ESCUELA POLITÉCNICA NACIONAL

**FACULTAD DE INGENIERÍA ELÉCTRICA
Y ELECTRÓNICA**

ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD ELECTRÓNICA EN LA EMAAP-Q

**PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO
EN ELECTRÓNICA Y CONTROL**

OMAR PATRICIO TOBAR ARAGÓN
omarptobar@hotmail.com

JOSÉ LUIS BENÍTEZ ALTUNA
joselbenitez10@yahoo.com

DIRECTOR: ING. ANA RODAS
arodas@epn.edu.ec

Quito, Octubre 2009

DECLARACIÓN

Nosotros, Omar Patricio Tobar Aragón y José Luis Benítez Altuna, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

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

Omar Patricio Tobar Aragón	José Luis Benítez Altuna

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Omar Patricio Tobar Aragón y José Luis Benítez Altuna, bajo mi supervisión.

_____

Ing. Ana Rodas
DIRECTORA DEL PROYECTO

AGRADECIMIENTO

A la Ing. Ana Rodas, por su colaboración, apoyo y paciencia en el desarrollo de este proyecto de titulación.

A la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito, por permitimos desarrollar este sistema en sus instalaciones.

Al Departamento de Seguridad Física y Radio Comunicaciones, por brindarnos la confianza en la elaboración de este proyecto.

A la Escuela Politécnica Nacional, por los conocimientos recibidos y valores adquiridos en nuestro período estudiantil.

A ti Madre Naturaleza, por el papel otorgado y desperdiciado en la impresión de los borradores de esta tesis. En compensación madre mía, cinco árboles serán plantados.

A nuestras familias, por soportar todos y cada uno de nuestros momentos duros en la Universidad, especialmente el prepo, primer nivel, segundo nivel, tercer nivel, etc.

Omar Patricio Tobar Aragón
José Luis Benítez Altuna

DEDICATORIA

A mis amigos, quienes siempre estuvieron junto a mí con su apoyo y sabiduría, en los momentos duros, en los momentos felices, siempre…

A mi hermana, la única que ha podido leer mi corazón a través de una simple mirada, mi mejor amiga…

A mi padre, quien a pesar de atravesar momentos duros no ha dejado de ser ejemplo digno de superación y amor a la vida. No abra enfermedad que separe tu amor de mi compañía…

Y… a lo más sagrado en la vida de todo hijo, a mi madre, mi amiga, mi compañera, la razón de mi fuerza, la razón de ser un profesional, es por ti que he alcanzado este sueño, para ti… mi Ingeniería.

Omar Patricio Tobar Aragón

DEDICATORIA

A Dios, que me supo dar la fuerza y voluntad para culminar esta etapa de mi vida.

A mis Padres, que me apoyaron en cada momento, que me dieron el amor, la confianza, los valores y la educación.

A mis hermanos, que siempre estuvieron junto a mí en los momentos difíciles de mi vida.

A toda mi familia, que de alguna forma siempre estuvieron a mi lado alentándome.

A mis amigos, que en los buenos y malos momentos nunca se separaron de mi lado.

José Luis Benítez

ÍNDICE

CONTENIDO **I**

RESUMEN **X**

PRESENTACIÓN **XI**

CAPÍTULO 1

DESCRIPCIÓN DE SISTEMAS DE SEGURIDAD ELECTRÓNICA

1.1 Origen del término seguridad 1
1.1.1 Políticas de seguridad 1
1.1.2 Doctrina de seguridad nacional 2
1.1.3 Seguridad ciudadana 2
1.1.4 Seguridad colectiva 3
1.1.5 Seguridad nacional 4

1.2 Organismos destinados a la seguridad 4
1.2.1 Fuerzas armadas 5
1.2.1.1 Organización 5
1.2.2 Policía nacional 6
1.2.2.1 Organización 6
1.2.3 Empresas de seguridad privada 7
1.2.3.1 Organización 7

1.3 Seguridad electrónica 8
1.3.1 Sistemas de seguridad electrónica 8
1.3.1.1 Estructura de un sistema 9
1.3.1.1.1 Central de monitoreo 9
1.3.1.1.2 Dispositivos sensores 10
1.3.1.1.3 Operadores 10

1.3.1.1.4 Equipos de alarma y alerta 10
1.3.1.1.5 Baterías 11
1.3.1.2 Sistema de monitoreo de alarma 12
1.3.1.2.1 Discriminador de audio 13
1.3.1.2.2 Sensor de rotura de vidrio 14
1.3.1.2.3 Sensor por contactos magnéticos 14
1.3.1.2.4 Detectores de presencia de doble tecnología 15
1.3.1.2.5 Sensores por infrarrojos pasivos 16
1.3.1.2.6 Sensores lineales 16
1.3.1.2.7 Sensores lineales de barrera de infrarrojos 17
1.3.1.2.8 Sensor de barrera por microondas 17
1.3.1.2.9 Central exterior 18
1.3.1.2.10 Central interior 18
1.3.1.2.11 Central selectora por zonas 19
1.3.1.3 Sistema de monitoreo de cámaras 20
1.3.1.4 Sistema de control de accesos 22
1.3.2 Complementos de la seguridad electrónica 23
1.3.2.1 Cristales blindados 23
1.3.2.2 Cerraduras de seguridad 24
1.3.2.3 Puertas blindadas 24
1.3.2.4 Puertas acorazadas 24
1.3.2.5 Cámaras acorazadas 24
1.3.2.6 Cajas fuertes 25
1.4 Explicación del proyecto 25

CAPÍTULO 2

ANÁLISIS DE VULNERABILIDAD DE LAS AGENCIAS DE RECAUDACIÓN

2.1 Requerimientos de la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito 27

2.2 Reconocimiento físico de las dependencias 28
2.2.1 Agencia de recaudación 12 de Octubre 29
2.2.1.1 Característica de seguridad física 29
2.2.2 Agencia de recaudación Atahualpa 30
2.2.2.1 Característica de seguridad física 31
2.2.3 Agencia de recaudación Iñaquito 32
2.2.3.1 Características de seguridad física 33
2.2.4 Agencia de recaudación La Luz 34
2.2.4.1 Características de seguridad física 35
2.2.5 Agencia de recaudación Mayorista 36
2.2.5.1 Características de seguridad física 37
2.2.6 Agencia de recaudación La Manzana 39
2.2.6.1 Características de seguridad física 39
2.2.7 Agencia de recaudación Carapungo 40
2.2.7.1 Características de seguridad física 41
2.2.8 Agencia de recaudación Quitumbe 42
2.2.8.1 Características de seguridad física 43
2.2.9 Agencia de recaudación Aeropuerto 44
2.2.9.1 Característica de seguridad física 45
2.2.10 Agencia de recaudación Parque Inglés 46
2.2.10.1 Características de seguridad física 46
2.2.11 Agencia de recaudación Ipiales del Sur 48
2.2.11.1 Características de seguridad física 48
2.2.12 Agencia de recaudación Chiriyacu 49
2.2.12.1 Característica de seguridad física 50
2.2.13 Agencia de recaudación Camal Metropolitano 51
2.2.13.1 Características de seguridad física 51
2.2.14 Agencia de recaudación San José Noroccidente 53
2.2.14.1 Características de seguridad física 53
2.2.15 Agencia de recaudación Chimbacalle 54
2.2.15.1 Característica de seguridad física 55

