborado: Por los Investigadores

3.3 Ubicación y Descripción de la Población

La ubicación de la población para este proyecto de investigación se encuentra en el departamento de Puno.

Se escogió dicha población, por presentar diferentes tipos de factores tecnológicos y por ser relativamente de fácil acceso, el cual ayuda bastante en la recopilación de datos.

3.4 Material Experimental

El material experimental es el Sistema de Alarma que es Autónomo, así como, el circuito cerrado de televisión (CCTV), los cuales son diseñados para

satisfacer las necesidades básicas de Seguridad en la Red de Agencias u Oficinas de Caja Rural Los Andes S.A.

Puesto que se tuvo que analizar y experimentar con cada parte y accesorios que cuenta cada uno de los sistemas instalados y diseñados para este proyecto de investigación.

3.5 Técnicas e Instrumentos para recolectar información

Para lograr recolectar información existe una gran variedad de instrumentos o técnicas tanto cualitativas como cuantitativas y se pueden usar ambos tipos en un mismo estudio, por tal razón nos apoyamos con la utilización de las siguientes técnicas con la finalidad de recolección de datos:

- **Entrevista:** Se aplicó un cuestionario a los funcionarios encargados y colaboradores de la administración, con el objetivo de saber sobre el conocimiento de la normativa legal sobre seguridad bancaria y transporte de valores y su nivel de cumplimiento. Para desarrollar esta técnica se aplicó entrevistas semi estructuradas, las cuales se basan en una guía de preguntas y el entrevistador puede aplicar preguntas adicionales para obtener mayor información o aclarar conceptos. En la entrevista cualitativa pueden hacerse preguntas sobre experiencias, opiniones, percepciones, conocimientos.

El formulario que se utilizó para la entrevista y recolección de información se adjunta en el Anexo I.

- **Documentos:** Se revisó el Método Mósler para análisis y evaluación de riesgos antisociales, así como también se revisó el Método Meseri para

análisis y evaluación del riesgo de incendio. Para la parte legal se ha revisado las resoluciones de la Superintendencia de Banca y Seguros referentes a la seguridad bancaria y para el transporte de valores la Ley y Reglamento de Vigilancia y Seguridad Privada, así como también Acuerdos Ministeriales y Resoluciones sobre la materia. Adicional para la parte conceptual se ha revisado varias teorías de seguridad bancaria y transporte de valores.

Dicha documentación se puede observar en el Anexo II

3.6 Técnicas para el procesamiento y análisis de datos

El procesamiento de la información recopilada se realizó en un sistema de planos y mediciones, documentos que se fueron desarrollando según se fue avanzando con el proceso de análisis y diseño del sistema de seguridad instalado en las Oficinas de Caja Rural - Los Andes S.A.

Una vez realizada el recojo de datos a través de los cuestionarios descritos, comienza una fase esencial para toda investigación, referida a la clasificación o agrupación de los datos referentes a cada variable objetivo de estudio y su presentación conjunta.

3.7 Procedimiento del experimento

Se realizó una breve encuesta a cada uno de los funcionarios encargados, de las diferentes Agencias u oficinas de Caja Rural – Los Andes S.A., midiendo su nivel de conocimiento en temas referidos a seguridad, planes de emergencia, plan de contingencia contra robos o asaltos, uso y manejo de extintores, plan de

acción contra actos antisociales, y finalmente recogiendo las sugerencias en base a la experiencia de algunos funcionarios en otras instituciones bancarias.

Seguidamente se procedió con la recopilación de información documentaria, que ayude en la implementación de los requisitos mínimos de seguridad en entidades financieras o bancarias. Obteniendo toda la información necesaria como documentos legales, Normativas y demás documentos.

Para finalizar se hizo la recopilación de información, para conocer el Sistema CCTV (Circuito Cerrado de Televisión) y los sistemas de seguridad, luego la calidad de los equipos y su funcionamiento, posteriormente se realizará un análisis para la implementación del sistema, por último obtener información concreta y clara de nuestro estudio de investigación.

Una vez recopilado todos esos datos se procedió a diseñar un sistema de seguridad acorde a la realidad de cada Agencia o Oficina mencionados en la tabla N° 7.

3.8 Plan de tratamiento de datos

Para el procesamiento de los datos se utilizará el Software de Excel 2013, donde se elaborará, la respectiva base de datos para poder atender las diferentes incidencias que se reporten en las Agencias o oficinas según la tabla N° 7.

Mediante el uso de este software se podrá realizar tablas resumen y cuadros comparativos de todo lo referido al sistema de alarma autónomo el cual está activo las 24 horas del día.

Mediante la realización de cuadros comparativos se podrá conocer cuántas de las señales del panel de alarma serán falsas o verdaderas, para que este no

incurra en mayor gasto para la empresa, y que el personal se vaya habituando al uso de dicho sistema.

3.9 Prueba de la Hipótesis

4 Hipótesis específica 01

Haciendo uso de un control dual remoto y/o biométrico, teniendo en cuenta los factores tecnológicos.

Validación:

El diseño de un Sistema Central de Alarma autónomo, en Caja Rural - Los Andes S.A., basado en las siguientes detalles:

- Llevar un control dual en el cierre de Agencia como de bóveda.
- Monitorear con el sistema de CCTV, el acceso a las áreas restringidas en este caso bóveda.
- Dar contraseñas personales e intransferible, con un periodo de cambio de tres meses.

Evaluando cada uno de los indicadores arriba mencionados se dará la validación de la hipótesis.

4.1.1 Hipótesis específica 02

Reducir el tiempo de retardo de los sensores, haciendo que las señales sean de menos peso y de fácil manejo.

Validación:

Diseñado el sistema de seguridad y eligiendo el medio de comunicación y/o transmisión se logró reducción del tamaño de las señales enviadas a la central de monitoreo, de acuerdo al medio de trasmisión el uso del sistema de alarma

se hace más fácil el manejo de este y el tiempo de reacción mejora notablemente. Se detalla las acciones realizadas:

- Conectar el sistema de alarma a internet se reducen costos y mejora la respuesta del panel de alarma se reduce drásticamente el tiempo de llegada a la central de alarma.
- El uso de la red telefónica hace que el sistema de alarmas sea más robusto, a diferencia de conectar a internet demora unas décimas de segundos en llegar las señales a la central de monitoreo, su ventaja es que se hace de fácil manejo a la hora de poder brindar un mantenimiento de urgencia.
- En los PACs se recurre al medio de transmisión via GSM o mensajes de texto. Lo cual resulta muy óptimo puesto que las condiciones tecnológicas que se encuentran responde favorablemente.

4.1.2 Hipótesis General

El implementar un Sistema Integral de Seguridad Bancaria ayuda a proteger y cuidar los bienes físicos de la entidad financiera, haciendo uso de cámaras CCTV, Central de Alarmas, haciendo uso de sensores y mejorando en cada una de estas en determinadas agencias, así mismo promoverá el mejoramiento de atención al cliente.

Validación:

Luego de haber validados nuestras dos hipótesis específicas, consecuentemente también se validara nuestra hipótesis general.



5 ANÁLISIS, E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN

5.1 ESCENARIO INICIAL

El escenario inicial en cual se encontró la oficina o agencia detalladas en la tabla N° 7 de Caja Rural Los Andes S.A., se detalla a continuación, teniendo en cuenta la muestra escogida para el presente proyecto de investigación.

Se describe individualmente en cada una de las Agencias, Oficinas y PACs, ubicados en la Región de Puno.

5.1.1 Oficina llave

La Oficina de llave, al iniciar este proyecto de investigación dicha oficina se encontró en proceso de remodelación y traslado.

En sus antiguas instalaciones se verificó un sistema de seguridad obsoleto, el cual no brindaba una adecuada protección a la agencia, se determinó cambiar el sistema de seguridad antiguamente instalado por las siguientes razones:

- El panel de control del sistema de alarma se encontraba desfasado, no brindaba las facilidades tecnológicas para la realización del proyecto de investigación.
- El panel de control, no permitía realizar cierres remotos.
- Panel de control no contaba con la interfaz necesaria para poder conectarse a red o internet.

- No contaba con alimentación de respaldo en caso de apagones, el panel no brindaba la facilidad para poder asignar nuevas claves u contraseñas de forma remota.
- El panel no brindaba la opción de programar remotamente las diferentes zonas de la agencia, así como tampoco se podía expandir a más zonas en caso de que la agencia se expanda.

Con respecto al circuito cerrado de televisión (CCTV), se encontró las siguientes deficiencias en la agencia de llave:

- La capacidad de almacenamiento del DVR, era muy poca dificultando la solución de algunos incidentes, este solo almacenada 20 días.
- La calidad de las cámaras eran bastante deficientes dificultando ver con claridad los diferentes puntos de la agencia.
- El cable utilizado para esas instalaciones, no era el adecuado y presentaba bastante deterioro.
- El software y hardware no daban las facilidades para la realización del proyecto de investigación, no presentaba algún tipo de conexión a red o internet el software de acceso era muy lento y dificultoso de manejar.

Es por estas razones es que se procedió a un nuevo diseño e instalación del sistema de seguridad en la Agencia de llave.

5.1.2 Oficina Coata

La oficina Coata Ubicada en el departamento de Puno, se inauguró en medio del desarrollo de la investigación.

Dicha oficina por estar considerada en la calidad de Nueva Oficina, no contaba con los requisitos mínimos de seguridad.

En esta oficina el proyecto se empezó desde cero, analizando las condiciones favorables para nuestro sistema de seguridad a implementar, analizando las ventajas y desventajas del lugar y que medios de transmisión son los mejores en este lugar, puesto que se encontraba en un lugar alejado y con serias deficiencias tecnológicas.

5.1.3 PAC Macari

Al tratarse de un punto de atención al cliente (PAC), con operaciones restringidas se presentó como un nuevo reto para esta investigación.

Se buscaba diseñar un nuevo sistema de seguridad para estos establecimientos, que cumpla con todo lo que hace el sistema de seguridad instalados en las oficinas o agencias, pero este debía de ser de bajo costo.

Realizando los respectivos análisis y estudios se logró cumplir con gran parte de las expectativas.

5.2 REQUISITOS DEL SISTEMA DE SEGURIDAD

Dentro de los sistemas de seguridad se incluyen los sistemas operativos, infraestructuras, aplicaciones de negocio, aplicaciones estándar o de uso generalizado, servicios y aplicaciones desarrolladas por los usuarios

El diseño e implantación de los sistemas de seguridad que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información.

Todos los requisitos de seguridad deberían identificarse en la fase de recogida de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información.

5.2.1 Requisitos mínimos

Según el Marco legal: Resolución Ministerial N° 0689-2000-IN/1701 los requisitos mínimos de seguridad que debe cumplir toda agencia bancaria y/o financiera son:

“...

- **Artículo 4.-** El local que ocupan las Oficinas deberán contar con sistema de alarma y protección contra asaltos, robos e intrusión, debidamente publicitados, según el formato.

El sistema de alarma contra asalto será silente (desde el ingreso del personal de la entidad hasta el cierre del local) pudiendo ser sonoro cuando en el local ya no se encuentre este personal.

Los Recibidores/Pagadores deberán disponer de un pulsador de alarma.

- **Artículo 5º.-** Todas las OFICINAS que efectúen transacciones en efectivo deberán estar protegidas por un servicio de vigilancia armada dotado con chaleco antibalas, con capacidad de efectuar.

El procedimiento de seguridad establecido por cada oficina así como de hacer funcionar la alarma a distancia con un pulsador inalámbrico bajo su control, durante las horas de operación, debiendo encontrarse instalados desde el horario de ingreso del personal de la entidad hasta el cierre del local.

- **Artículo 6º.-** El personal de vigilancia deberá contar con adiestramiento permanente y especializado. Dicho personal estará sujeto a las normas del Reglamento de Servicios de Seguridad Privada de la DICSCAMEC o a las normas reglamentarias específicas de la Policía Nacional, según corresponda.
- **Artículo 11º.-** La Unidad de Seguridad Interna, previa evaluación, determinará las necesidades de vigilancia, adiestramiento especializado al que se refiere el Art. 6º, sistemas, equipos, dispositivos de seguridad y alarma que requieran las OFICINAS, elaborando a su vez las normas y procedimientos para su mejor operación y mantenimiento.
- **Artículo 12º.-** Todas las OFICINAS deberán contar con un sistema de alarma a distancia con capacidad de reportar eventos de asalto e intrusión a una central de alarma de operación continua de propiedad de las Empresas, Asociación o Fundación del Sistema Financiero o de terceros. Esta central deberá contar con los medios de comunicación

necesarios para transmitir la información de manera eficiente e inmediata a los órganos de auxilio de la Policía Nacional.

- **Artículo 13º.-** Las OFICINAS deberán contar con un sistema de energía de respaldo para permitir la continuidad en el funcionamiento de sus sistemas operativos de seguridad.
- **Artículo 17º.-** Todas las puertas de bóveda y caja fuerte de seguridad de las OFICINAS deberán estar dotadas de cerraduras especiales de llave, clave, retardo (corto y largo plazo).
- **Artículo 18º.-** Para la apertura y cierre de la puerta de bóveda y/o caja fuerte de seguridad, la OFICINA deberá contar con un plan dual en los mecanismos de seguridad, claves o llaves y sus combinaciones, debiendo efectuarse los cambios de claves cada vez que se reemplace a la persona responsable. La llave duplicada deberá guardarse en custodia en otro local. ...”

5.2.2 Aplicación Bancaria

Los requisitos de un Sistema de Seguridad en una entidad financiera o Bancaria, hace uso de varias aplicaciones.

Una aplicación Bancaria o Financiera sirve para consumir y brindar los servicios que ofrece la entidad. Estas aplicaciones pueden realizar entre otras cosas las siguientes transacciones:

- Transferencias directas, entre bancos locales, o extranjeros.
- Pago de servicios como agua, luz, teléfono, etc.
- Consulta de saldos.

- Pago de tarjeta de crédito.
- Recargas electrónicas de telefonía celular.

Estas aplicaciones son accesibles desde muchos equipos como dispositivos móviles, etc.

Una aplicación bancaria debe cumplir al menos con las siguientes características:

- Eficiencia.
 - Seguridad.
 - Funcionalidad.
- **Eficiencia:** Ya que la razón de utilizar una aplicación bancaria es para tiempo, los tiempo de respuesta no deben ser muy grandes para lo cual se debe implementar sistemas de balanceo de carga con algoritmos que reduzcan este tiempo.
- **Seguridad:** Una aplicación bancaria debe brindar al usuario la seguridad de acceso para realizar transacciones de manera segura sin que peligre su información y los activos de su cuenta bancaria, para esto se deben implementar métodos de encriptación, certificados digitales, etc.
- **Funcionalidad:** el sistema debe permitir la fácil mantenibilidad además de ser interoperable con otras aplicaciones para esto se debe utilizar estándares como el ISO8583 que especifica las transacciones financieras bancarias para transmisión de datos. Además, ese debe ser altamente

disponible para que el usuario realice sus transacciones en cualquier momento

5.3 SISTEMA DE SEGURIDAD IMPLEMENTADO

El sistema de seguridad diseñado e implementado son de dos tipos de acuerdo a la clasificación que adquiere y estos se detallan a continuación:

5.3.1 Sistema de seguridad en Oficinas

5.3.1.1 Central de alarma

Una instalación se compone de ciertas partes básicas: central de alarma, sensores y sistemas de aviso y señalización. A estos se les puede sumar un cuarto elemento que sería el intercomunicador con la Central Receptora de Alarmas y que siempre es opcional su colocación en la instalación, aunque es absolutamente aconsejable su utilización.