2.3 Vulnerabilidad de las agencias de recaudación 57

2.4 Análisis básico y ubicación de equipos 59
2.4.1 Características generales encontradas 59
2.4.2 Características específicas encontradas 61
2.4.2.1 Agencia de recaudación 12 de Octubre 63
2.4.2.2 Agencia de recaudación Atahualpa 65
2.4.2.3 Agencia de recaudación Iñaquito 67
2.4.2.4 Agencia de recaudación La Luz 70
2.4.2.5 Agencia de recaudación Mayorista 72
2.4.2.6 Agencia de recaudación La Manzana 74
2.4.2.7 Agencia de recaudación Carapungo 77
2.4.2.8 Agencia de recaudación Quitumbe 79
2.4.2.9 Agencia de recaudación Aeropuerto 81
2.4.2.10 Agencia de recaudación Parque Inglés 83
2.4.2.11 Agencia de recaudación Ipiales del Sur 86
2.4.2.12 Agencia de recaudación Chiriyacu 88
2.4.2.13 Agencia de recaudación Camal Metropolitano 91
2.4.2.14 Agencia de recaudación San José Noroccidente 93
2.4.2.15 Agencia de recaudación Chimbacalle 95

2.5 Diseño de instalaciones eléctricas para el sistema de seguridad electrónica 97
2.6 Funcionamiento General del Sistema de Seguridad Monitoreada 98

CAPÍTULO 3

DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA

3.1 Criterios generales 101
3.1.1 Determinación de enlace 101

3.1.1.2 Enlace ADSL 102
3.1.1.3 Enlace Agencia – Matriz 103
3.1.1.4 Enlace vía ADSL 103
3.1.1.5 Tiempos de respuesta del enlace 107
3.1.2 Procedimientos para instalación de equipos y correcto uso de materiales 110
3.1.2.1 Área de atención al público 111
3.1.2.2 Área de funcionarios EMAAP-Q 111

3.2 Determinación de zonas 112
3.2.1 Optimización de zonas 114
3.2.1.1 Agencia Chiriyacu 114
3.2.1.2 Agencia Parque Inglés 115
3.2.1.3 Agencia Aeropuerto 115
3.2.1.4 Agencia La Manzana 116

3.3 Especificaciones técnicas 119
3.3.1 Paneles de control 119
3.3.2 Teclado 122
3.3.3 Transmisor vía TCP/IP 124
3.3.4 Sirena 124
3.3.5 Gabinete de protección para la sirena 125
3.3.6 Botones de pánico 125
3.3.7 Baterías de respaldo para los paneles 125
3.3.8 Discriminador de audio 126
3.3.9 Contacto magnético para montaje en superficie 126
3.3.10 Contacto magnético lanfor tecnología direccionable 2 hilos 127
3.3.11 Contacto magnético lanfor 128
3.3.12 Sensor de movimiento 128
3.3.13 Botón de pánico inalámbrico 129
3.3.14 Receptor inalámbrico 129
3.3.15 Computador para soporte de software de la central de monitoreo 129

3.4 Requerimientos del software 130

3.5 Presupuesto referencial 132
3.5.1 Elección de marcas referenciales 132
3.5.2 Modelos de equipos 133
3.5.2.1 Panel de control Vista 128FBP 133
3.5.2.2 Teclado 6164SP 134
3.5.2.3 Transmisores de información vía IP 135
3.5.2.4 Sirena 135
3.5.2.5 Gabinete para sirena 136
3.5.2.6 Botones de pánico 136
3.5.2.7 Baterías de respaldo 137
3.5.2.8 Discriminador de audio 138
3.5.2.9 Contactos magnéticos para montaje en superficie 139
3.5.2.10 Contacto magnético lanfor tecnología direccionable 2 hilos 139
3.5.2.11 Contacto magnético lanfor 140
3.5.2.12 Sensor de movimiento 140
3.5.2.13 Botón de pánico inalámbrico y receptor 141
3.5.2.14 Cuadro resumido de costos 142

3.6 Implementación del sistema de seguridad electrónica 143
3.6.1 Equipos a utilizar 143
3.6.1.1 Panel de control DSC PC 5020 144
3.6.1.2 Teclado DSC PK5500 144
3.6.1.3 Sirena de 122 db Chowsons International 145
3.6.1.4 Transmisor vía TCP/IP 146
3.6.1.5 Dispositivos complementarios 147
3.6.2 Reconocimiento visual 147
3.6.2.1 Paneo exterior 147
3.6.2.2 Paneo interior 151
3.6.3 Instalación de dispositivos 154
3.6.3.1 Tendido del cableado 154
3.6.3.1.1 Primer tendido 156

3.6.3.1.2 Segundo tendido 158
3.6.3.1.3 Tercer tendido 159
3.6.3.1.4 Cuarto tendido 160
3.6.3.2 Posicionamiento de equipo 164
3.6.3.2.1 Instalación de botones de pánicos 164
3.6.3.2.2 Instalación del teclado de control 166
3.6.3.2.3 Instalación del magnético adhesivo 167
3.6.3.2.4 Instalación del sensor de movimiento PIR 168
3.6.3.2.5 Instalación de la sirena 169
3.6.3.2.6 Instalación del receptor inalámbrico Enkriptor 170
3.6.3.2.7 Instalación del panel de control y módulo T-Link 171
3.6.3.3 Acoplamiento de los dispositivos electrónicos al panel de control 172
3.6.3.3.1 Conexión del teclado 174
3.6.3.3.2 Conexión del T-Link 175
3.6.3.3.3 Conexión de dispositivos sensores de monitoreo 175
3.6.3.3.4 Cableado de dispositivos secundarios 178
3.6.4 Configuración del panel de control 179
3.6.4.1 Asignación del teclado 179
3.6.4.2 Supervisión de los módulos 180
3.6.4.3 Programación básica 180
3.6.4.4 Configuración del módulo T-Link 184

3.7 Instalación del software 185
3.7.1 Software de monitoreo de alarmas 186
3.7.1.1 Ejecución y configuración del software 190
3.7.2 Software de configuración remota de alarmas 200
3.7.2.1 Ejecución y configuración del software 206

CAPÍTULO 4

PRUEBAS Y RESULTADOS

4.1 Pruebas a través del software de configuración 213
4.1.1 Ingreso al sistema 213
4.1.2 Prueba de configuración remota de tiempo de vida 214
4.1.3 Prueba de armado remoto del sistema 217
4.1.4 Prueba de desarmado del sistema 218

4.2 Software de monitoreo 219
4.2.1 Prueba de vida del sistema 219
4.2.2 Prueba de botón de pánico 223
4.2.3 Prueba de botón de pánico inalámbrico 225
4.2.4 Prueba de reporte de cierre 226
4.2.5 Prueba de reporte de apertura 228
4.2.6 Prueba de fallo de energía 229
4.2.7 Revisión de historial 231
4.2.7.1 Exportación de historial a archivo XLS 233
4.2.8 Prueba de botones de pánico del teclado 235
4.2.8.1 Prueba de alarma de incendio 235
4.2.8.2 Prueba de emergencia médica 236
4.2.8.3 Prueba de robo en proceso 237

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones 239

5.2 Recomendaciones 241

REFERENCIAS BIBLIOGRÁFICAS 244

ANEXOS 245

RESUMEN

En el año 2007, la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito realizó un estudio para encontrar las posibles respuestas a una necesidad financiera planteada: reducción de personal de seguridad en todas las dependencias pertenecientes a la misma.

Como reemplazo a esta reducción de personal planteada se encontró una solución económicamente viable capaz de cumplir los requerimientos y necesidades de la Empresa: un monitoreo electrónico de sus instalaciones con la seguridad y confianza de una respuesta armada a cualquier necesidad presentada.

El proyecto aquí planteado consistió en la implementación de los dispositivos necesarios para realizar un seguimiento en tiempo real del estado físico de 12 agencias de recaudación de la EMAAP-Q, siendo parte del mismo y como necesidad para el monitoreo, la implementación de una central de vigilancia con comunicación vía ADSL entre paneles y central, aprovechando la conexión existente entre la matriz de la EMAAP-Q y sus dependencias.

Tras la implementación y puesta en marcha del Sistema de Seguridad Electrónica se obtuvieron resultados satisfactorios debido a la reducción del personal de seguridad privada, por ende, se efectuó una reducción del gasto vigilancia beneficiosa para la Empresa Metropolitana de Alcantarillado y Agua Potable Quito. Además, con los procedimientos y protocolos planteados por el Departamento de Seguridad Física, se ha concebido un control efectivo al acudir a una emergencia en progreso en todas las agencias de recaudación.

PRESENTACIÓN

Este proyecto tiene como fin optimizar de una manera efectiva, eficiente, eficaz y económica el Sistema de Seguridad Física Integral de la EMAAP-Q mediante el empleo de un sistema electrónico para el monitoreo de alarmas que permitan la aplicación de una respuesta armada para mantener el control sobre todos los elementos utilizados en la prevención de pérdidas.

Uno de sus objetivos es asegurar el desempeño del Departamento de Seguridad Física y Radio Comunicaciones de la EMAAP-Q mediante el empleo de un Sistema Integral de Seguridad Electrónica en apoyo directo a la Unidad de Seguridad Física, para alcanzar de esta manera, optimizar en un futuro todas las dependencias de la empresa al implementar el mencionado sistema.

La seguridad en las Agencias de Recaudación, Distritos, Plantas, Tanques, Bodegas y Pozos de la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito es de vital importancia para que el personal que labora en dichos sitios se encuentre continuamente respaldado, así como también es de vital importancia, reflejar dicha seguridad a toda la ciudadanía que se encuentra ligada a las mencionadas dependencias para recibir de ellas un bien o servicio.
Para comprender de mejor manera el trabajo aquí realizado, en el capítulo 1 se describen los conceptos necesarios para justificar el porque del desarrollo de este proyecto y los beneficios que el mismo conllevaría a la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito tras su implementación y puesta en marcha.

El capítulo 2 muestra los análisis de vulnerabilidad y los levantamientos realizados a las agencias de recaudación localizadas en distintas partes de la ciudad; estos consisten en brindar una clara idea de los equipos necesarios

para cubrir un óptimo sistema de alarmas y sus precisas ubicaciones en el área para el cumplimiento de su labor.

En el capítulo 3 se detalla los procedimientos de instalación y configuración de equipos, las normas que rigieron el mencionado proceso y la programación necesaria para la central de monitoreo con el fin de permitir una comunicación eficiente con los distintos paneles de control a instalar.

El capítulo 4 resume las pruebas realizadas con el sistema a pleno funcionamiento, los datos obtenidos del mismo y una memoria técnica sobre los eventos suscitados tras un periodo de dos meses de puesta en marcha.

Finalmente, en el capítulo 5 de detallan las conclusiones obtenidas tras la culminación del proyecto y las recomendaciones necesarias para el desarrollo del sistema en fases posteriores.

CAPÍTULO 1. DESCRIPCIÓN DE SISTEMAS DE SEGURIDAD ELECTRÓNICA

1.1 ORIGEN DEL TÉRMINO SEGURIDAD

El término seguridad proviene de la palabra latina *securitas*. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia.

La seguridad se puede definir como una sensación directamente ligada a la percepción de bienestar y tranquilidad por parte de una persona, ente o sistema en un medio abierto y de constante roce con el mundo y su movimiento.

En otras palabras, se podría relacionar a la seguridad con el campo alimenticio, industrial, social, vial, jurídico, etc. denotando que en todos ellos se define el bienestar como ente principal en su significado neto.

1.1.1 POLÍTICAS DE SEGURIDAD

Una política de seguridad hace referencia a la preparación de un plan de acción para enfrentar un riesgo en el caso que el mismo pueda presentarse súbitamente, o a su vez, imponer doctrinas capaces de mantener un cierto nivel de seguridad pre establecido.

Este debe prepararse analizando cada uno de los riesgos posibles que puedan atacar el bien a proteger, programando secuencias de manejo apropiado de la situación, movimiento adecuado del personal involucrado en el inconveniente, brindando protección inmediata al ente en riesgo y eliminando toda posible amenaza ligada a la situación de crisis.

1.1.2 DOCTRINA DE SEGURIDAD NACIONAL

La Doctrina de Seguridad Nacional, o comúnmente conocida por sus siglas como DSN, se basa principalmente en considerar a todas las personas que conformen un país como posibles amenazas a la seguridad de la misma.

Esta doctrina dio inicios con la llamada Guerra Fría, conflicto protagonizado por Estados Unidos y la Unión Soviética, con roces tanto en los campos y niveles ideológico, político, económico, tecnológico, militar e informativo.

La necesidad de la DSN la creó Estados Unidos y la divulgaron los países latinoamericanos, todo debido a que la primera potencia mundial estaba convencida que la Unión Soviética tenía como objetivo el convertirse en la única potencia mundial y reorganizar la sociedad mediante la expansión del comunismo soviético. Fue así que el temor los llevó a imaginar que los países sub desarrollados, específicamente de Latinoamérica, crearían focos de resistencia comunista, valiéndose de la influencia de la revolución cubana de 1959, y a la vez, que los estudiantes americanos con su creciente pensamiento comunista desarrollaran afecto al ideal soviético. Por primera vez surgía la idea de que el pueblo del propio país podía constituir una amenaza a la seguridad nacional.

En la actualidad, la doctrina de seguridad nacional propaga una visión amplia del enemigo, ya que no sólo se consideran terroristas insurgentes a las personas con armas como bombas o revólveres, sino también a las personas que propagan ideas en contra del concepto de la sociedad nacional que tiene el gobierno.