La central de alarmas es la que recibe la señal eléctrica de los detectores o sensores que por algún motivo son activados. Al recibir esta señal, los circuitos electrónicos que lleva en su interior, hacen que se pongan en marcha el sistema de alarma y aviso.

Los sensores son elementos capaces de comprobar las variaciones de una condición de reposo en un lugar determinado y envían información de esa variación a la Central de Alarmas.

Son de reducido tamaño y se alimentan a través de una fuente de alimentación de baja tensión

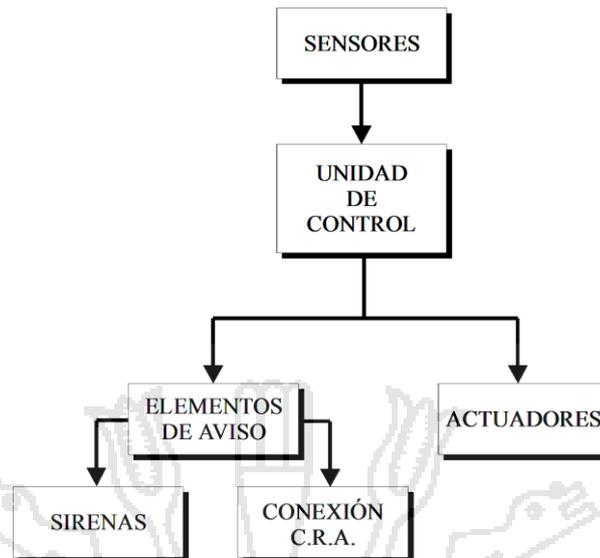


Figura N° 22: Esquema central de alarma

Fuente: Seguridad Bancaria

Elaborado: Por los Investigadores

Son de reducido tamaño y se alimentan a través de una fuente de alimentación de baja tensión

Para la realización de este proyecto de investigación después de varias pruebas con diferentes paneles de alarma se optó por usar el panel central de marca BOSCH en sus diferentes series D9412GV4, D7412GV4, D7212GV4.

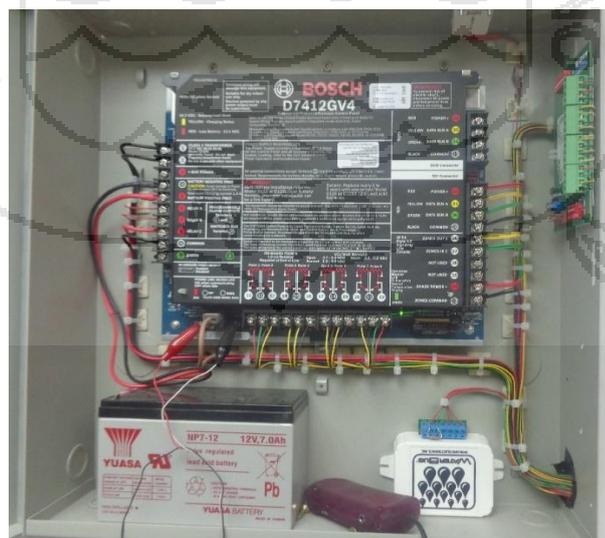


Figura N° 23: Panel de Control Bosch

Fuente: Imagen tomada 05/01/2015 Of. llave

Elaborado: Por los Investigadores

5.3.1.1.1 Características de una Central de Alarma

Las principales características de la central de alarmas se detallan a continuación:

a) **Conexión y desconexión:**

La central de alarmas dispone de mecanismos para controlar el acceso a las zonas protegidas, y efectuar su conexión y desconexión. Esta puede ser de distintos tipos: llave de seguridad, tarjeta codificada y teclado.

b) **Circuitos de detección:**

- **Circuito Retardado:**

En este circuito se conectarán los detectores que detecten al usuario del sistema al conectar la alarma y salir del inmueble, o bien para entrar y desconectar, sin que en ninguno de los dos casos se dispare la alarma.

- **Circuito instantáneo:**

Aquí se conectarán todos los detectores que no sean activados por el usuario al poner en marcha o desconectar el sistema.

En el momento que el detector o detectores conectados a este circuito observan una anomalía, el sistema se acciona inmediatamente, activando los sistemas de aviso instalados. Este circuito sólo funcionará con el sistema conectado o armado.

c) **Circuito Tamper:**

Este circuito tiene la finalidad de garantizar que no se produzca sabotaje o manipulación alguna en el sistema, durante la desconexión del mismo, como

por ejemplo, arrancar una sirena, abrir un volumétrico, etc., haciendo disparar la alarma cuando esto ocurra.

Por lo tanto, este circuito está permanentemente en vigilancia, aunque la alarma esta desconectada.

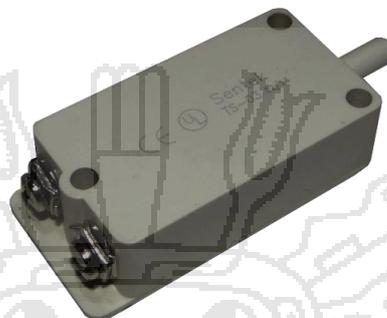


Figura N° 24: Circuito Tamper
Fuente: Hoja de datos de Dispositivos SEGURICENTRO
Elaborado: Por SEGURICENTRO

d) Zona cableada:

Circuito cerrado donde se han instalado y conexionado en serie los detectores.

Se diversifican en zonas para que en el momento de su activación se sepa el lugar exacto de ubicación.

No conviene instalar muchos detectores por zona, ya que cuando se active uno de ellos, sólo sabremos la zona activada. Sólo se suelen conectar unos tres detectores por zona

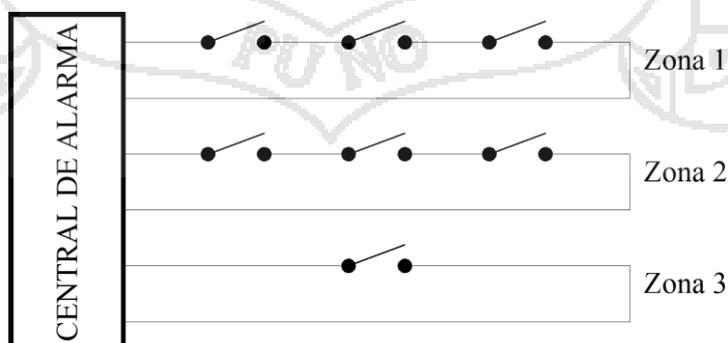


Figura N° 25: Zona Cableada
Fuente: Sensores y Actuadores en Microbótica
Elaborado: Por José Suarez

e) Zona multiplexada

Instalando en cada detector un pequeño módulo codificador, que introduce un código que sólo identificará la central de alarmas, permite instalar todos los detectores en una sola zona cableada, pero con la peculiaridad de que cuando sea activado algún detector, la central identificará al detector exacto activado.

Este sistema permite simplificar de forma considerable la instalación, a una sola tirada de dos cables, abaratando consecuentemente los costes de la instalación.

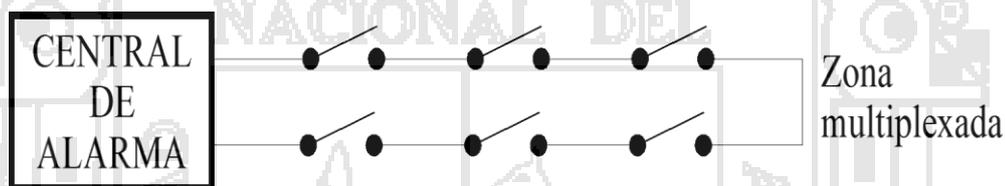


Figura Nº 26: Zona Multiplexada
Fuente: Sensores y Actuadores en Microbótica
Elaborado: Por José Suarez

f) Balanceo de línea

Es un sistema de protección para la instalación de detectores realizada. Consiste en colocar al final de las zonas cableadas una resistencia con un valor predeterminado y suministrado por el fabricante de la central, en serie con los detectores, cerrando de esta forma el circuito.

En el momento que por causas de manipulación externa, se modifica el valor óhmico de la instalación (cortocircuito en el cableado o en los detectores), la central detecta la modificación del mismo y hace activar la central.

Es un sistema en la práctica insaboteable, ya que un posible intruso no puede saber el valor de la resistencia para intentar cortar la tirada de detectores, colocando otra de igual valor, y aunque lo supiera, en el momento

del cambio, como tendría que cortar por breves mementos la línea (aunque sólo fueran décimas de segundo), se activaría la alarma. Si intenta colocar otra resistencia en paralelo, se modificaría el valor general de la línea, con lo que igualmente es activada la alarma.

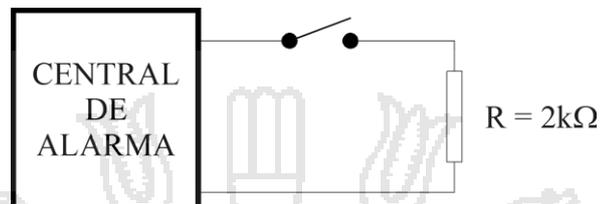


Figura Nº 27: Circuito balanceo de Línea
Fuente: Sensores y Actuadores en Microbótica
Elaborado: Por José Suarez

g) Programación por tiempos

Nos permite programar los tiempos de activación de las zonas. Pueden programarse zonas de activación no instantánea, en las que por necesidad de paso del usuario para entrar o para desactivar o activar la alarma, les sea necesario un tiempo determinado.

Este tiempo puede variar desde varios segundos a varios minutos dependiendo de las características de la instalación de la alarma.

h) Conexión con Central Receptora de Alarmas.

Por medio de un circuito electrónico, marca automáticamente el número de teléfono programado de la central receptora de alarma para su comunicación con ella.

La conexión que efectúe la central puede variar desde la comunicación de existencia de alarma, a otras como las de situación de atraco.

Los sistemas comunican cualquier incidencia del sistema a la central receptora, activación y desactivación de la central, activación de zonas o de detectores, etc.).

Igualmente se puede utilizar la conexión telefónica desde la central receptora al sistema concreta, para realizar cualquier variación deseada en la programación de la central de alarmas, o para pedirle datos como el estado actual, incidencias producidas, etc.

5.3.1.2 Circuito cerrado de televisión

El sistema de vigilancia por circuito cerrado de televisión (CCTV) consta de un conjunto de dispositivos que permiten captar y enviar datos (imágenes y sonidos) desde la zona vigilada a los lugares donde elija el cliente con el objetivo de controlar y proteger un espacio definido.

Cada sistema de acuerdo con sus espacios y usos debe tener las cámaras aplicables a ese entorno. El criterio de selección involucra ciertos parámetros a tomar en cuenta tales como: sensibilidad, resolución y capacidad para aislar el ruido en la señal.

Todo el sistema está desarrollado para cubrir las zonas más vulnerables, internas y externas, además de tener todo el equipamiento de video grabación en forma centralizada en un solo punto, para de esta forma derivar las conexiones de monitoreo a los sitios dispuestos por la agencia de Caja Rural – Los Andes S.A.

- Diseño de arquitectónico definido
- Ubicación de equipos
- Recorridos
- Materiales

5.3.2 Sistema de seguridad en PAC

Se desarrolló un sistema básico de seguridad que cumpla con lo requerido para el funcionamiento de dichos PAC.

En la figura N° 28 se muestra el funcionamiento básico de este sistema de seguridad implementado en el PAC de Macari.



Figura N° 28: Funcionamiento de Alarma en PAC
Fuente: Sistema de Seguridad Implementado
Elaborado: Por los Investigadores

5.3.2.1 Distribución del sistema de alarma

Por ser reducido el espacio en estos PAC, se usan una cantidad mínima de sensores y dispositivos electrónicos.

La distribución de dichos dispositivos se muestra en la figura N° 29.

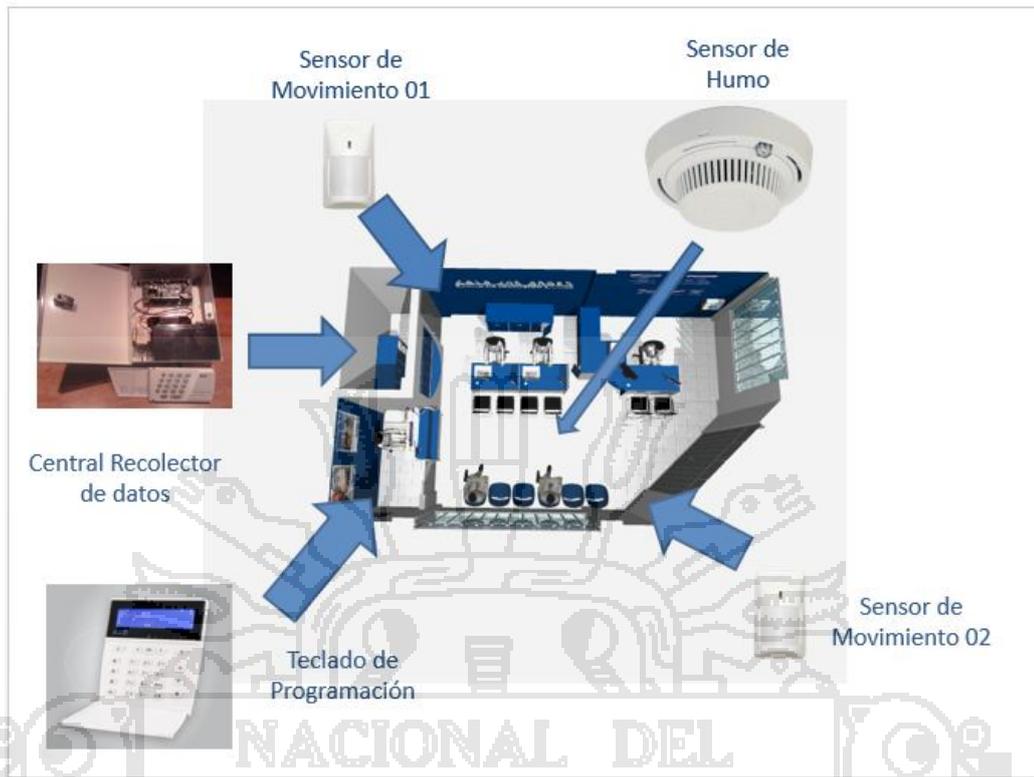


Figura Nº 29: Ubicación de dispositivos
Fuente: Sistema de Seguridad Implementado
Elaborado: Por los investigadores

Como este establecimiento realiza operaciones básicas, se tiene que asegurar ventanilla con los requisitos mínimos de seguridad.

La distribución de estos dispositivos de seguridad en ventanilla se muestra en la figura Nº 30.



Figura Nº 30: Dispositivos de Seguridad en Ventanilla
Fuente: Sistema de Seguridad Implementado
Elaborado: Por los Investigadores

5.3.2.2 Distribución del CCTV

Este punto de atención al cliente también cuenta con un kit básico de circuito cerrado de televisión, la disposición de las cámaras se muestran en la figura N° 31.