1.1.3 SEGURIDAD CIUDADANA

La seguridad ciudadana es un término que principalmente se refiere a la situación política actual de los países latinoamericanos. Trata específicamente

los temas de la lucha contra la violencia y delincuencia en los países que la conforman.

A diferencia del término Seguridad Nacional, la expresión de Seguridad Ciudadana contempla la prevención de incidentes internos salvaguardando la integridad de los ciudadanos de un país.

Existen dos conceptos y nociones del término "seguridad ciudadana" según la mayoría de conocedores del tema. El primero se refiere a una condición o un estado de un conjunto de seres humanos: a la ausencia de amenazas que ponen en peligro la seguridad de un conjunto de individuos. En ese sentido, el término tiene un significado normativo. Describe una situación ideal que probablemente es inexistente en cualquier lugar del mundo pero que funciona “como un objetivo a perseguir”

El segundo concepto se refiere a políticas públicas encaminadas a acercar la situación real a la situación ideal, es decir, se refiere a políticas que apuntan hacia la eliminación de las amenazas de seguridad o hacia la protección de la población ante esas amenazas. En ese sentido, el término se refiere a prácticas sociales empíricamente existentes.

1.1.4 SEGURIDAD COLECTIVA

La seguridad colectiva es un sistema dirigido a mantener la paz, sobre el cual, todo integrante del mismo acuerda con su grupo que un ataque hacia alguno de ellos será tratado como un ataque hacia todos y resultará en una respuesta militar colectiva inminente.

Las grandes alianzas en nuestro planeta que reflejan la “Seguridad Colectiva”, pueden ser ejemplificadas por la Organización del Tratado del Atlántico Norte (OTAN), así como la Organización de la Naciones Unidas (ONU).

Al emplear un sistema de seguridad colectiva, la ONU espera que sirva para disuadir a los estados miembros a actuar de manera que amenacen la paz y, de esta manera, minimizar las posibilidades de conflicto.

1.1.5 SEGURIDAD NACIONAL

Se refiere a la noción de estabilidad en la sociedad de un país, argumentando que la misma sería beneficiosa para el desarrollo del mismo.

Sus puntos clave se basan en precautelar los recursos del estado y las estrategias correctas para conseguirlo.

En sus inicios, los objetivos de la seguridad nacional se basan en su totalidad a prevenir conflictos armados, hoy en día, sus bases abarcan muchos puntos, sumando a los anteriores el trato adecuado al terrorismo, riesgos climáticos y medioambientales y la migración de su población a otros países.

1.2 ORGANISMOS DESTINADOS A LA SEGURIDAD

Ya sea partiendo de siglos anteriores hasta llegar a nuestra actualidad, toda sociedad existente en el mundo a poseído organismos o grupos sociales regidos por sus líderes con la misión de precautelar la integridad y mantener la paz interna de una comunidad.

Hoy en día, todos los países del mundo vigilan sus intereses propios con grupos de personas capacitados y normalizados a realizar actividades de prevención de riesgos.

Dentro de los organismos que brindan los mencionados servicios en un estado, se puede diferenciarlos y clasificarlos como aquellos destinados a la protección nacional: Fuerzas Armadas, y aquellos destinados a la protección interna o ciudadana: Policía Nacional y Empresas de Seguridad Privada.

1.2.1 FUERZAS ARMADAS

La historia de las Fuerzas Armadas se remonta a los mismos inicios del ser humano, ya que en estas instancias surgía la necesidad de formar sociedades o grupos humanos, los cuales, necesitaban defenderse de posibles amenazas por parte de otras sociedades o tribus.

Actualmente se puede definir a las Fuerzas Armadas como la institución militar de un país, siendo una organización capaz de actuar ante amenazas externas en caso de guerra y amenazas internas en respuesta a emergencias civiles en situaciones de desastre.

1.2.1.1 Organización

Tomando como ejemplo las Fuerzas Armadas ecuatorianas, y teniendo en cuenta que su estructura interna es compartida por la mayoría de países en el mundo, se puede dividir su organización como en la Figura 1.1, una fuerza terrestre, una fuerza aérea y una fuerza naval. Su comandante en jefe es el Presidente de la República y en su vértice jerárquico se encuentra el Jefe del Comando Conjunto de las Fuerzas Armadas.

Figura 1.1 *Las tres ramas de las Fuerzas Armadas Ecuatorianas*

1.2.2 POLICÍA NACIONAL

La policía nacional tiene como principal tarea mantener el orden interno de un país. Es un ente destinado a brindar seguridad a un individuo o sociedad, aplicando de ser necesario represión con el fin de hacer cumplir las normas y leyes jurídicas que rijan a un estado.

Las labores de la Policía Nacional se clasifican y dividen en muchas áreas y especializaciones, las cuales poseen sus debidas capacitaciones (Figura 1.2), debido a que el mencionado ente es el responsable directo de armonizar y mantener la paz interna de un país.

Figura 1.2 *Personal de la Policía Nacional en capacitación*

Algunas de las actividades que realiza esta entidad son: mantenimiento del orden público, la seguridad de las personas y de los bienes, la conservación de la moralidad pública, la prevención e investigación de los delitos, la aprehensión de los delincuentes, el control del tránsito, transporte terrestre y movimiento migratorio en el País; y, otras funciones de carácter general que deben cumplirse veinticuatro horas al día en todo el País.

1.2.2.1 Organización

En el Ecuador la Policía Nacional es dirigida por el Ministerio de Gobierno, el cual también maneja la Comisión Especial de Límites Internos de la

República, el Consejo Nacional de Tránsito y Transporte Terrestre, el Consejo Consultivo de Política Migratoria y el Consejo Nacional de Gobernadores.

1.2.3 EMPRESAS DE SEGURIDAD PRIVADA

Esta tiene como fin brindar sus servicios de protección y resguardo utilizando como medio un grupo humano certificado con las herramientas necesarias para aplicar dicho servicio, valiendo denotar que no es un servicio público, sino netamente privado.

Las empresas de Seguridad Privada al igual que la Policía Nacional se ven regida a leyes y reglamentos, valiendo denotar que en el uso y aplicación de los mismos, solo la Policía Nacional se ve facultada a realizar ciertas actividades como arrestos, requisas, uso de armas de fuego y control de tránsito.

Las empresas dedicadas a la seguridad privada solo se limitan al resguardo y protección de un área previamente establecida por el ente contratante, especificando este último claramente los alcances y limitaciones de las obligaciones en cuanto al servicio ya sea en horario de trabajo habitual (8 horas), permanente (24 horas), según la necesidad planteada.

La seguridad privada cumple muchas actividades, de las cuales vale destacar y dar a conocer los servicios de transporte y custodia de bienes, resguardo de instalaciones y guardias VIP o guarda espaldas

1.2.3.1 Organización

En el Ecuador las empresas de seguridad poseen una asociación que las representa: ANESI (Asociación Nacional de Empresas de Seguridad e Investigación Ecuador), la cual, es la única institución que agrupa a todas las empresas de Seguridad legalmente constituidas en el Ecuador.