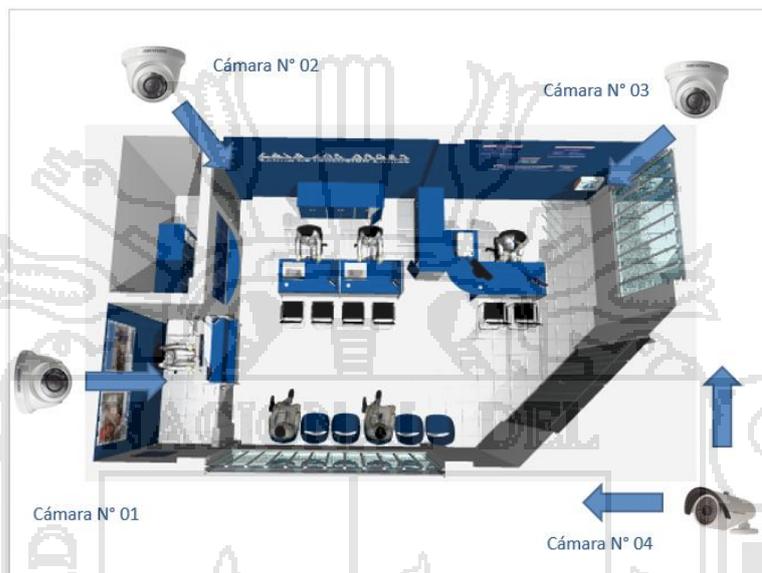


Figura N° 31: Ubicación de las Cámaras
Fuente: Sistema de Seguridad Implementado
Elaborado: Por los Investigadores

5.4 DISPOSITIVOS ELECTRONICOS UTILIZADOS

Los dispositivos electrónicos utilizados son:

5.4.1 Panel central Bosch

Para la realización de esta investigación se optó por usar el panel de alarma central marca Bosch por presentar mayores beneficios a la hora de implementar el sistema de seguridad.

Esta marca de paneles muestra una amplia posibilidad de conexión ya sea de por línea telefónica, red celular, conexión a la red o internet. En la tabla N° 8 se muestra las diferentes características básicas que presenta las diferentes versiones de estos paneles.

Características	D9412GV4	D7412GV4	D7212GV4
Control de Acceso	yes - 8 doors	Yes - 2 doors	No
Códigos de Acceso (Armado / Desarmado)	999	399	99
Tarjetas	999	399	N/A
Funciones personalizadas protegida (Contraseña)	16	4	4
Número de puntos	246	75	40
Número de relés fuera de placa	128	64	24
Número de Áreas	32	8	4
Número de Teclados D1255(Bòveda)	16	16	8
Número de Teclados D1260(Princ)	8	8	8
Número de líneas de teléfono compatibles	2	2	1

Tabla N° 8: Características de los paneles Bosch

Fuente: Hoja de Datos equipos Bosch

Elaborado: Por los Investigadores

En la figura N° 32 se muestra el panel central Bosch instalado en la oficina de llave.

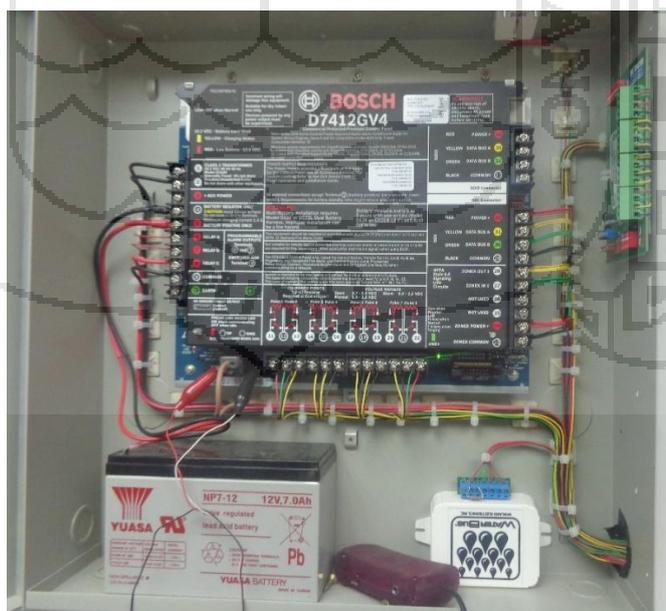


Figura N° 32: Panel de Alarma Oficina llave

Fuente: Imagen tomada 05/01/2015 Of. llave

Elaborado: Por los Investigadores

En la figura N° 33 se muestra una rápida y breve descripción del panel central de alarma, donde se observa que brinda bastante zona de programación y bastantes salidas rele.

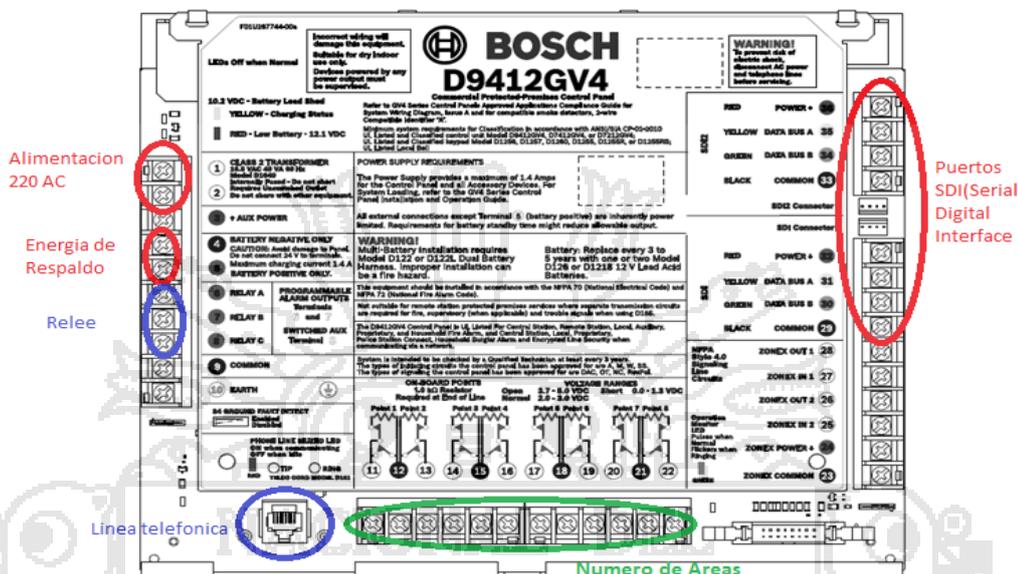


Figura N° 33: Descripción del Panel
Fuente: Hoja de Datos equipos BOSCH
Elaborado: Por los Investigadores

Para mayor información respecto al panel central de alarma, especificaciones técnicas, número total de zonas programables, etc. se puede recurrir al datasheet del producto.

5.4.2 Tarjetas Expansoras

El Modulo de Expansión D8125 POPEX, se utiliza para multiplexar y así obtener el control de más zonas con un solo panel y tener bien identificados los sensores y en qué zonas se encuentran.

Instalando en cada detector un pequeño módulo codificador, que introduce un código que sólo identificará la central de alarmas, permite instalar todos los detectores en una sola zona cableada, pero con la peculiaridad de que cuando sea activado algún detector, la central identificará al detector exacto activado.

El método de conexión para la utilización de este módulo de expansión se muestra en la figura N° 34.

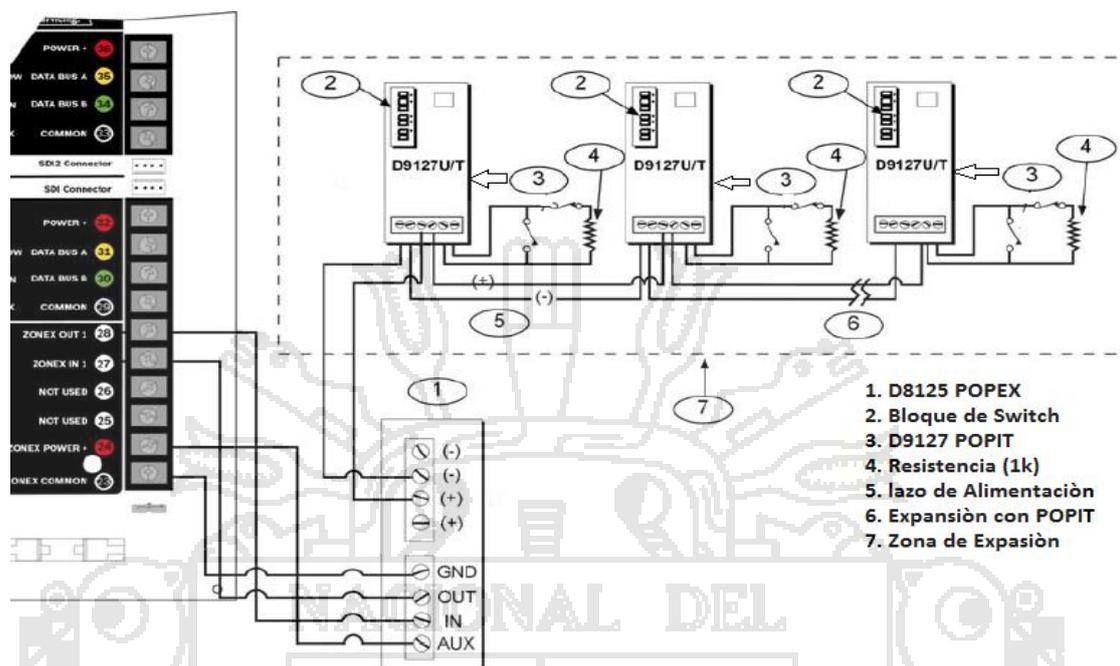


Figura N° 34: Conexión tarjetas expansoras
Fuente: Hoja de Datos equipos BOSCH
Elaborado: Por los Investigadores

5.4.3 Sensor de movimiento

Los sensores de movimiento se ajustan excepcionalmente a las aplicaciones comerciales en interiores. La tecnología de fusión de datos de los sensores garantiza que los sensores envíen condiciones de alarma basadas en información precisa. La potente combinación de características únicas de la serie Professional proporciona un nivel de detección superior y elimina prácticamente las falsas alarmas.

La carcasa de protección en dos piezas con auto bloqueo, la burbuja de nivel orientable integrada, la altura de montaje flexible y los tres soportes de montaje opcionales simplifican la instalación y reducen el tiempo de un mantenimiento.

El patrón de cobertura del sensor se muestra en a figura N° 35, los demás datos técnicos se pueden obtener en la hoja de datos del fabricante o datasheet.

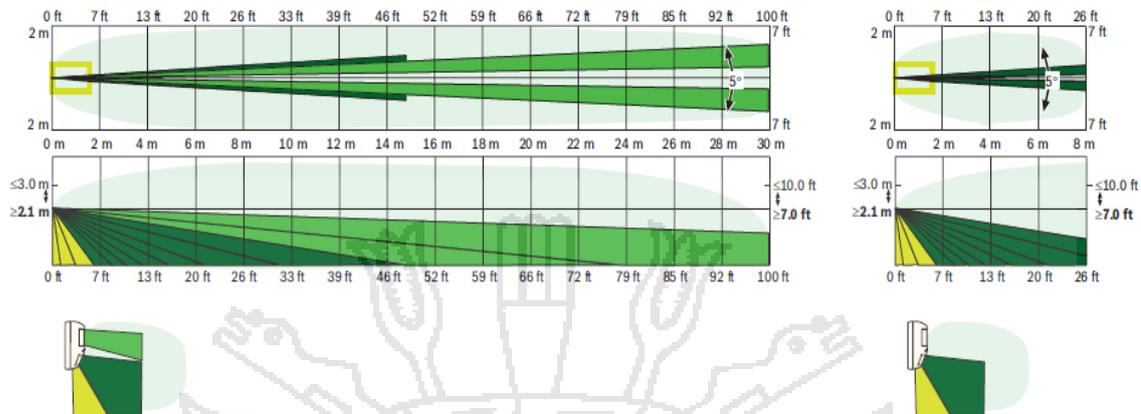


Figura N° 35: Cobertura de un sensor PIR

Fuente: Hoja de datos PIR

Elaborado: Por seguricentro

5.4.4 Detector de humo

Estos modelos de detectores usan una fuente de luz LED infrarroja (IR) y un fotodiodo de silicón para medir la luz en una cámara. Una delgada pantalla cubre la cámara para impedir el ingreso de insectos y reducir la acumulación de polvo, y así minimizar las falsas alarmas.

Durante un incendio, las partículas de humo reflejan la luz en el fotodiodo. Cuando las mediciones del fotodiodo superan el umbral de alarma, el detector emite una señal que indica la presencia de una condición de alarma.

Una vez despejada la condición de alarma, interrumpa el suministro de energía en el panel de control para restablecer el detector. Cuando se usa un módulo de inversión de relé D132B, la luz de LED no bloquea la alarma¹.

¹http://resource.boschsecurity.us/documents/Datasheet_D273_Famil_Data_sheet_esAR_2700896011.pdf

5.4.5 Sensores de Ruptura de Vidrios

Es un potente microprocesador basado en la ruptura acústica de vidrios, su avanzado diseño ayuda a descartar cualquier tipo de falsas alarmas, gracias al rápido procesamiento y al testeado continuo.

El rango de acción o funcionamiento en base al espesor del vidrio y a la distancia entre el sensor y el vidrio se detalla en la figura N° 36, de acuerdo a la serie utilizada se puede obtener mejores rendimientos.

El sensor usado para estos fines es de la marca Vitron y de la serie RG 71, este muestra mejor desempeño que los otros y su campo de acción es mayor que los demás.

Typ of Glass Model	Plate			Tempered, Laminated, Wired		
	Size	Thickness	Max. Range	Size	Thick ness	Max. Range
RG70 RG70FM	Minimum 30x30cm (12"x12")	3.2- 6.4mm (1/8"-1/4")	4.5m (15ft)	Minimum 30x30cm (12"x12")	6.4mm (1/4")	3m (10ft)
RG71 RG71FM	Minimum 50x50 cm (20"x20") Minimum 30x30cm (12"x12")	3.2- 6.4mm (1/8"-1/4")	9m (30ft) 6m (20ft)	Minimum 30x30cm (12"x12")	6.4mm (1/4")	6m (20ft)

Figura N° 36: Características del sensor de ruptura
 Fuente: Hoja de datos del dispositivo
 Elaborado: Por seguricentro

En la figura N° 37 y 38, se muestra el campo de visión de acuerdo al ángulo en el que se encuentra posicionado.

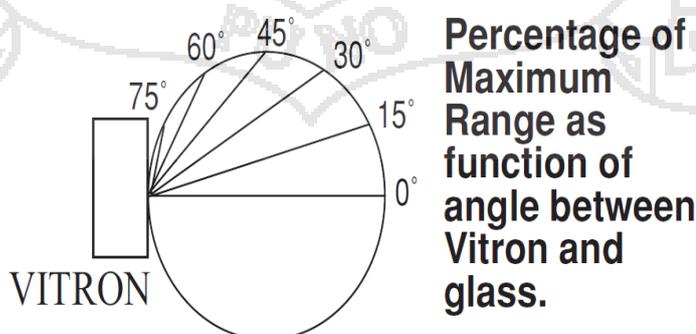


Figura N° 37: Ángulos de funcionamiento
 Fuente: Hoja de datos del dispositivo
 Elaborado: Por seguricentro

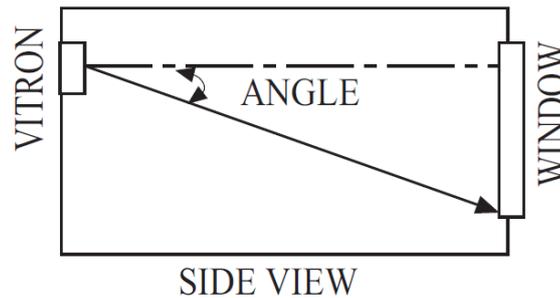


Figura Nº 38: Posición del sensor de ruptura
Fuente: Hoja de datos del dispositivo
Elaborado: Por seguricentro

5.4.6 Receptor pasarela de comunicaciones

El receptor/pasarela de comunicaciones Conettix D6600 con componentes de hardware Conettix IP funciona con las siguientes configuraciones:

- Comunicaciones por línea telefónica en la red telefónica conmutada pública (RTC).
- Comunicaciones en Internet o intranet en una red LAN o WAN mediante el protocolo de datagrama de usuario y protocolo de Internet (UDP/IP) estándar.
- Comunicaciones simultáneas por RTC y LAN o WAN.

El entorno de red disminuye el tiempo que tarda en informarse sobre la señal y ofrece una notificación instantánea si el sitio se ve afectado por problemas de comunicación.

Un dispositivo D6600 con hardware Conettix IP es compatible con los paneles de control de incendios y de seguridad de la mayoría de fabricantes. Con los paneles de control de Bosch Security Systems, también se puede conseguir una programación remota de alta velocidad en la red.

5.5 MEDIOS DE COMUNICACIÓN

En la comunicación de nuestro sistema alarma con la central de monitoreo, se usó las distintas redes públicas que se ofrecen en nuestro país.

Y con la variedad de soluciones en interconexión que nos brinda el panel central de alarmas Bosch se considera a los siguientes tipos de comunicación, por ser estos conocidos y brindar mejor respuesta para las necesidades de las diferentes agencias según la tabla N° 7.

5.5.1 Comunicación por Red Telefónica Conmutada (RTC)

La Red Telefónica Conmutada(RTC), se define como el conjunto de elementos constituido por todos los medios de transmisión y conmutación necesarios para enlazar a voluntad dos equipos terminales mediante un circuito físico que se establece específicamente para la comunicación y que desaparece una vez que se ha completado la misma. Se trata por tanto, de una red de telecomunicaciones conmutada.

- **Funciones:** El servicio de identificación de números marcados (DNIS) regula los ajustes de la tarjeta de líneas en función del número de teléfono marcado por el panel de control.

El procesamiento de alarmas por identificación de llamada (ID de llamada) almacena los protocolos de intercambio correspondientes. El procesamiento recupera automáticamente los formatos cuando se procesa la misma identificación de llamada.

- **Configuración de las comunicaciones RTC:** Esta configuración utiliza líneas telefónicas existentes. La señal de un panel de control se transmite por una línea telefónica analógica RTC al receptor D6600. El dispositivo

D6600 convierte la señal a un formato de datos común y la envía por una red LAN Ethernet, WAN RS-232 a un sistema de automatización de centrales receptoras de alarmas.

- **Ventajas:** Gestiona más comunicadores de campo con menos tarjetas de líneas y le permite crear líneas virtuales.

Reduce el período de tiempo que las llamadas permanecen conectadas al receptor. Reduce el gasto económico en hardware fijo o en las facturas telefónicas mensuales.

En la figura N° 39, se muestra como debería de ser una central de monitoreo implementada con el método de comunicación RTC.

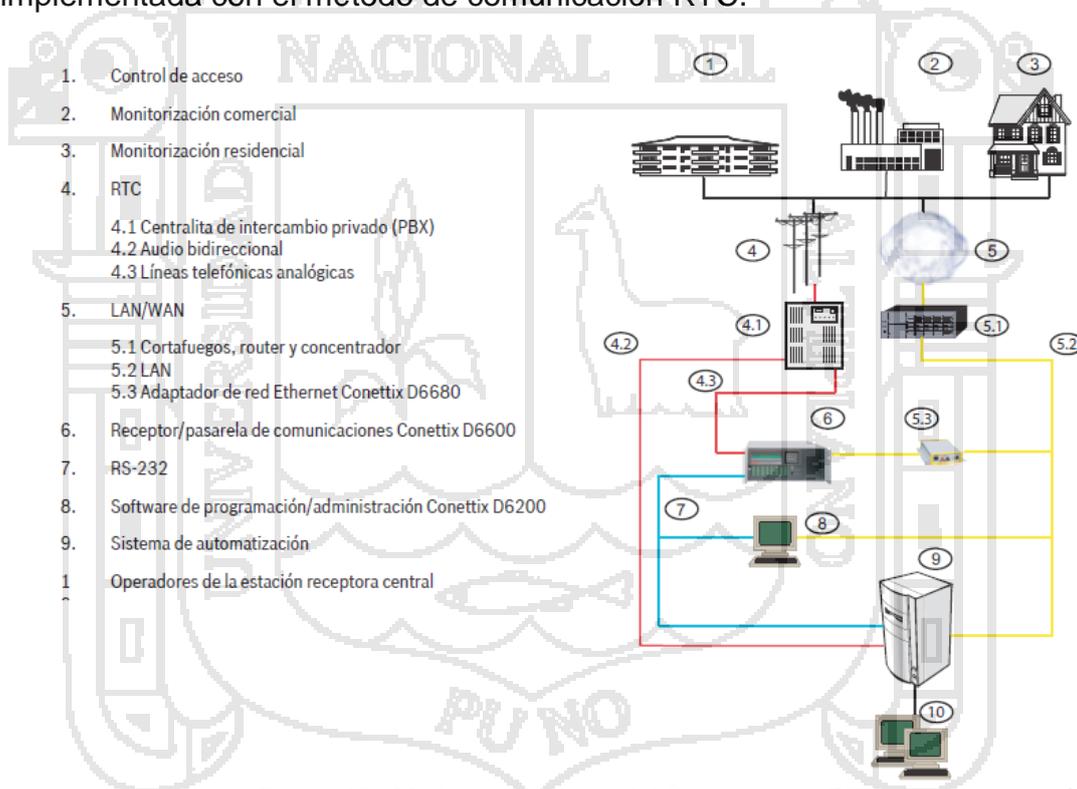


Figura N° 39: Interconexión del Sistema por RTC
Fuente: Sensores y Actuadores en Microbotica
Elaborado: Por los Investigadores

Los formatos de comunicación que se pueden usar por la RTC

- Acron Superfast
- Ademco Slow

- Ademco Express
- ROBOFON
- Scantronics Scancom
- SERIEE FSK/DTMF

Mediante cualquiera de estos formatos se puede lograr comunicación, solo dependería del diseñador que formato de comunicación logra usar dentro del RTC.

5.5.2 Comunicación por Red o Celular

Teniendo como medio de comunicación la RTC, el siguiente paso en la investigación es la interconexión por Red, el cual implica un gran reto por el mismo ámbito de trabajo de la empresa.

Adicionando el módulo Ethernet de captura del comunicador Conettix C900V2 funciona con la mayoría de los paneles de control mediante un formato de comunicador digital estándar y proporciona seguridad integral. El módulo enlaza el comunicador digital a la red telefónica conmutada pública (PSTN, Public Switched Telephone Network), la interfaz telefónica del comunicador digital y a una red Ethernet. Con el enlace Ethernet, el módulo C900V2 puede:

- Establecer comunicación con el comunicador del panel de control.
- Descodificar y enviar señales a un receptor/pasarela de comunicaciones Conettix D6600.
- Devolver un mensaje de confirmación al comunicador del panel de control

Los datos no cambian aunque el panel de control se comunique a través de una línea telefónica o del módulo C900V2. El módulo C900V2 autoriza a los paneles de control del comunicador digital a funcionar a través de una red IP como una red de área local (LAN, Local Area Network), una red de área extendida (WAN, Wide Area Network) o Internet.

Captura datos de alarmas y eventos de paneles de control basados en comunicadores a través de CONTACT ID, SIA, Modem II, Modem IIe, Modem IIIa2, Pulse y otros formatos.

- **Funcionamiento:** Cuando el comunicador tiene un mensaje que comunicar, el módulo C900V2 simula un marcado por tono y tensiones de línea, haciendo que el comunicador se comporte como si estuviera conectado a un receptor digital de una central receptora de alarmas a través de la RTC.

El módulo C900V2 descodifica y convierte a datos el mensaje que ha transmitido el comunicador para enviarlos a través de cualquier red UDP/IP. Después de que el receptor/pasarela de comunicaciones Conettix D6600 reciba un mensaje o evento, enviará un mensaje de confirmación al dispositivo C900V2. El dispositivo C900V2 devuelve una respuesta pertinente al comunicador, manteniendo la confirmación de principio a fin.

El dispositivo C900V2 funciona en modo de interceptación, conectando el comunicador a la red bajo circunstancias normales. Si el dispositivo C900V2 pierde el contacto con el receptor/pasarela de

Presupuesto de Alarma Electrónica - Macari					
Ítem	Cantidad	Unidad	Descripción	Precio Ref. \$	Sub total \$
1	1	Und.	Teclado de Programación	60	60
2	1	Und.	Batería 12v - 1.2Amperios	40	40
3	1	Und.	Sirena de 12v - 50w	60	60
4	2	Und.	Sensor PIR Detector de Movimientos	70	140
5	1	Und.	Sensor Magnético	30	30
6	1	Und.	Sensor de Humo	70	70
7	1	Und.	Central de Alarmas	300	300
8	20	Mts.	Cable de conexión	1.5	30
9	1	Und.	Chip - Movistar o Claro	10	10
			Instalación - Mano de Obra	120	120
			Sub total - Incluye IGV		860
			TOTAL		860

Tabla Nº 9: Costos del sistema de alarma en PAC

Fuente: Catalogo Seguricentro

Elaborado: Por los Investigadores

El proyecto resulta económicamente factible por que el sistema instalado cubre las necesidades básicas de seguridad, a veces con ciertas limitaciones pero se debe a las inclemencias de la naturaleza.

5.6.2 Oficinas

El costo, en sistemas de seguridad en esta oficina fue relativamente bajo puesto que la compra se hizo directamente con un proveedor en Lima, el cual brindo los sensores y paneles a bajo costo, los costos se muestran en la tabla Nº 10.

También se realizó un ahorro significativo en mano de obra, puesto que los ejecutores realizaron dichas labores de instalación.

ITEM	CODIGO	DESCRIPCION	CANT.	P.UNIT. \$	P.TOTAL \$
1	NEO-DT-AM	PIR ANTIMASKING OPTICO INMUNE MASCOTAS HASTA 25 KG. CROW	5	\$46.61	\$233.05
2	RK-815DTG3	PIR INFROROJO CON ANTICLOAK MARCA RISCO	3	\$80.51	\$241.53
3	BKT-38	SOPORTE PLASTICO PARA PIR UNIVERSAL	8	\$2.54	\$20.32
4	RK-150DTG3	PIR DE TECHO CON MICROONDAS MARCA CROW	1	\$97.46	\$97.46
5	D-273TH	DETECTOR DE HUMO FOTOE. + TEMP. MARCA BOSCH	9	\$33.90	\$305.10
6	RK-600S	DETECTOR DE GOLPE DIGITAL SHOCKTEC MARCA RISCO	6	\$23.73	\$142.38
7	SM-226L	SENSOR MAGNETICO PESADO MARCA SECO LARM	2	\$13.98	\$27.96
8	SM-217	SENSOR MAGNETICO LIVIANO MARCA SECO LARM	2	\$3.05	\$6.10
9	HUB-2B	BOTON PULSADOR DE EMERG. CON RETENCION	4	\$19.49	\$77.96
10	WT-101	PULSADOR INALAMBRICO DE 1 CANAL MARCA VISONIC	1	\$25.42	\$25.42
11	WR-200	RECEPTOR INALAMBRICO DE 1 CANAL MARCA VISONIC	1	\$42.37	\$42.37
12	W-HSR	FLASH ESTROBOSCOPICO CON SIRENA MARCA BOSCH	1	\$52.54	\$52.54
13	FMM-100SAT	ESTACION MANUAL DE INCENDIO MARCA BOSCH	1	\$22.88	\$22.88
14	RG-71GM	DISCRIMINADOR DE AUDIO MARCA RISCO	2	\$29.66	\$59.32
15	TY-580S	SIRENA ELECTRONICA DE 30 WATTS MOD. TY580S	1	\$11.86	\$11.86
16	EAP-5D1MQ	FUENTE DE PODER DE 5 AMP. MARCA SECO LARM + GAB.	1	\$102.55	\$102.55
17	CAJ-MET	CAJA METALICA PARA EXPANSOR	2	\$10.17	\$20.34
18	SS-072	TAMPER SWITH PARA GABINETE MARCA SECO LARM	3	\$2.54	\$7.62
19	YUA-1270	BATERIA DE 12 VOLTS. 7.0 AMP. MARCA YUASA	2	\$29.66	\$59.32
20	D-7212G-V4	CENTRAL DE ALARMA DE 8 A 40 ZONAS MARCA BOSCH	1	\$177.12	\$177.12
21	D-1260	BOTONERA ALFANUMERICA MARCA BOSCH MOD. D-1260	1	\$127.12	\$127.12
22	D-720	BOTONERA DE LED MARCA BOSCH MOD. D-720	1	\$50.85	\$50.85
23	D-8128D	EXPANSOR OCTOPOBIT DE 8 ZONAS MARCA BOSCH	3	\$23.73	\$71.19
24	TR-3.0 AMP.	TRANSFORMADOR DE 220-16 DE 3.0 AMP.	1	\$11.86	\$11.86
25	D-8103	GABINETE METALICO PARA CENTRAL MARCA BOSCH	1	\$40.68	\$40.68
26	D-101	CERRADURA C/LLAVE PARA CENTRAL BOSCH MOD. D-101	1	\$2.54	\$2.54
27	B-426	INTERFACE PARA REDES MARCA BOSCH MOD. B-426	1	\$193.22	\$193.22
				SUB TOTAL	\$2,230.66
				I.G.V. 18%:	\$401.52
				TOTAL\$	\$2,632.18

Tabla Nº 10: Costo del Sistema de alarma en Oficinas
Fuente: Catalogo Seguricentro
Elaborado: Por los Investigadores

5.7 CONTRASTACION

El sistema de alarma funciona correctamente y las 24 horas del día, registrando todos los incidentes que se puedan presentar en el transcurrir de las labores diarias en las respectivas agencias que se tomaron como muestra según la tabla Nº 7.

En las tablas N° 11 y 12, nuestra base de datos elaborada en Excel el cual registra todas las aperturas y cierres de las agencias, en este caso la tabla N° 11 pertenece a la Oficina llave.