1.3 SEGURIDAD ELECTRÓNICA

La Seguridad Electrónica se refiere a la aplicación de dispositivos electrónicos que cumplen la función de precautelar la integridad de personas o bienes materiales, informando y alertando de posibles agresiones a un organismo capaz de tratar y procesar dicha información para evitar inconvenientes.

El desarrollo de la misma como aplicación de la tecnología es sumamente grande debido a que avanza a la par de toda innovación efectuada en la industria electrónica. En la actualidad, se han desarrollado equipos capaces de informar de una cantidad muy grande de variables físicas que pueden ser aprovechadas para alertar una actividad considerada vital en el campo de la Seguridad Física.

Los campos que trata abarcan una gran cantidad de sistemas, pudiendo denotar aquellos destinados a las alarmas de intrusión, protección contra incendios, circuito cerrado de televisión, control de acceso, protección perimetral, automatización de portones y la integración/ automatización del hogar y la industria.

En esta búsqueda de optimizar la seguridad electrónica y a fin de unir los esfuerzos para lograr una protección integral de alta calidad, se debe orientar la eficiencia no solo a detectar y controlar las eventualidades, sino en tratar de evitarlas.

1.3.1 SISTEMAS DE SEGURIDAD ELECTRÓNICA

Existen diferentes tipos de sistemas de seguridad electrónica, cada uno de ellos se destina para ejercer seguimiento de alguna actividad específica.

En la actualidad los sistemas más comunes son los destinados a monitoreo de alarmas, monitoreo de cámaras y control de accesos. Todos estos, consignados a vigilar las instalaciones sobre las cuales se los implementará.

1.3.1.1 Estructura de un Sistema

Todos los sistemas de seguridad electrónica comparten en común su estructura primaria, estando ésta conformada por una central de monitoreo, los dispositivos sensores que alertarán los cambios de variables físicas en el sistema, un operador que verifique su estado y los equipos de alarma para alertar las emergencias presentadas.

1.3.1.1.1 Central de Monitoreo

El monitoreo se refiere a la vigilancia de un individuo o sistema, la interpretación de los datos que salen del mismo, todo con el fin de reconocer situaciones de alarma. El planteamiento de que éste sea electrónico indica que los dispositivos necesarios para hacer su vigilancia se van a valer de la tecnología, para emitir, transmitir e informar situaciones consideradas inapropiadas para el sistema de monitoreo en cuestión.

Dentro de las bases principales que pueden tener los diferentes Sistemas de Seguridad Electrónica, se puede resaltar el lugar considerado clave para realizar esta actividad: la Central de Monitoreo

El Centro de Monitoreo cumple la funcionalidad de monitorear uno o varios sistemas de seguridad electrónica, centralizando toda la información de ingreso en uno o varios monitores para facilitar el trabajo de los operadores para el control de personas, bienes o activos.

Reciben vía radio, teléfono, GPRS, Internet u otro medio de comunicación el salto de la alarma y se encargan de poner en marcha los mecanismos de actuación previstos como pueden ser el envío de las fuerzas del orden, de los bomberos o ayuda médica urgente, así como el envío de algún vigilante de una empresa de seguridad.

Figura 1.3 *Central de monitoreo*

1.3.1.1.2 Dispositivos sensores

Estos equipos deben sensar los cambios en las variables físicas que puedan ser interpretadas como modificaciones en la estructura de un sistema de vigilancia.

1.3.1.1.3 Operadores

Esta persona tiene el deber de alertar cualquier actividad considerada como inusual o no permitida en un sistema, informando dichos acontecimientos a un ente capacitado para reaccionar oportunamente a la emergencia.

Para cumplir sus funciones debe utilizar todas las interfaces que la central de monitoreo le pueda brindar, basándose principalmente en la utilización de monitores de computadoras, teléfonos y radios.

1.3.1.1.4 Equipos de alarma y alerta

Estos pueden constar de elementos visuales o acústicos que tienen la función de alertar a las personas a cargo de las instalaciones de que algo está sucediendo y de ahuyentar a los intrusos.

Por ejemplo, las sirenas (Figura 1.4) emiten ruidos agudos que alcanzan los 120 dB de potencia siendo muy molestas para el intruso. Estas sirenas además de perturbar al intruso le aíslan acústicamente de lo que sucede en el exterior porque no le permite escuchar la proximidad de un ente de respuesta a la situación de emergencia.

Figura 1.4 *Sirena de 120 db*

Los equipos de alarma y alerta tienen una importante función dentro del sistema de seguridad, pues sin ellos de nada servirían los detectores. A través de la activación de estos elementos el intruso es consciente de que el sistema le ha detectado y de que los servicios de seguridad están en camino, estos elementos tienen una clara intención intimidatoria y persuasiva.

Cabe mencionar que para un funcionamiento a prueba de sabotajes o inconvenientes presentados, es necesario hacer sistemas robustos, incluyendo a los mismos ciertos equipos capaces de mantener la función global sin ningún percance.

1.3.1.1.5 Baterías

Las baterías (Figura 1.5) cumplen la función de dotar de electricidad al sistema a pesar de que el mismo sufra una pérdida en su suministro eléctrico general. Su autonomía depende directamente de la relación Amph (amperio sobre hora) y el propio sistema avisa a la Central de Monitoreo que se ha cortado el suministro eléctrico y se ha activado el suministro auxiliar.

Figura 1.5 *Batería de 6 V, 4.5 Amph*

1.3.1.2 Sistema de Monitoreo de Alarmas

El Sistema de Monitoreo de Alarmas se dedica a precautelar el robo o ingreso no permitido a una instalación física de un ente que pueda amenazar la integridad del mismo.

Se encuentra conformado por una central de monitoreo, paneles de control, sensores de movimiento, botones de pánico, etc. que en conjunto conforman este tipo de sistema, teniendo en cuenta que cada uno de los dispositivos que puede ser acoplado tiene una razón de implementarse según la necesidad del propietario.

Su central receptora de alarmas recibe toda la información que concierne a un sistema capaz de monitorear eventos considerados como atentados a los componentes del mismo. Su ubicación difiere de la finalidad del mismo. Existen centrales manejadas por empresas de seguridad que se ocupan de vigilar los recintos donde se han instalado los sistemas pertenecientes a la misma, así como existen centrales propias de empresas privadas, que monitorean sus instalaciones con su propio personal y recursos humanos.

Las centrales están conformadas por un computador sobre el cual se almacena toda la información proveniente de las instalaciones monitoreadas. Este tipo de eventos pueden ser: saltos de la pre alarma y alarma, fallos de

batería o falta de electricidad en la instalación, sabotaje y conexiones/ desconexiones de la alarma; indicando siempre y manteniendo como información vital en todo momento las fechas, horas y minutos en los que ocurren los eventos detallados.