Oficina	Fecha	Hora	ID Señal	Evento	Condición	Descrip. Condic.
ILAVE	02-05-2014	08:48:17	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	02-05-2014	14:38:53	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	04-05-2014	08:49:51	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	04-05-2014	19:19:59	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	05-05-2014	08:48:48	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	05-05-2014	19:21:53	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	06-05-2014	08:48:24	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	06-05-2014	20:47:17	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	07-05-2014	08:46:36	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	08-05-2014	08:46:44	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	08-05-2014	20:18:25	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	09-05-2014	08:45:14	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	09-05-2014	14:57:24	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	11-05-2014	08:49:20	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	11-05-2014	14:01:47	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	12-05-2014	08:48:59	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	12-05-2014	20:21:56	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	13-05-2014	08:46:36	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	13-05-2014	19:52:35	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	14-05-2014	08:41:26	O	0002	IO*	Apertura Horario no Establecid
ILAVE	14-05-2014	20:07:01	C	0002	CAG	ACTIVACION DE AGENCIA

Oficina	Fecha	Hora	ID Señal	Evento	Condición	Descrip. Condic.
ILAVE	02-05-2014	08:48:17	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	02-05-2014	14:38:53	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	04-05-2014	08:49:51	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	04-05-2014	19:19:59	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	05-05-2014	08:48:48	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	05-05-2014	19:21:53	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	06-05-2014	08:48:24	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	06-05-2014	20:47:17	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	07-05-2014	08:46:36	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	08-05-2014	08:46:44	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	08-05-2014	20:18:25	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	09-05-2014	08:45:14	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	15-05-2014	08:48:42	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	15-05-2014	19:45:29	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	16-05-2014	08:49:21	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	16-05-2014	14:19:57	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	18-05-2014	08:46:44	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	18-05-2014	19:09:08	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	19-05-2014	08:48:26	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	19-05-2014	20:34:39	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	20-05-2014	08:48:27	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	20-05-2014	19:13:16	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	21-05-2014	08:46:25	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	21-05-2014	19:58:29	C	0002	CAG	ACTIVACION DE AGENCIA

Oficina	Fecha	Hora	ID Señal	Evento	Condición	Descrip. Cond.
ILAVE	02-05-2014	08:48:17	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	02-05-2014	14:38:53	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	04-05-2014	08:49:51	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	04-05-2014	19:19:59	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	05-05-2014	08:48:48	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	05-05-2014	19:21:53	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	06-05-2014	08:48:24	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	06-05-2014	20:47:17	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	07-05-2014	08:46:36	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	08-05-2014	08:46:44	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	08-05-2014	20:18:25	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	09-05-2014	08:45:14	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	22-05-2014	08:46:30	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	22-05-2014	19:41:42	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	23-05-2014	08:46:34	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	23-05-2014	14:56:12	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	25-05-2014	08:45:30	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	25-05-2014	20:00:34	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	26-05-2014	08:45:43	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	26-05-2014	20:06:18	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	27-05-2014	08:46:36	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	27-05-2014	19:47:58	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	28-05-2014	08:46:56	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	28-05-2014	19:59:49	C	0002	CAG	ACTIVACION DE AGENCIA

Oficina	Fecha	Hora	ID Señal	Evento	Condición	Descrip. Condic.
ILAVE	02-05-2014	08:48:17	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	02-05-2014	14:38:53	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	04-05-2014	08:49:51	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	04-05-2014	19:19:59	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	05-05-2014	08:48:48	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	05-05-2014	19:21:53	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	06-05-2014	08:48:24	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	06-05-2014	20:47:17	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	07-05-2014	08:46:36	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	08-05-2014	08:46:44	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	08-05-2014	20:18:25	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	09-05-2014	08:45:14	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	29-05-2014	08:54:49	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	29-05-2014	20:14:07	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	30-05-2014	08:54:09	O	0002	OAG	DESACTIVACION DE AGENCIA
ILAVE	30-05-2014	23:32:29	C	0002	CAG	ACTIVACION DE AGENCIA
ILAVE	31-05-2014	08:21:10	O	0002	IO*	Apertura Horario no Establecid
ILAVE	31-05-2014	20:00:46	C	0002	CAG	ACTIVACION DE AGENCIA

Tabla N° 11: Apertura y Cierre de la Oficina llave

Fuente: Panel de Alarma BOSCH

Elaborado: Por los Investigadores

La siguiente tabla N° 12 muestra la base de datos elaborada en Excel el cual registra todas las aperturas y cierres de las agencias, en este caso pertenece a la Oficina Coata.

Oficina	Fecha	Hora	ID Señal	Evento	Condición	Descrip. Cond.
COATA	09-05-2014	18:55:01	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	12-05-2014	08:48:10	E401	001	OAG	DESACTIVACION DE AGENCIA
COATA	12-05-2014	18:55:12	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	13-05-2014	08:39:55	E401	001	IO*	Apertura Horario no Establecid
COATA	13-05-2014	19:01:46	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	14-05-2014	08:42:19	E401	001	IO*	Apertura Horario no Establecid
COATA	14-05-2014	19:03:01	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	15-05-2014	21:48:34	E401	001	IO*	Apertura Horario no Establecid
COATA	15-05-2014	08:42:40	E401	001	IO*	Apertura Horario no Establecid
COATA	15-05-2014	21:51:25	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	15-05-2014	19:08:07	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	16-05-2014	08:37:56	E401	001	IO*	Apertura Horario no Establecid
COATA	16-05-2014	19:05:38	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	17-05-2014	09:12:25	E401	001	IO*	Apertura Horario no Establecid
COATA	17-05-2014	13:29:43	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	19-05-2014	08:44:14	E401	001	IO*	Apertura Horario no Establecid
COATA	19-05-2014	20:39:18	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	20-05-2014	08:43:39	E401	001	IO*	Apertura Horario no Establecid
COATA	20-05-2014	19:27:38	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	21-05-2014	08:48:38	E401	001	OAG	DESACTIVACION DE AGENCIA
COATA	21-05-2014	18:53:03	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	22-05-2014	08:44:51	E401	001	IO*	Apertura Horario no Establecid
COATA	22-05-2014	18:58:39	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	23-05-2014	08:41:52	E401	001	IO*	Apertura Horario no Establecid

Oficina	Fecha	Hora	ID Señal	Evento	Condición	Descrip. Cond.
COATA	09-05-2014	18:55:01	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	12-05-2014	08:48:10	E401	001	OAG	DESACTIVACION DE AGENCIA
COATA	12-05-2014	18:55:12	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	13-05-2014	08:39:55	E401	001	IO*	Apertura Horario no Establecid
COATA	23-05-2014	19:35:45	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	24-05-2014	09:18:12	E401	001	OAG	DESACTIVACION DE AGENCIA
COATA	24-05-2014	13:32:34	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	26-05-2014	08:44:40	E401	001	IO*	Apertura Horario no Establecid
COATA	26-05-2014	19:03:27	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	27-05-2014	08:44:03	E401	001	IO*	Apertura Horario no Establecid
COATA	27-05-2014	19:29:22	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	28-05-2014	08:49:17	E401	001	OAG	DESACTIVACION DE AGENCIA
COATA	28-05-2014	19:09:21	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	29-05-2014	19:32:41	E401	001	IO*	Apertura Horario no Establecid
COATA	29-05-2014	19:33:44	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	29-05-2014	19:32:37	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	30-05-2014	08:38:17	E401	001	IO*	Apertura Horario no Establecid
COATA	30-05-2014	19:47:17	R401	001	CAG	ACTIVACION DE AGENCIA
COATA	31-05-2014	09:09:40	E401	001	IO*	Apertura Horario no Establecid
COATA	31-05-2014	13:55:46	R401	001	CAG	ACTIVACION DE AGENCIA

Tabla N° 12: Apertura y Cierra de la Oficina Coata

Fuente: Panel de Alarma BOSCH

Elaborado: Por los Investigadores

Como se observa en las tablas N° 11 y 12, el sistema de alarma funciona las 24 horas del día, y reporta cualquiera incidente dentro o fuera del horario de atención al público.

Observando los datos de las tablas N° 11 y 12 se valida la hipótesis específica 02, que nos planteamos para la investigación, puesto que la oficina de llave cuenta con una comunicación de red telefónica (RTC), donde se observa que la frecuencia con la que reporta el número de incidentes de la agencia es mejor y más amplia que de la oficina de Coata.

Para validar la hipótesis específica 01, se divide la agencia en 2 partes, partición bóveda y partición agencia, esto implica tener un panel de acceso principal en agencia y otro teclado de acceso en lo que es puerta de bóveda.

En la tabla N° 13 se muestra, la base de datos de cierre y apertura de la partición de bóveda, el cual se usa un sistema dual al receptor pagador se le proporciona clave de acceso a bóveda y al coordinador de operación se le brinda llave de bóvedas y claves de caja buzón.

Oficina	Fecha	Hora	ID Señal	Evento	Descrip. Condi.
ILAVE	02-05-2014	14:21:28	C	0004	ACTIVAN
ILAVE	02-05-2014	09:03:08	C	0004	ACTIVAN
ILAVE	02-05-2014	08:58:05	O	0004	Apertura Horario no Establecid
ILAVE	02-05-2014	14:18:38	O	0004	DESACTIVAN
ILAVE	04-05-2014	19:01:59	C	0004	ACTIVAN
ILAVE	04-05-2014	09:29:33	C	0004	ACTIVAN
ILAVE	04-05-2014	08:56:23	O	0004	Apertura Horario no Establecid
ILAVE	04-05-2014	15:15:03	O	0004	DESACTIVAN
ILAVE	05-05-2014	19:11:38	C	0004	ACTIVAN
ILAVE	05-05-2014	09:00:21	O	0004	DESACTIVAN
ILAVE	06-05-2014	18:44:40	C	0004	ACTIVAN
ILAVE	06-05-2014	09:11:00	C	0004	ACTIVAN
ILAVE	06-05-2014	08:55:30	O	0004	Apertura Horario no Establecid
ILAVE	06-05-2014	18:43:04	O	0004	DESACTIVAN
ILAVE	07-05-2014	08:58:24	O	0004	Apertura Horario no Establecid
ILAVE	08-05-2014	20:07:20	C	0004	ACTIVAN
ILAVE	08-05-2014	09:04:23	O	0004	DESACTIVAN
ILAVE	09-05-2014	14:31:07	C	0004	ACTIVAN

Oficina	Fecha	Hora	ID Señal	Evento	Descrip. Condic.
ILAVE	02-05-2014	14:21:28	C	0004	ACTIVAN
ILAVE	02-05-2014	09:03:08	C	0004	ACTIVAN
ILAVE	02-05-2014	08:58:05	O	0004	Apertura Horario no Establecid
ILAVE	02-05-2014	14:18:38	O	0004	DESACTIVAN
ILAVE	04-05-2014	19:01:59	C	0004	ACTIVAN
ILAVE	04-05-2014	09:29:33	C	0004	ACTIVAN
ILAVE	04-05-2014	08:56:23	O	0004	Apertura Horario no Establecid
ILAVE	04-05-2014	15:15:03	O	0004	DESACTIVAN
ILAVE	05-05-2014	19:11:38	C	0004	ACTIVAN
ILAVE	05-05-2014	09:00:21	O	0004	DESACTIVAN
ILAVE	06-05-2014	18:44:40	C	0004	ACTIVAN
ILAVE	06-05-2014	09:11:00	C	0004	ACTIVAN
ILAVE	06-05-2014	08:55:30	O	0004	Apertura Horario no Establecid
ILAVE	06-05-2014	18:43:04	O	0004	DESACTIVAN
ILAVE	09-05-2014	08:56:02	O	0004	Apertura Horario no Establecid
ILAVE	11-05-2014	13:50:40	C	0004	ACTIVAN
ILAVE	11-05-2014	09:01:02	O	0004	DESACTIVAN
ILAVE	12-05-2014	18:44:01	C	0004	ACTIVAN
ILAVE	12-05-2014	08:58:51	O	0004	Apertura Horario no Establecid
ILAVE	13-05-2014	19:04:10	C	0004	ACTIVAN
ILAVE	13-05-2014	08:54:19	O	0004	Apertura Horario no Establecid
ILAVE	14-05-2014	19:00:48	C	0004	ACTIVAN
ILAVE	14-05-2014	16:40:43	C	0004	ACTIVAN
ILAVE	14-05-2014	16:38:57	C	0004	ACTIVAN
ILAVE	14-05-2014	08:52:50	O	0004	Apertura Horario no Establecid
ILAVE	14-05-2014	17:33:52	O	0004	DESACTIVAN
ILAVE	14-05-2014	16:39:00	O	0004	DESACTIVAN
ILAVE	15-05-2014	18:41:45	C	0004	ACTIVAN
ILAVE	15-05-2014	08:56:02	O	0004	Apertura Horario no Establecid
ILAVE	16-05-2014	13:51:06	C	0004	ACTIVAN
ILAVE	16-05-2014	09:00:33	O	0004	DESACTIVAN
ILAVE	18-05-2014	18:33:48	C	0004	ACTIVAN
ILAVE	18-05-2014	13:22:04	C	0004	ACTIVAN
ILAVE	18-05-2014	18:31:04	O	0004	DESACTIVAN
ILAVE	18-05-2014	09:02:23	O	0004	DESACTIVAN
ILAVE	19-05-2014	19:25:02	C	0004	ACTIVAN
ILAVE	19-05-2014	09:05:20	C	0004	ACTIVAN
ILAVE	19-05-2014	16:26:31	O	0004	DESACTIVAN
ILAVE	19-05-2014	09:04:13	O	0004	DESACTIVAN
ILAVE	20-05-2014	19:25:51	C	0004	ACTIVAN
ILAVE	20-05-2014	08:55:01	O	0004	Apertura Horario no Establecid
ILAVE	21-05-2014	19:54:36	C	0004	ACTIVAN
ILAVE	21-05-2014	08:57:32	O	0004	Apertura Horario no Establecid

Oficina	Fecha	Hora	ID Señal	Evento	Descrip. Condic.
ILAVE	02-05-2014	14:21:28	C	0004	ACTIVAN
ILAVE	02-05-2014	09:03:08	C	0004	ACTIVAN
ILAVE	02-05-2014	08:58:05	O	0004	Apertura Horario no Establecid
ILAVE	02-05-2014	14:18:38	O	0004	DESACTIVAN
ILAVE	04-05-2014	19:01:59	C	0004	ACTIVAN
ILAVE	04-05-2014	09:29:33	C	0004	ACTIVAN
ILAVE	04-05-2014	08:56:23	O	0004	Apertura Horario no Establecid
ILAVE	04-05-2014	15:15:03	O	0004	DESACTIVAN
ILAVE	05-05-2014	19:11:38	C	0004	ACTIVAN
ILAVE	05-05-2014	09:00:21	O	0004	DESACTIVAN
ILAVE	06-05-2014	18:44:40	C	0004	ACTIVAN
ILAVE	06-05-2014	09:11:00	C	0004	ACTIVAN
ILAVE	06-05-2014	08:55:30	O	0004	Apertura Horario no Establecid
ILAVE	06-05-2014	18:43:04	O	0004	DESACTIVAN
ILAVE	22-05-2014	19:09:02	C	0004	ACTIVAN
ILAVE	22-05-2014	08:54:32	O	0004	Apertura Horario no Establecid
ILAVE	23-05-2014	14:06:54	C	0004	ACTIVAN
ILAVE	23-05-2014	08:57:44	C	0004	ACTIVAN
ILAVE	23-05-2014	08:54:28	O	0004	Apertura Horario no Establecid
ILAVE	23-05-2014	13:37:52	O	0004	DESACTIVAN
ILAVE	25-05-2014	19:25:56	C	0004	ACTIVAN
ILAVE	25-05-2014	09:03:14	O	0004	DESACTIVAN
ILAVE	26-05-2014	19:23:56	C	0004	ACTIVAN
ILAVE	26-05-2014	12:19:23	C	0004	ACTIVAN
ILAVE	26-05-2014	12:19:17	C	0004	ACTIVAN
ILAVE	26-05-2014	08:51:34	C	0004	ACTIVAN
ILAVE	26-05-2014	19:20:53	O	0004	Apertura Horario no Establecid
ILAVE	26-05-2014	08:49:45	O	0004	Apertura Horario no Establecid
ILAVE	26-05-2014	12:19:21	O	0004	DESACTIVAN
ILAVE	26-05-2014	12:13:17	O	0004	DESACTIVAN
ILAVE	27-05-2014	19:15:44	C	0004	ACTIVAN
ILAVE	27-05-2014	18:00:56	C	0004	ACTIVAN
ILAVE	27-05-2014	12:29:13	C	0004	ACTIVAN
ILAVE	27-05-2014	08:57:20	C	0004	ACTIVAN
ILAVE	27-05-2014	19:15:41	O	0004	Apertura Horario no Establecid
ILAVE	27-05-2014	08:53:36	O	0004	Apertura Horario no Establecid
ILAVE	27-05-2014	18:00:03	O	0004	DESACTIVAN
ILAVE	27-05-2014	12:28:08	O	0004	DESACTIVAN
ILAVE	28-05-2014	19:43:28	C	0004	ACTIVAN
ILAVE	28-05-2014	18:26:33	C	0004	ACTIVAN
ILAVE	28-05-2014	11:10:18	C	0004	ACTIVAN
ILAVE	28-05-2014	08:52:40	C	0004	ACTIVAN
ILAVE	28-05-2014	19:41:56	O	0004	Apertura Horario no Establecid