Una propiedad que pueden tener estos sistemas, es que permiten la desconexión por coacción, en la que el propietario aparentemente desconecta la alarma pero el sistema avisa a la central de alarmas de que el usuario está desconectando el sistema bajo amenaza.

Las principales características de una central de alarmas son:

- Conexión y desconexión.
- La central de alarmas dispone de mecanismos para controlar el acceso a las zonas protegidas, y efectuar su conexión y desconexión, en los sistemas avanzados, se pueden activar unas zonas mientras otras permanecen desactivadas.
- Todas las centrales tienen sus propios mecanismos anti sabotaje.
- Botones de aviso a la central de alarmas: policía, bomberos, urgencias médicas.
- Conexión desconexión remota.
- Aviso situación de atraco.

Los dispositivos que conforman un Sistema de Monitoreo de Alarmas común pueden ser:

1.3.1.2.1 Discriminador de audio

Este tipo de sensores activan la alarma si detectan la rotura del cristal. El sensor cuando está activado queda “escuchando” los ruidos que se producen a su alrededor y, activan el sistema en caso de que se produjera un ruido agudo como el producido en la rotura de un cristal. Estos sensores se instalan cerca del cristal a proteger, pero nunca en el propio cristal. (Figura 1.6)

Figura 1.6 *Discriminador de Audio DSC, modelo Acuity*

1.3.1.2.2 Sensor de rotura de vidrio

A diferencia de un discriminador de audio, este tipo de sensor se coloca sobre el cristal que se desea monitorear. (Figura 1.7) Su función específica se basa en la detección de vibraciones, mismas que pueden ser producidas por un forcejeo de la misma al intentar romperla o trisarla.

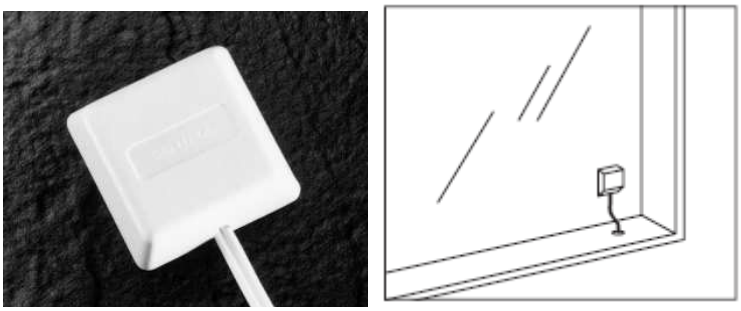


Figura 1.7 *Sensor de rotura de vidrio SENTROL. Se muestra la forma en que debe ser colocado*

Su tecnología se basa en un transductor piezoeléctrico, razón por la cual dicho dispositivo no necesita alimentación externa, al contrario, el mismo produce una variación eléctrica por excitación del cristal del que esta compuesto.

1.3.1.2.3 Sensor por contactos magnéticos

Constan de dos piezas colocadas, una en el marco de la puerta o ventana y otra en la hoja de apertura. Se instalan directamente sobre la superficie a proteger, detectan la apertura de puertas, ventanas e ingresos tipo lanfor.

Su funcionamiento se basa en unas láminas que por la acción de la atracción del campo magnético formado por un imán, cierran el circuito. (Figura 1.8)

Figura 1.8 *Contactos magnéticos Honeywell con cable reforzado*

Al abrir la puerta o ventana, se separa el imán de las láminas y éstas, al separarse, interrumpen la corriente del circuito establecido activando así la alarma. Existen distintos modelos de sensores dependiendo de su aplicación, ya sea en caso de que el mismo deba funcionar o no en la intemperie, sobre tensiones, a prueba de golpes, puertas metálicas, de madera, etc.

1.3.1.2.4 Detectores de presencia de doble tecnología

Se trata de detectores de presencia evolucionados a partir de los sensores de radar y de los sensores volumétricos, básicamente sería como incluir los dos detectores en un mismo elemento de forma que la alarma se activaría sólo en el caso de que se activaran los dos, evitando con ello las falsas alarmas.

En el mercado se lo conoce también como sensor DUAL TEC.

Los antiguos sensores por radar, funcionaban con un emisor de microondas y un receptor en el mismo elemento, de forma que cuando en la zona vigilada varían las ondas reflejadas (por la intrusión) el detector envía una señal eléctrica a la central con la que se activa la alarma.

Los sensores volumétricos detectan el movimiento dentro de un volumen determinado. Se instalan siempre dentro de los locales y cubren varios metros cuadrados. Su campo de detección (Figura 1.9) varía desde los 6 metros

cuadrados hasta los 70 o incluso más, aumentando con ello, claro está, su precio. Los sensores por radar y volumétricos simples prácticamente no se utilizan pues su evolución natural ha dado paso a los detectores de presencia de doble tecnología.

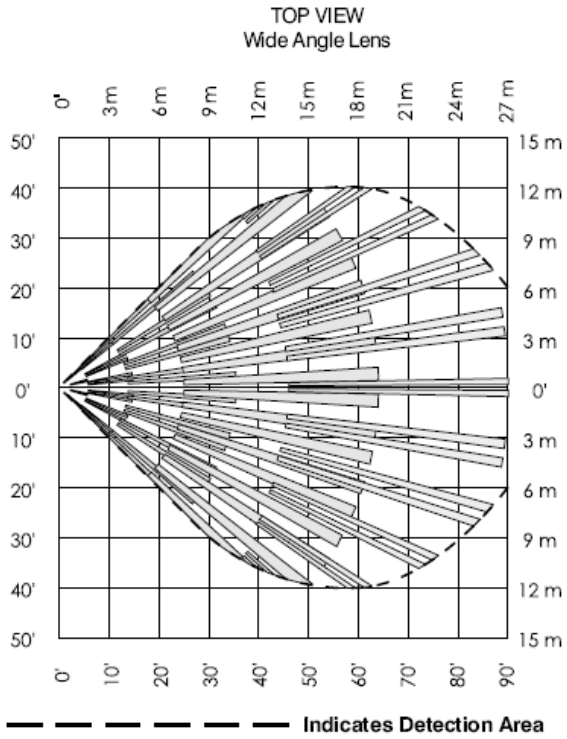


Figura 1.9 *Campo de detección típico de un sensor de movimiento*

1.3.1.2.5 Sensores por infrarrojos pasivo

El sensor por infrarrojos pasivo o PIR, memoriza la cantidad de luz infrarroja existente en la zona vigilada y cuando se produce en ella una variación en estas radiaciones, es captada por el detector, accionando la alarma. El detector cubre áreas en forma de abanico.

1.3.1.2.6 Sensores lineales

Los sensores lineales son sensores que actúan al romperse una determinada barrera debido al paso por ella de un individuo u objeto. La instalación se compone de un elemento emisor y un receptor y pueden ser por infrarrojos o microondas.

1.3.1.2.7 Sensores lineales de barrera de infrarrojos

Un emisor lanza 2 haces de luz invisibles hacia el receptor situado a varias decenas de metros. (Figura 1.10) Los dos haces están separados uno del otro por unos 10 o 15 cm. Estos haces son recogidos por el receptor saltando la alarma sólo en el caso de que se corten ambos haces a la vez. Este tipo de sensores pueden llegar a cubrir distancias de 600 metros lineales. Son detectores bastante caros.

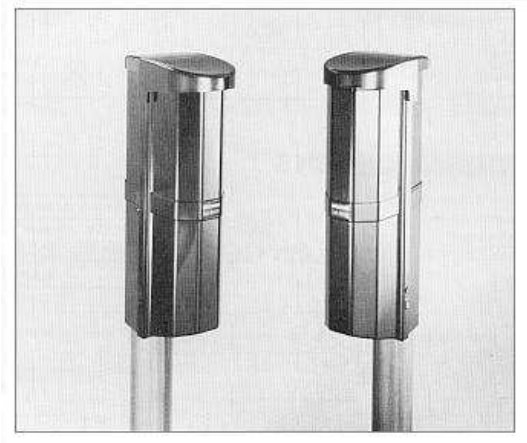


Figura 1.10 *Barrera Infrarroja de doble haz montada sobre pedestal*

1.3.1.2.8 Sensor de barrera por microondas

A veces, se utiliza en los perímetros a proteger un sistema de barrera por microondas, que consiste en la colocación de unos cables especiales enterrados. El emisor lanza impulsos eléctricos de alta frecuencia sobre el terreno a proteger formando una onda de superficie. En condiciones normales la onda permanece inalterable y si se produce una intrusión la onda varía, percibiéndolo el receptor y haciendo saltar la alarma. Son instalaciones caras y poco utilizadas a nivel de instalaciones de viviendas o pequeños locales.

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

1.3.1.2.9 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 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.

1.3.1.2.10 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 accesos e incendios.

Las mismas varían principalmente por el número de zonas que posea y la cantidad tope a la que se pueda expandir.

Poseen características específicas que valen ser tomadas en cuenta al momento de adquirirlas, como los son: modo de transmisión de la información, tipo de sensores permitidos, dedicada solo a robo, robo – accesos, o robo – accesos –incendio.

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

La central, 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.

Se trata de centrales más complejas y más fiables que las de exterior, proporcionan ciertas posibilidades muy importantes:

- Programación de tiempos: salida y entrada de cada zona.
- Comunicación permanente con la Central de Monitoreo.
- Aviso de situación de atraco, de necesidades médicas, bomberos.
- Circuito támper, etc.

En la Figura 1.11 se puede observar un panel de control interior, conjuntamente con la variedad de dispositivos que se pueden acoplar al mismo.

Figura 1.11 *Panel de control y dispositivos para seguridad electrónica*

1.3.1.2.11 Central selectora por zonas

Se trata de una variante de la Central Interior en la que el propio equipo comunica a la central cual es el detector/detectores que se han accionado para seguir la pista del intruso si se desplaza por el recinto y así actuar en consecuencia.

Las instalaciones de seguridad física se pueden complementar con la instalación de sistemas de monitorización y grabación de eventos, pudiendo los mismos estar permanentemente grabando o accionarse de forma automática o manual en caso de situación de robo o atraco.

1.3.1.3 Sistema de monitoreo de cámaras

Este tipo de central se dedica exclusivamente al monitoreo de sistemas denominados como Circuito Cerrado de Televisión (CCTV).

Los equipos que utiliza son cámaras de seguridad las cuales enfocan lugares sensibles a amenazas. Las imágenes aquí obtenidas son transmitidas vía cable coaxial (comúnmente de 75 Ohms) a una central de monitoreo; ésta procede a almacenarlas en formato dedicado a video en un equipo DVR (Digital Video Recorder) y a la par, muestra las mencionadas grabaciones en tiempo real en uno o varios monitores según la necesidad y predisposición de los operadores. (Figura 1.12)

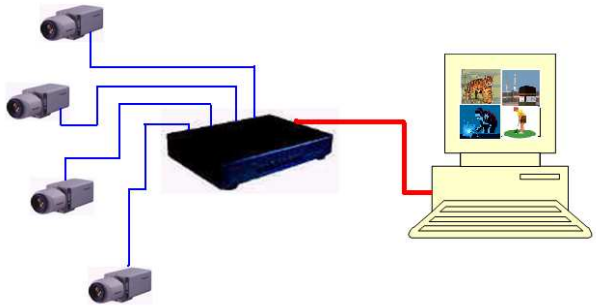


Figura 1.12 *Esquema de un Circuito Cerrado de Televisión*

La denominación de “Circuito Cerrado de Televisión” se debe a dos grandes diferencias que posee con la visualización de imágenes en televisión que comúnmente se conoce:

- Todos sus componentes se encuentran entrelazados, es decir, no existe difusión abierta, y

- Es un sistema dedicado para un número concreto y definido de personas. No es de carácter público.

Este tipo de sistema inició con fines muy limitados debido a la tecnología que utilizaba, sus fines radicaban principalmente en el monitoreo de una instalación cercana al punto de grabación de las imágenes y envío del respectivo registro de eventos.

Actualmente y debido a los adelantos tecnológicos en esta área, se poseen cámaras de alta resolución con capacidades de variar sus características como panorámica, enfoque, inclinación y zoom; ya sea utilizando como comunicación para este fin los protocolos RS232, RS485, PELCO o mediante enlace vía internet utilizando direcciones IP.

Los usos para este tipo de sistemas pueden ser muy grandes; se pueden destacar las siguientes debido a las altas prestaciones que se presentan para las mismas:

- Monitoreo de viviendas
- Prevención de actos vandálicos
- Vigilancia en comercios
- Supervisión de obras
- Monitoreo de prisiones
- Monitoreo de instalaciones dedicadas a la recaudación de dinero

Debido a que el funcionamiento de una cámara de seguridad es permanente tanto en el día como en la noche, y siendo sumamente necesaria la grabación a poca luz para realizar un monitoreo eficiente, se ha adaptado a las mismas un mecanismo de visualización nocturna, conformada por LEDS infrarrojos.

Existe una gran variedad de cámaras de video vigilancia destinadas a cubrir las más diversas necesidades. Se puede encontrar cámaras para instalaciones de interior, con carcasa estanca para exterior, con infrarrojos

para visión nocturna, ocultas en diferentes dispositivos, con carcasa irrompible anti vandálica, con óptica intercambiable, con señal de vídeo inalámbrica o con servidor web de vídeo incorporado para ver por Internet (más conocidas como cámaras IP).

1.3.1.4 Sistema de control de accesos

Un sistema de control de accesos permite la conexión y desconexión de los sistemas de seguridad tipo cerradura electrónica.

Para la lectura de la información se pueden utilizar teclados o lectoras de radio frecuencia, en el primero de estos casos, la información es ingresada digitando cierta cantidad de números, los cuales se comparan con una base de datos en la central de monitoreo y se procede a conceder o negar el acceso a cierta área.