Oficina	Fecha	Hora	ID Señal	Evento	Descrip. Cond.
ILAVE	02-05-2014	14:21:28	C	0004	ACTIVAN
ILAVE	02-05-2014	09:03:08	C	0004	ACTIVAN
ILAVE	02-05-2014	08:58:05	O	0004	Apertura Horario no Establecid
ILAVE	02-05-2014	14:18:38	O	0004	DESACTIVAN
ILAVE	04-05-2014	19:01:59	C	0004	ACTIVAN
ILAVE	04-05-2014	09:29:33	C	0004	ACTIVAN
ILAVE	04-05-2014	08:56:23	O	0004	Apertura Horario no Establecid
ILAVE	04-05-2014	15:15:03	O	0004	DESACTIVAN
ILAVE	05-05-2014	19:11:38	C	0004	ACTIVAN
ILAVE	05-05-2014	09:00:21	O	0004	DESACTIVAN
ILAVE	06-05-2014	18:44:40	C	0004	ACTIVAN
ILAVE	06-05-2014	09:11:00	C	0004	ACTIVAN
ILAVE	06-05-2014	08:55:30	O	0004	Apertura Horario no Establecid
ILAVE	06-05-2014	18:43:04	O	0004	DESACTIVAN
ILAVE	28-05-2014	08:50:31	O	0004	Apertura Horario no Establecid
ILAVE	28-05-2014	18:25:27	O	0004	DESACTIVAN
ILAVE	28-05-2014	11:04:50	O	0004	DESACTIVAN
ILAVE	29-05-2014	19:43:19	C	0004	ACTIVAN
ILAVE	29-05-2014	18:08:55	C	0004	ACTIVAN
ILAVE	29-05-2014	16:04:27	C	0004	ACTIVAN
ILAVE	29-05-2014	19:41:51	O	0004	Apertura Horario no Establecid
ILAVE	29-05-2014	18:07:40	O	0004	DESACTIVAN
ILAVE	29-05-2014	16:04:25	O	0004	DESACTIVAN
ILAVE	29-05-2014	09:04:05	O	0004	DESACTIVAN
ILAVE	30-05-2014	23:14:38	C	0004	ACTIVAN
ILAVE	30-05-2014	12:19:47	C	0004	ACTIVAN
ILAVE	30-05-2014	23:13:28	O	0004	Apertura Horario no Establecid
ILAVE	30-05-2014	08:58:44	O	0004	Apertura Horario no Establecid
ILAVE	30-05-2014	12:17:26	O	0004	DESACTIVAN
ILAVE	31-05-2014	08:53:40	C	0004	ACTIVAN
ILAVE	31-05-2014	19:24:17	O	0004	Apertura Horario no Establecid
ILAVE	31-05-2014	08:43:39	O	0004	Apertura Horario no Establecid
COATA	09-05-2014	18:50:16	E401	003	Apertura Horario no Establecid
COATA	09-05-2014	16:03:42	E401	004	Apertura Horario no Establecid
COATA	09-05-2014	18:51:21	R401	003	ACTIVAN
COATA	09-05-2014	17:18:45	R401	003	ACTIVAN
COATA	09-05-2014	15:59:05	R401	003	ACTIVAN
COATA	09-05-2014	16:03:45	R401	004	ACTIVACION GENERAL
COATA	09-05-2014	16:00:22	R401	004	ACTIVACION GENERAL
COATA	12-05-2014	18:45:12	E401	003	Apertura Horario no Establecid
COATA	12-05-2014	11:46:05	E401	003	Apertura Horario no Establecid
COATA	12-05-2014	18:46:15	R401	003	ACTIVAN
COATA	12-05-2014	11:49:29	R401	003	ACTIVAN

Oficina	Fecha	Hora	ID Señal	Evento	Descrip. Condic.
ILAVE	02-05-2014	14:21:28	C	0004	ACTIVAN
ILAVE	02-05-2014	09:03:08	C	0004	ACTIVAN
ILAVE	02-05-2014	08:58:05	O	0004	Apertura Horario no Establecid
ILAVE	02-05-2014	14:18:38	O	0004	DESACTIVAN
ILAVE	04-05-2014	19:01:59	C	0004	ACTIVAN
ILAVE	04-05-2014	09:29:33	C	0004	ACTIVAN
ILAVE	04-05-2014	08:56:23	O	0004	Apertura Horario no Establecid
ILAVE	04-05-2014	15:15:03	O	0004	DESACTIVAN
ILAVE	05-05-2014	19:11:38	C	0004	ACTIVAN
ILAVE	05-05-2014	09:00:21	O	0004	DESACTIVAN
ILAVE	06-05-2014	18:44:40	C	0004	ACTIVAN
ILAVE	06-05-2014	09:11:00	C	0004	ACTIVAN
ILAVE	06-05-2014	08:55:30	O	0004	Apertura Horario no Establecid
ILAVE	06-05-2014	18:43:04	O	0004	DESACTIVAN
COATA	13-05-2014	18:26:28	E401	003	Apertura Horario no Establecid
COATA	13-05-2014	18:27:59	R401	003	ACTIVAN
COATA	14-05-2014	17:14:36	E401	003	Apertura Horario no Establecid
COATA	14-05-2014	15:22:15	E401	003	Apertura Horario no Establecid
COATA	14-05-2014	09:08:00	E401	003	Apertura Horario no Establecid
COATA	14-05-2014	18:44:02	R401	003	ACTIVAN
COATA	14-05-2014	15:24:02	R401	003	ACTIVAN
COATA	14-05-2014	11:13:08	R401	003	ACTIVAN
COATA	15-05-2014	18:57:35	E401	003	Apertura Horario no Establecid
COATA	15-05-2014	11:10:05	E401	003	Apertura Horario no Establecid
COATA	15-05-2014	21:48:38	R401	003	ACTIVAN
COATA	15-05-2014	11:11:32	R401	003	ACTIVAN
COATA	16-05-2014	18:39:37	E401	003	Apertura Horario no Establecid
COATA	16-05-2014	18:41:54	R401	003	ACTIVAN
COATA	17-05-2014	13:22:02	E401	003	Apertura Horario no Establecid
COATA	17-05-2014	13:23:53	R401	003	ACTIVAN
COATA	19-05-2014	18:36:25	E401	003	Apertura Horario no Establecid
COATA	19-05-2014	18:38:07	R401	003	ACTIVAN
COATA	20-05-2014	19:07:50	E401	003	Apertura Horario no Establecid
COATA	20-05-2014	17:27:29	E401	003	Apertura Horario no Establecid
COATA	20-05-2014	08:47:33	E401	003	Apertura Horario no Establecid
COATA	20-05-2014	19:12:00	R401	003	ACTIVAN
COATA	20-05-2014	17:38:25	R401	003	ACTIVAN
COATA	20-05-2014	08:54:04	R401	003	ACTIVAN
COATA	21-05-2014	18:41:21	E401	003	Apertura Horario no Establecid
COATA	21-05-2014	17:31:52	E401	003	Apertura Horario no Establecid
COATA	21-05-2014	08:58:43	E401	003	Apertura Horario no Establecid
COATA	21-05-2014	18:42:57	R401	003	ACTIVAN
COATA	21-05-2014	17:37:20	R401	003	ACTIVAN

Oficina	Fecha	Hora	ID Señal	Evento	Descrip. Condic.
ILAVE	02-05-2014	14:21:28	C	0004	ACTIVAN
ILAVE	02-05-2014	09:03:08	C	0004	ACTIVAN
ILAVE	02-05-2014	08:58:05	O	0004	Apertura Horario no Establecid
ILAVE	02-05-2014	14:18:38	O	0004	DESACTIVAN
ILAVE	04-05-2014	19:01:59	C	0004	ACTIVAN
ILAVE	04-05-2014	09:29:33	C	0004	ACTIVAN
ILAVE	04-05-2014	08:56:23	O	0004	Apertura Horario no Establecid
ILAVE	04-05-2014	15:15:03	O	0004	DESACTIVAN
ILAVE	05-05-2014	19:11:38	C	0004	ACTIVAN
ILAVE	05-05-2014	09:00:21	O	0004	DESACTIVAN
ILAVE	06-05-2014	18:44:40	C	0004	ACTIVAN
ILAVE	06-05-2014	09:11:00	C	0004	ACTIVAN
ILAVE	06-05-2014	08:55:30	O	0004	Apertura Horario no Establecid
ILAVE	06-05-2014	18:43:04	O	0004	DESACTIVAN
COATA	21-05-2014	09:03:08	R401	003	ACTIVAN
COATA	22-05-2014	18:45:37	E401	003	Apertura Horario no Establecid
COATA	22-05-2014	08:47:16	E401	003	Apertura Horario no Establecid
COATA	22-05-2014	18:48:36	R401	003	ACTIVAN
COATA	22-05-2014	08:48:43	R401	003	ACTIVAN
COATA	23-05-2014	18:46:00	E401	003	Apertura Horario no Establecid
COATA	23-05-2014	08:54:26	E401	003	Apertura Horario no Establecid
COATA	23-05-2014	18:48:07	R401	003	ACTIVAN
COATA	23-05-2014	08:58:46	R401	003	ACTIVAN
COATA	24-05-2014	13:27:05	E401	003	Apertura Horario no Establecid
COATA	24-05-2014	11:54:45	E401	003	Apertura Horario no Establecid
COATA	24-05-2014	11:57:17	R401	003	ACTIVAN
COATA	26-05-2014	18:53:10	E401	003	Apertura Horario no Establecid
COATA	26-05-2014	18:54:36	R401	003	ACTIVAN
COATA	26-05-2014	18:53:06	R401	003	ACTIVAN
COATA	27-05-2014	19:10:31	E401	003	Apertura Horario no Establecid
COATA	27-05-2014	17:17:25	E401	003	Apertura Horario no Establecid
COATA	27-05-2014	11:50:30	E401	003	Apertura Horario no Establecid
COATA	27-05-2014	19:12:01	R401	003	ACTIVAN
COATA	27-05-2014	17:19:47	R401	003	ACTIVAN
COATA	27-05-2014	11:52:41	R401	003	ACTIVAN
COATA	28-05-2014	18:41:59	E401	003	Apertura Horario no Establecid
COATA	28-05-2014	08:57:39	E401	003	Apertura Horario no Establecid
COATA	28-05-2014	18:45:56	R401	003	ACTIVAN
COATA	28-05-2014	12:59:36	R401	003	ACTIVAN
COATA	29-05-2014	19:23:28	E401	003	Apertura Horario no Establecid
COATA	30-05-2014	18:57:28	E401	003	Apertura Horario no Establecid
COATA	30-05-2014	17:46:53	E401	003	Apertura Horario no Establecid
COATA	30-05-2014	12:37:30	E401	003	Apertura Horario no Establecid

Oficina	Fecha	Hora	ID Señal	Evento	Descrip. Condic.
ILAVE	02-05-2014	14:21:28	C	0004	ACTIVAN
ILAVE	02-05-2014	09:03:08	C	0004	ACTIVAN
ILAVE	02-05-2014	08:58:05	O	0004	Apertura Horario no Establecid
ILAVE	02-05-2014	14:18:38	O	0004	DESACTIVAN
ILAVE	04-05-2014	19:01:59	C	0004	ACTIVAN
ILAVE	04-05-2014	09:29:33	C	0004	ACTIVAN
ILAVE	04-05-2014	08:56:23	O	0004	Apertura Horario no Establecid
ILAVE	04-05-2014	15:15:03	O	0004	DESACTIVAN
ILAVE	05-05-2014	19:11:38	C	0004	ACTIVAN
ILAVE	05-05-2014	09:00:21	O	0004	DESACTIVAN
ILAVE	06-05-2014	18:44:40	C	0004	ACTIVAN
ILAVE	06-05-2014	09:11:00	C	0004	ACTIVAN
ILAVE	06-05-2014	08:55:30	O	0004	Apertura Horario no Establecid
ILAVE	06-05-2014	18:43:04	O	0004	DESACTIVAN
COATA	30-05-2014	18:59:04	R401	003	ACTIVAN
COATA	30-05-2014	17:49:33	R401	003	ACTIVAN
COATA	30-05-2014	12:44:35	R401	003	ACTIVAN
COATA	31-05-2014	13:21:53	E401	003	Apertura Horario no Establecid
COATA	31-05-2014	13:23:34	R401	003	ACTIVAN

Tabla N° 13: Apertura y Cierre de Bóveda

Fuente: Panel de Alarma BOSCH

Elaborado: Por los Investigadores

Con estos datos de la tabla N° 13 se valida la hipótesis específica 01, donde se verifica la aplicación de un sistema dual y remoto, para la apertura de bóveda.

Se hace uso de un sistema remoto por que el panel central de alarma nos permite cerrar electrónicamente tanto las particiones de bóveda como de agencia. La rapidez de esta dependerá del tipo de comunicación con la que cuente las respectivas oficinas mencionadas en la tabla N° 7.

En base a estos datos obtenidos se valida nuestra hipótesis general, ya que el panel central de alarmas Bosch es un dispositivo electrónico que nos brinda muchas posibilidades de conexión, conexión por red, conexión por vida telefónica.

El panel central de alarma, es un equipo robusto el cual brinda una buena disposición para poder cubrir bastantes zonas, y una amplia gama de soluciones.

Gracias a la implementación de este sistema de seguridad se logró reducir el número de incidentes de falsas alarmas o incidentes inoportunos, dando una capacitación constante al personal o funcionarios de cada agencia, sobre temas de seguridad y el uso básico del sistema central de alarma.

En la figura N° 41, se muestra que Caja Rural Los Andes S.A., mantiene un índice bajo en lo que es reporte de alarmas con la respectiva verificación policial, comparado con otras entidades el índice de reporte es bajo y esto significa un gran ahorro para la empresa.

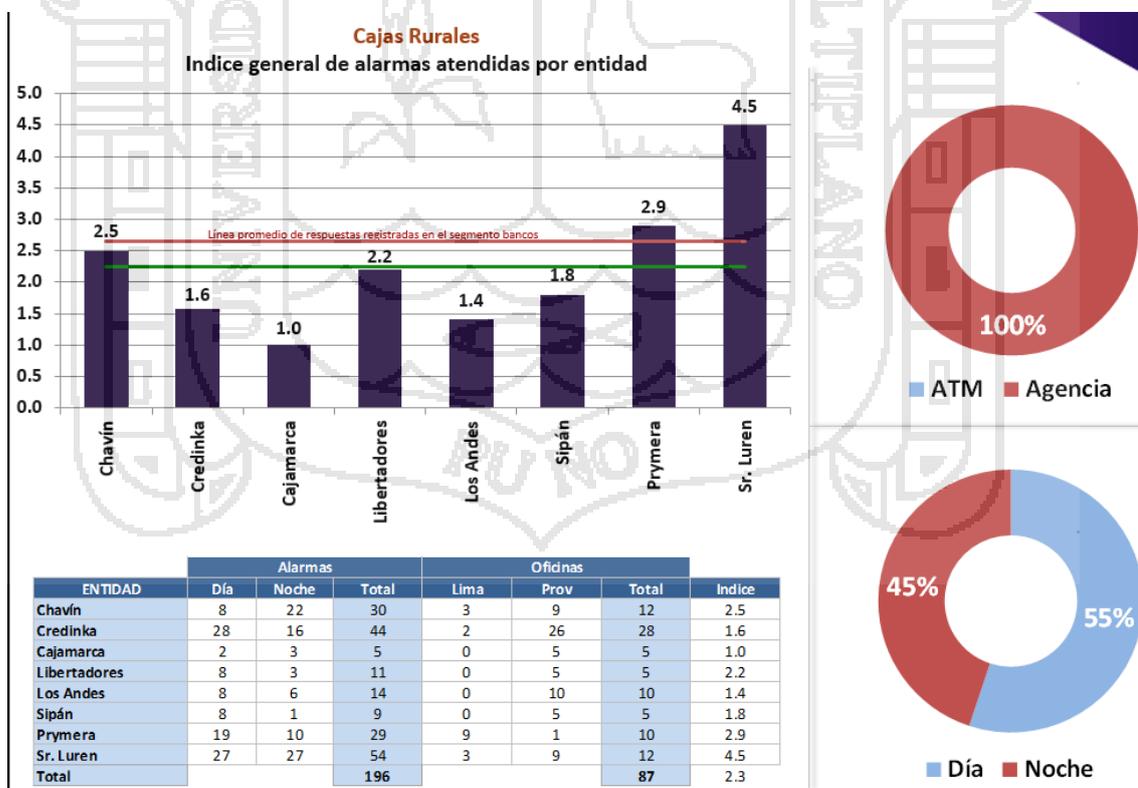


Figura N° 41: Alarmas Atendidas
Fuente: superintendencia de Banca y Seguros (SBS)
Elaborado: Por SBS

En la tabla N° 14 se muestra al detalle el reporte de las falsas alarmas, y el respectivo descargo hecho por policías de la zona, por lo general siempre resulta en una falsa alarma o mal manejo de los funcionarios.

FECHA	HORA	OFICINA	TIPO ALARMA	UNIDAD	RESULTA	NOVEDAD
02/03/2014	18:45:41	HUANCANE	Failed to Test		FALSA ALARMA	
06/03/2014	06:12:38	ACORA	ALARMA INTRUSION	SOS ILAVE CHAVEZ A PIE	FALSA ALARMA	IDNICA AG CERRADA S/N EXTERNA C ORTE DE AC EN LA ZONA
06/03/2014	06:14:22	ACORA	FALTA CORRIENTE	SOS ILAVE CHAVEZ A PIE	ALARMA REAL	IDNICA AG CERRADA S/N EXTERNA C ORTE DE AC EN LA ZONA
07/03/2014	22:50:19	AYAVIRI	FALTA CORRIENTE	A PIE, TCO GARCIA GOMEZ	FALSA ALARMA	CORTE DE AC EN UNA CUADRA
10/03/2014	22:50:47	AZANGARO	ALARMA INTRUSION	SO POMACOSI BENAVENTE A PIE	FALSA ALARMA	INDICA AG CERRADA APARENTEMENTE ESTA S/N AL COSTADO DERECHO HAY UN HOSPEDAJE EL MISMO QUE ESTA CERRADO TAMBIEN SE LE COMUNICIA AL SR DIMAS LOAYZA
11/03/2014	11:34:20	TARACO	ALARMA DE PULSADOR INALAMBRICO	A PIE SO CHURA	FALSA ALARMA	SE ENTREVISTO CON MERY OLGA PANDIA, INDICA ERROR DEL VIGILANTE
12/03/2014	13:39:45	AYACUCHO	ALARMA PULSADOR	PN-13736	FALSA ALARMA	AREA DE VENTANILLAS//SO2 TORRES CANAZAS PAUL, SE ENTREVISTO CON LA FUNC. JANET ACASIO NAVARRO, INDICA ERROR HUMANO
12/03/2014	22:17:40	JULIACA	FALTA CORRIENTE	PR-7191	FALSA ALARMA	BRIG AZA VEGA AG CERRADO S/N AC OK
13/03/2014	16:33:42	ACORA	ALARMA DE PULSADOR INALAMBRICO	SO TICONA MAMANI	FALSA ALARMA	SRTA DELIA PACO ZARATE IUNDIRA ERRO HUMANO
14/03/2014	12:23:11	TARACO	ALARMA PULSADOR	A PIE, TCO2 HUALLANAY CAYATA	FALSA ALARMA	SE ENTREV SRTA MARILUZ HUANCA APAZA, POR ERROR S/N
15/03/2014	18:52:18	HUANCANE	Failed to Test		FALSA ALARMA	NO ENVIA AUTOTEST
15/03/2014	20:12:00	CARABAYA	FALTA CORRIENTE	PR-14646	FALSA ALARMA	SOB.JULIO MAYTA
16/03/2014	05:58:57	TARACO	FALLA COM. CAIDA RED	A PIE TCO. LLAGUNO PANDIE,	FALSA ALARMA	AG. CERRADA XTERNAMENTE SN. AC NORMAL EN LA ZONA
18/03/2014	01:51:19	ESPINAR	Failed to Test	KO-79711	FALSA ALARMA	TCO CONDORI AGENCIA CERRADA S/N EXTERNA AC OK NO SE APRECIA NADA INUSUAL LOCALES CONTIGUOS, LLUVIAS EN LA ZONA
19/03/2014	04:52:00	ESPINAR	Failed to Test	KO-7971	FALSA ALARMA	BRIG ZAMBRANO VERIFICA AGENCIA CERRADA S/N EXTERNA HUBO CORTE DE FLUIDO

						ELECTRICO PERO RESTABLECIO S/N...
23/03/2014	01:23:27	ACORA	FALTA CORRIENTE	SO SUPO CHAÑA,	FALSA ALARMA	AG CERRADA PARTE EXTERNA SIN NOEVDAD CORTE DE AC EN LA ZOPNA EL ISMO QUE YA RESTABLECIO
25/03/2014	14:44:40	AYACUCHO	ALARMA DE PULSADOR INALAMBRICO	TCO MEJIA VASQUEZ	FALSA ALARMA	INDICA VP ROLY HUAMAN CORDOVA INDICA TODO S/N
28/03/2014	02:02:08	ACORA	FALLA COM. CAIDA RED	A PIE SO. TEC. 3 YAPO QUISPE	FALSA ALARMA	DIVAL AG CERRADA, S/n PARTE EXTERNA, LUCES INTERNAS PRENDIDAS, AC OK EN LA ZONA
29/03/2014	04:40:48	ESPINAR	Failed to Test		ALARMA REAL	SE COMUNICA AL SR DIMAS SEG AGENCIA TOTALMENTE INOPERATIVA...SE LE INDICA COORDINAR LA VIGILANCIA PARTICULAR INTERNA Y PODER ADOPTAR LAS MEDIDAS DE SEGURIDAD RESPECTIVAS PARA EL FIN DE SEMANA...
31/03/2014	02:49:23	ACORA	Failed to Test		FALSA ALARMA	SO JORGE CHIPANA A PIE IDNICA AG CERRADA FLUIDO NORMAL EN LA ZONA
31/03/2014	22:08:53	MACUSANI	FALTA CORRIENTE		FALSA ALARMA	MAYOR NIETO INDICA QUE HUBO CORTE DE AC EN LA ZONA EL MISMO QUE YA RESTABLECIO AG SIN NOEVDAD
01/04/2014	21:05:21	ACORA	Failed to Test	A PIE, SUP. TICONA MAMANI RUBEN	FALSA ALARMA	AGENCIA CERRADA S/N AC NORMAL EN LA ZONA
01/04/2014	22:37:35	HUANCANE	FALLA COM. CAIDA RED		FALSA ALARMA	
02/04/2014	23:13:30	JULIACA	ALARMA INTRUSION	PR-14647	FALSA ALARMA	SUP PARIAPASA INDICA AG CERRADA S/N EXETRNA FLUIDO NORMAL
02/04/2014	23:15:07	JULIACA	ALARMA INTRUSION	PR-14647	FALSA ALARMA	SUP PARIAPASA INDICA AG CERRADA S/N EXETRNA FLUIDO NORMAL
04/04/2014	17:58:53	MACUSANI	ALARMA DE PULSADOR INALAMBRICO	MAY. NIETO RODRIGUEZ	FALSA ALARMA	LE REPORTA AG. SN.- HAY CORTE DE AC Y FUERTES LLUVIAS. LA CAJA ESTA CERRADA PERSONAL EN EL INTERIOR
05/04/2014	18:38:17	CHIVAY	FALTA CORRIENTE	BRIG ROMERO PEREZ A PIE	FALSA ALARMA	AGENCIA CERRADA S/N EXTERNA AC OK EN LA VIA PUBLICA. SE COORDINA RONDAS
05/04/2014	19:46:49	ACORA	Failed to Test	SO3 BERRIOS JUAN	FALSA ALARMA	AGENCIA CERRADA S/N EXTERNA AC OK NO SE APRECIA NADA INSUAL
07/04/2014	07:09:57	HUANCANE	Apertura Horario no Establecid	A PIE, TCO3 HUAMATICO LUIS	FALSA ALARMA	TOCAN LA PUERTA NO SALE NADIE PARTE EXTERNA S/N

07/04/2014	19:01:19	AYAVIRI	ALARMA DE CAJA FUERTE	SO. SUCA ORTIZ A PIE	FALSA ALARMA	CON LA SRTA CARMEN MAMANI FUNC. AGENCIA S/N DESCONOCE...
08/04/2014	05:28:36	JULIACA	ALARMA INTRUSION	KR-9072	FALSA ALARMA	TEC. DELGADO CARDENAS INDICA AG. CERRADA PARTE EXTERNA SIN NOVEDAD
09/04/2014	22:34:12	CHIVAY	Failed to Test	SO CHALCO A PIE	FALSA ALARMA	AGENCIA CERRADA S/N EXTERNA AC OK NO HAY NADA INUSUAL EN AREAS COLINDANTES, LA RED MOVISTAR ESTA CON PROBLEMAS POR LO CUAL HAY PROBLEMA DE COMUNICACION ZONAL
10/04/2014	22:18:56	CHIVAY	Failed to Test	SO VARGAS PAREJAA POR SUS PROPIOS	FALSA ALARMA	AG CERRADA CORTE DE AC EN LA ENTIDAD EN LA ZONA EL FLUIDO ES NORMAL
12/04/2014	00:01:48	AYACUCHO	FALTA CORRIENTE	PN-13736	FALSA ALARMA	SO2 TORRES CANASAS AGENCIA CERRADA S/N EXTERNA AC OK EN LA ZONA NO SE PUEDE VER INTERIOR
12/04/2014	06:34:24	SICUANI	Apertura Horario no Establecid	SO ARIAS A PIE	FALSA ALARMA	SR ANIBAL CAHUANA ADM INDICA INGRESO TEMPRANO POR LIMPIEZA
12/04/2014	14:47:09	CHIVAY	Failed to Test	SOB. RAMOS APAZA (A PIE)	FALSA ALARMA	INDICA AG CERRADA PARTE EXTERNA SIN NOVEDAD
13/04/2014	12:18:20	CHIVAY	DISC. AUDIO	BRIG. FIDEL TACO (A PIE)	FALSA ALARMA	INDICA AG. CERRADA PARTE EXTERNA SIN NOVEDAD
13/04/2014	13:53:48	SICUANI	ALARMA INTRUSION		FALSA ALARMA	SEG. VERIFICO SN
16/04/2014	04:54:53	ESPINAR	Failed to Test	SO 2 RAUL QUISPE ORDOÑEZ	FALSA ALARMA	INDICA AG CERRADA PARTE EXTERNA SIN NOVEDAD AC NORMAL EN LA ZONA
16/04/2014	19:50:38	ACORA	FALTA CORRIENTE	A PIE	FALSA ALARMA	18:17 / SOSUP. SONCO CHIPANA, AG. CERRADA XTERNAMENTE SN HUBO CORTE MOMENTANEO
17/04/2014	03:41:18	CHIVAY	Failed to Test	A PIE SOT TALAVERA RODRIGUEZ	FALSA ALARMA	A UNA CDRA HAY UN CAMION DESCARGA MERCADERIA, AC NORMAL.
17/04/2014	12:30:57	CHIVAY	Failed to Test	TCO2. FLORES CAHUANA A PIE	FALSA ALARMA	AGENCIA CERRADA S/N EXTERNA FLUIDO ELECTRICO NBORMAL EN LA ZONA...
17/04/2014	15:45:54	HUANCANE	FALTA CORRIENTE	A PIE, TCO2 CHOQUEHUANCA	FALSA ALARMA	NAVIDAD, AGENCIA CERRADA CORTE DE AC EN LA ZONA
18/04/2014	04:25:07	CHIVAY	Failed to Test	A PIE SO. QUISPE	FALSA ALARMA	AG CERRADA, S/N PARTE EXTERNA, AC OK EN LA ZONA

18/04/2014	17:21:21	MACUSANI	FALTA CORRIENTE	A PIE TCO CRUZ CHOQUEHUANCA	FALSA ALARMA	COORDINA RONDAS CORTE DE AC EN LA ZONA.
18/04/2014	17:35:47	HUANCANE	FALTA CORRIENTE	SUP ASTUDILLO QUIROZ A PIE	FALSA ALARMA	AGENCIA S/N EXTERNA CORTE DE AC EN LA ZONA
19/04/2014	04:31:45	ESPINAR	Failed to Test	TCO ALARCON A PIE	FALSA ALARMA	AGENCIA CERRADA S/N EXTERNA AC OK NO SE APRECIA NADA INUSUAL POR LA ZONA
19/04/2014	20:06:17	ACORA	FALTA CORRIENTE	SO SUP SONCO CHIPANA JAVIER	FALSA ALARMA	INDICA HAY RAYOS EN LA ZONA, CORTE AC EN LA ZONA
20/04/2014	16:51:49	SICUANI	FALTA CORRIENTE	PL-12238	FALSA ALARMA	TCO HURTADO CUADROS SR ALVAREZ DUEÑO DE INMUEBLE REALIZABA LIMPIEZA, AGENCIA CERRADA S/N EXTERNA AC OK EN LA ZONA, SO COLQUE CIA SICUANI TAMBIEN CONFIRMA AC OK EN LA ZONA
21/04/2014	03:36:32	CHIVAY	Failed to Test	A PIE	FALSA ALARMA	TCO 2DA FLORES CAHUANA DE ALDAS QUIEN INDICA LOCAL CERRADO PARTE EXTERNA S/N.
21/04/2014	06:54:19	ESPINAR	Apertura Horario no Establecid	KO-7971	FALSA ALARMA	AGENCIA SN-CERRADA NO SALE PERSONAL
21/04/2014	16:24:59	CHIVAY	ALARMA PULSADOR	TEC FLORES CAHUANA ALEJANDRO	FALSA ALARMA	SE ENTREVISTA CON KELLY CRUZ RAMOS ADM DE AG. LA MISMA QUE REPORTA ERROR HUMANO JOP
22/04/2014	01:50:29	DESAGUADERO	Failed to Test		FALSA ALARMA	A PIE SO 1 ARESMENDI QUISPE LUIS AG CERRADO AC OK
22/04/2014	02:57:50	CHIVAY	Failed to Test	A PIE	FALSA ALARMA	SO CHALCO MASILLA AG CERRADO S/N AC OK
23/04/2014	04:37:08	ESPINAR	Failed to Test	KO-7095	FALSA ALARMA	TEC 1 CONDORI BALLNEAS WUILBER AG CERRADO S/N AC OK
24/04/2014	02:47:54	CHIVAY	Failed to Test	SO QUENALLA LINARES A PIE	FALSA ALARMA	AGENCIA CERRADA S/N HAY CORTE DE AC EN LA ZONA...
25/04/2014	04:46:08	DESAGUADERO	Failed to Test	SO. CENTENO ARISTILLON A PIE	FALSA ALARMA	AGENCIA CERRADA S/N EXTERNA FLUIDO OK EN LA ZONA...
25/04/2014	14:30:10	AZANGARO PUNO	ALARMA PULSADOR	SO3 GONZALES RAMOS A PIE	FALSA ALARMA	OF. ASESOR DE NEGOCIOS // SR TA BRIGIDA MAQUE ADM INDICA ERROR S/N
27/04/2014	11:26:47	CHIVAY	Failed to Test	A PIE TEC. FLORES CAHUANA	FALSA ALARMA	AG CERRADA, S/N PARTE EXTERNA, PTAS Y VENTANAS CONFORME, AC OK EN LA ZONA
01/05/2014	23:46:03	CHIVAY	FALLA COM. CAIDA RED	A PIE, BRIG BRAVO PATIÑO ALFREDO	FALSA ALARMA	AGENCIA CERRADA S/N AC NORMAL

06/05/2014	00:13:10	HUANCANE	Failed to Test	SOB. ASTUDILLO QUIROZ (A PIE)	FALSA ALARMA	AGENCIA CERRADA PARTE EXTERNA SIN NOVEDAD, NO HAY NOVEDADES
07/05/2014	05:47:06	APLAO	ALARMA INTRUSION	KP-0901	FALSA ALARMA	SISTEMAS (PIR)// SOB. CASTAÑA CONDORI INDICA QUE SE ENTREVISTO CON EL SR. LUIS URQUIZO (ADM) QUIEN SE ENCONTRABA EN EL INTERIOR...
08/05/2014	04:34:37	ESPINAR	Failed to Test	SOB. SITURE VILA (A PIE)	FALSA ALARMA	AG CERRADA PARTE EXTERNA SIN NOVEDAD, FLUIDO ELECTRICO NORMAL EN LA ZONA
09/05/2014	01:19:50	HUANCANE	FALLA COM. CAIDA RED	PL-12191	FALSA ALARMA	SO. VEGA AG CERRADA, PTAS Y VENTANAS OK, S/N PARTE EXTERNA, AC OK EN LA ZONA, AG COLINDA CON AGENCIA BANCARIA CREDINKA Y TDAS PARTICULARES
09/05/2014	09:03:03	AZANGARO PUNO	ALARMA PANICO	A PIE, TCO3 SANCHEZ CHAVEZ GIANMARCO	FALSA ALARMA	SE ENTREV. SR. VICTGOR LIMA CACERES , POR ERROR S/N AL DIGITAL LA ALARMA DE BOVEDA
10/05/2014	20:19:39	ACORA	FALTA CORRIENTE	SO SONCO CHIPANA A PIE	FALSA ALARMA	AGENCIA CERRADA S/N EXTERNA BAJA DE VOLTAGE EN LA ZONA
11/05/2014	02:24:01	CHIVAY	Failed to Test	A PIE SO. 2 FLORES CAHUANA	FALSA ALARMA	AG CERRADA, S/N PARTE EXTERNA, CORTE DE AC EN CALLE
11/05/2014	03:35:41	ACORA	BATERIA BAJA	A PIE SO. SUP. LLAVE FLORES SIMON	FALSA ALARMA	AG CERRADA, S/N PARTE EXTERNA, AC INESTABLE EN LA ZONA
11/05/2014	15:53:52	MACUSANI	DISC. AUDIO	SO3 FLORES QUISPE A PIE	FALSA ALARMA	AGENCIA CERRADA S/N EXTERNA AC OK NO HAY DAÑOS
12/05/2014	12:11:38	AYACUCHO	SOLICITAN APOYO POLICIAL	PN-17316	ALARMA REAL	FUNCIONARIO DAVID ENRIQUE AYBAR REALIZA UN MAL MANEJO DE DINERO.....SO SERNA CON LA SRTA LIZBETT HINOSTROZA CALDERON FUNC. SE ORIENTA DE COMO PROCEDER ANTE ESTE TIPO DE SITUACION...
13/05/2014	09:03:00	HUANCANE	ALARMA INTRUSION	SO3. HUAMNTICO CHIPANA A PIE	FALSA ALARMA	CON SR MAMANI QUIILA FUNC AGENCIA S/N..
14/05/2014	08:42:03	AZANGARO PUNO	FALLA COM. CAIDA RED		FALSA ALARMA	RESTABLECIO OK...

Tabla N° 14: Reporte de Alarmas
Fuente: Panel de Alarma BOSCH
Elaborado: Por los Investigadores

CONCLUSIONES

PRIMERO: El sistema CCTV (Circuito Cerrado de Televisión) es uno de los más completos, permite obtener una seguridad y vigilancia confiable; la principal característica de las cámaras LS VISION es evitar cualquier situación y actos indebidos ocurridos en algún lugar o área específica, en este caso en las diferentes AGENCIAS DE CAJA RURAL – LOS ANDES S.A.

SEGUNDO: El diseño implementado se realizó con tecnología, cable UTP clase 5, contando con cámaras fijas y PTZ inteligentes con un control de TX y RX adecuado, que pueden ser adaptados a cualquier hora tanto el día como la noche, esto permite el manejo confiable y discreto del sistema.

TERCERO: El sistema de alarma funciona tanto local como remotamente aun presentándose las dificultades tecnológicas que se presenta. Por ser el ambiente de trabajo de la empresa el sector rural.

CUARTO: Los medios de comunicación más óptimos para la central de alarma, es la red telefónica conmutada (RTC) y la conexión vía internet o red, estos dos medios de comunicación sacan el máximo provecho al panel de control, y la interconexión se hace más rápida.

SUGERENCIAS Y RECOMENDACIONES

PRIMERO: Es necesario tener en cuenta los espacios verticales, horizontales, cuartos de interconexión y control, para el adecuado cableado de las soluciones de redes de datos, para lograr el orden de direccionamiento de equipos.

SEGUNDO: Se recomienda utilizar otro tipo de conexión como la fibra óptica porque es el mejor medio de transmisión en cuanto a distancia y ancho de banda, para obtener una mejor comunicación y dotando de una estabilidad más segura en el sistema

TERCERO: Es necesario implementar un procedimiento de estudio tecnológico, para la apertura de nuevas Oficinas o agencias, debiendo de cumplir ciertos estándares tecnológicos, para así poder garantizar una buena interconexión de la oficina o agencia con la central de monitoreo.

BIBLIOGRAFÍA

- Calderón, J. A. (1990). *Seguridad Bancaria*. Guatemala: Banco de Guatemala.
- Couch, L. (1995). *Modern Communications Systems: Principles and Applications*. Prentice Hall.
- Guada, J. J. (2006). *Diseño e Implementación de un Sistema de Control de Acceso*.
- Herrera, E. (2003). *Tecnologías y Redes de Transmisión de datos*. México: Editorial Limusa.
- Horn, D. (1992). *Electronic Components, a complete reference*. Mac Graw Hill.
- Horn, D. (1993). *Build your own home security sistem*. Mac Graw Hill.
- Maloney, T. J. (2006). *Electrónica Industrial Moderna*. Editorial Pearson Educación.
- Marcelo, J. S. (2002). *Sensores y Actuadores en Microbótica*. Badajoz.
- Martín, J. (1990). *Telecommunications and the Computer*. Prentice Hall.
- Maureen, J. (1995). *Audio and video interiors {magazine}*. Los Angeles: Electronic Pre-Press Tri Graphics.
- MCcomb, G. (s.f.). *Installing home and auto security systems*. Texas: Radio Shack, a division of Tandy Corp. FT. Worth.
- Peña, J. D. (2003). *Comunicaciones en el Entorno Industrial*. España: Editorial UOC.
- Sergio Talens Oliag, J. H. (1998). *Internet Redes de computadores y sistemas de información*. Paraninfo.
- Stallings, W. (2000). *Comunicaciones y Redes de Computadores*. Madrid: Editorial Prentice Hall.
- Tomasi, W. (1996). *Sistemas de Comunicaciones Electrónicas*. Prentice Hall.



ANEXO I: MATRIZ DE SUPERVISIÓN

MATRICES DE INSPECCION DE SEGURIDAD PARA CUMPLIMIENTO DE RESOLUCION MINISTERIAL N° 0689-2000-IN/1701							
<p>Agencia: _____</p> <p>Fecha: _____</p>		<p>Calificación: (1) Cumple; (0,5) Cumple parcialmente; (0) No cumple. Total 90</p>					
MATRIZ	DETALLES A VERIFICAR	CALF.	OBSERVACIONES	ACCIONES A TOMAR	INICIO dd/mm/año	FIN dd/mm/año	
<p>Documentación Especifica a Presentar por Agencia</p>	<p>Planes</p>	Seguridad contra actos antisociales					
		Emergencia					
		Contingencia					
	<p>Contrato o certificado de instalación</p>	Del sistema CCTV					
		Del sistema de control de accesos					
		Del sistema de alarmas					
	<p>Planos e inventarios</p>	Del sistema CCTV					
		Del sistema de control de accesos					
		Del sistema de alarmas					
		Recursos contra incendios					
	<p>Contrato o certificado de mantenimiento</p>	Del sistema CCTV					
		Del sistema de control de accesos					
		Del sistema de alarmas					
	<p>Permisos actualizados</p>	Instalaciones eléctricas					
		Municipales					
		De Bomberos					
	<p>Permisos actualizados</p>	De SBS					
		Certificado de resistencia de la infraestructura física y/o repotenciación y readecuación en paredes y ventanas					
	<p>Certificado de cumplimiento de estándares internacionales de bóvedas, cajas fuertes y puertas de bóveda</p>	Certificado de cumplimiento de estándares internacionales de bóvedas, cajas fuertes y puertas de bóveda					
TOTAL (19)							
% DE CUMPLIMINETO							

ANEXO II: MATRIZ MÉTODO MOSLER Y MÉTODO MESERI

MATRIZ DE ANALISIS Y EVALUACION DE RIESGOS METODO MOSLER														
N°	Agencia Bancaria QS Riesgo	ANALISIS						EVALUACION					CLASE DE RIESGO	
		F	S	P	E	A	V	I	D	C	Pb	ER		
1	Asalto													Elevado
2	Robo													Elevado
3	Hurto													Muy Reducido
4	Fraude / Estafa													Normal
5	Vandalismo													Muy Reducido
6	Terrorismo													Muy Reducido
7	Incendio Probocado													Normal

MATRIZ DE ANALISIS Y EVALUACION DE RIESGOS METODO MOSLER																													
N°	Escenario Riesgo	ESCENARIO 1							ESCENARIO 2							ESCENARIO 3							ESCENARIO n						
		F	S	P	E	A	V	CR	F	S	P	E	A	V	CR	F	S	P	E	A	V	CR	F	S	P	E	A	V	CR
1	Asalto																												
2	Robo																												
3	Accidente																												
n	Otros Riesgo																												

EVALUACION DEL RIESGO DE INCENDIO "METODO MESERI"							
CONSTRUCCIÓN				CONCENTRACIÓN			
Nro. de pisos	Altura	Coeficiente	Puntos	Factor de concentración	CoeficientePuntos		
1 ó 2	menor que 6 m	3		Menor de U\$S 800 m2	3		
3, 4 ó 5	entre 6 y 15 m	2		Entre U\$S 800 y 2.000 m2	2		
6, 7, 8 ó 9	entre 15 y 27 m	1		Más de U\$S 2.000 m2	0		
10 ó más	más de 27 m	0		PROPAGABILIDAD			
Superficie mayor sector de incendios		Coeficiente	Puntos	Vertical	CoeficientePuntos		
de 0 a 500 m2		5		Baja	5		
de 501 a 1.500 m2		4		Media	3		
de 1.501 a 2.500 m2		3		Alta	0		
de 2.501 a 3.500 m2		2		Horizontal	CoeficientePuntos		
de 3.501 a 4.500 m2		1		Baja	5		
más de 4.500 m2		0		Media	3		
Resistencia al fuego		Coeficiente		Puntos	Alta	0	
Resistente al fuego (hormigón)		10		DESTRUCTIBILIDAD			
No combustible		5		Por calor		CoeficientePuntos	
Combustible		0		Baja	10		
Falsos techos		Coeficiente	Puntos	Media	5		
Sin falsos techos		5		Alta	0		
Con falso techo incombustible		3		Por humo		CoeficientePuntos	
Con falso techo combustible		0		Baja	10		
SITUACION				Media	5		
Distancia Bomberos	Tiempo	Coeficiente	Puntos	Alta	0		
Menor de 5 km	5 minutos	10		Por corrosión		CoeficientePuntos	
entre 5 y 10 km.	5 y 10 minutos	8		Baja	10		
Entre 10 y 15 km.	10 y 15 minutos	6		Media	5		
entre 15 y 25 km.	15 y 25 minutos	2		Alta	0		
Más de 25 km.	más de 25 minutos	0		Por agua		CoeficientePuntos	
Accesibilidad edificio		Coeficiente	Puntos	Baja	10		
Buena		5		Media	5		
Media		3		Alta	0		
Mala		1		SUBTOTAL (X)		0	
Muy mala		0					
PROCESOS							
Peligro de activación		Coeficiente	Puntos	FACTORES DE PROTECCION			
Bajo		10		Medios de protección		SVCV Puntos	
Medio		5		Extintores	12		
Alto		0		Bocas de incendio equipadas	24		
Carga térmica		Coeficiente	Puntos	Bocas hidrantes exteriores	24		
Baja		10		Detectores automáticos de incendio	04		
Media		5		Rociadores automáticos	58		
Alta		0		Instalaciones fijas especiales	24		
Combustibilidad		Coeficiente	Puntos	SUBTOTAL (Y)			0
Baja		5					
Media		3					
Alta		0		BRIGADAS CONTRA INCENDIOS			
Orden y limpieza		Coeficiente	Puntos	Brigadas internas		CoeficientePuntos	

Bajo	0		Existe brigada contra incendios	1
Medio	5		No existe brigada contra incendios	0
Alto	10		BCI	0
Almacenamiento en altura	Coficiente	Puntos		
Menor de 2 m	3		Calculo del Coficiente de Protección "P" $P = (5X / 129) + (5Y / 26) + BCI$	000
Entre 2 y 4 m	2			
Más de 4 m	0			