En el uso de lectoras de radio frecuencia RFID, como se muestra en la Figura 1.13, se utiliza tarjetas magnéticas con un chip de identificación único. Para otorgar o negar un ingreso, la lectora confirma el número de tarjeta y su registro sobre la base de datos.

Figura 1.13 *Lectora RFID*

El uso de este sistema de seguridad electrónica permite una administración electrónica de visitantes, ingresos y egresos de personal, verificación en

cumplimientos de horarios, etc. El único fin es salvaguardar las instalaciones y el personal de una empresa al impedir el acceso no autorizado de público en general a la misma.

Debido a que un control de accesos óptimo se encuentra distribuido en toda una edificación, se puede aprovechar el mismo para rastreo y ubicación de personal y visitantes para realizar evacuaciones exitosas en caso que se encuentre sufriendo cierto tipo de percances físicos como un incendio o atentado terrorista.

Gozan de mayor seguridad los dispositivos que sólo pueden desconectarse por teclado en lugar del accionamiento a través de llave o tarjeta magnética, pues éstas se pueden perder o robar, mientras que para la desconexión a través de teclado hace falta saber los códigos que la desactivan y son fáciles de cambiar si es necesario por el administrador del sistema.

1.3.2 COMPLEMENTOS DE LA SEGURIDAD ELECTRÓNICA

Existen ciertos dispositivos o conjuntos de equipos capaces de complementar la noción de seguridad, aliándose con la seguridad electrónica para brindar completa satisfacción a una necesidad.

1.3.2.1 Cristales blindados

Este tipo de elementos se utiliza en ciertas áreas de seguridad perimetrales o de interiores. Los cristales blindados, por sus características son capaces de soportar impactos violentos, ofreciéndo una excelente protección contra robo y agresiones, dependiendo el nivel de blindaje, son capaces de resistir impactos de armas de diversos calibres, sin ser perforados. Las principales aplicaciones de los cristales blindados suelen ser instalaciones de seguridad correspondientes a bancos, joyerías, agencias de recaudación, etc.

El cristal blindado está compuesto por varias capas de vidrio que van intercaladas en una o varias capas de materiales sintéticos, generalmente poli carbonatos con los que se obtiene una gran resistencia a los proyectiles.

1.3.2.2 Cerraduras de seguridad

Con objeto de impedir la entrada a las personas no autorizadas a la zona protegida se instalan cerraduras de seguridad que por sus características hacen muy difícil su anulación. Cerraduras anti-taladro, anti-tarjeta, anti-ácido, etc.

1.3.2.3 Puertas blindadas

Son las más utilizadas como puertas de acceso a oficinas y comercios. Las puertas tienen una chapa de acero de dos milímetros de grosor en cada una de las dos caras de la puerta. Al cerrar con la acción de la llave, la puerta queda bloqueada por cuatro lados, es decir que un mecanismo accionado por la llave hace que cuatro barras de acero se introduzcan en el marco superior, el inferior y en los laterales.

1.3.2.4 Puertas acorazadas

Son puertas de mayor resistencia que las anteriores tanto en su estructura, formada por tubos de acero y hormigones especiales, como en los mecanismos de cierre y de cerradura. Este tipo de puerta es más cara que la anterior.

1.3.2.5 Cámaras acorazadas

Son habitaciones de alta seguridad que tienen como objeto proteger los bienes albergados en su interior, normalmente tienen una puerta de acceso de al menos 20 centímetros de grosor formadas por planchas de acero. Las

paredes techo y suelo suelen estar formadas también por planchas de acero y hormigón.

1.3.2.6 Cajas fuertes

Se utiliza este tipo de dispositivos para guardar cosas de gran valor como pueden ser joyas y documentos. Están fabricadas con materiales metálicos tratados para conseguir una mayor dureza. Su apertura puede ser con llave, con tarjeta, con combinación numérica o la combinación de ambos sistemas. Se suelen colocar en lugares discretos ya se trate de la vivienda o la oficina y se anclan a la pared o el suelo mediante obra.

1.4 EXPLICACIÓN DEL PROYECTO

Este proyecto tiene como fin dotar a la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito un Sistema de Seguridad Electrónica capaz de monitorear sus dependencias las 24 horas, los 365 días del año, a través de conexiones vía ADSL.

Contemplará el análisis, diseño y configuración de todos los equipos y accesorios necesarios para el correcto funcionamiento del Sistema Integrado de Seguridad Electrónica en las dependencias de la EMAAP-Q, constando los mismos de paneles de control, sensores, dispositivos para transmisión/ recepción de datos y central de monitoreo para procesamiento de la información. Los doce paneles de control transmitirán su información pertinente a la Central de Monitoreo mediante enlaces tipo ADSL administrados por el Departamento de Recursos Informáticos, utilizando la infraestructura actual que posee la EMAAP-Q con estas dependencias.

Debido a que el deseo de la Empresa Metropolitana de Alcantarillado y Agua Potable es obtener un sistema capaz de expandirse e integrar en un futuro los subsistemas de seguridad electrónica como Circuitos Cerrados de Televisión

y Control de Accesos, este proyecto contempla la elección de los equipos específicos para que integren a futuro estos requerimientos.

La implementación de un sistema electrónico de seguridad integrado, permitirá ejercer una adecuada vigilancia electrónica y facilitará las funciones que realiza el personal de operadores del Centro de Seguridad, mediante la integración en un software único de administración y control, de los sistemas de circuito cerrado de televisión, control de accesos, e intrusión; interrelacionando las diferentes aplicaciones de cada sistema, mediante programación lógica a través de software; todo esto, con la finalidad de salvaguardar la integridad de los recursos humanos, tecnológicos, valores en custodia, información y bienes de las dependencias de la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito.

CAPÍTULO 2. ANÁLISIS DE VULNERABILIDAD DE LAS AGENCIAS DE RECAUDACIÓN

2.1 REQUERIMIENTOS DE LA EMPRESA METROPOLITANA DE ALCANTARILLADO Y AGUA POTABLE DE QUITO

El Departamento de Seguridad Física y Radio Comunicaciones es el ente destinado a velar la integridad de todo el personal de la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito. También es responsable de las personas ajenas a sus instalaciones que realicen visitas temporales a las mismas, para obtener un servicio público como respuesta a una necesidad.

Con el deseo de optimizar sus recursos, brindar un mejor servicio y tecnificar sus labores, el Departamento de Seguridad Física y Radio Comunicaciones planteó la reducción de vigilantes de seguridad privada y la colocación en su reemplazo de un Sistema Electrónico, capaz de monitorear sus dependencias permanentemente; alertando, a una central de alarmas, todo tipo de inconvenientes, y, comunicando dichas emergencias a una empresa de seguridad que sea capaz de brindar el servicio de Respuesta Armada.

El Departamento de Seguridad Física y Radio Comunicaciones dió las pautas a seguir para la ejecución de este sistema. Dentro de las características que el mismo debía cumplir se encontraban:

- La Empresa Metropolitana de Alcantarillado y Agua Potable de Quito debía poseer su propia Central de monitoreo, independiente de cualquier empresa privada que pueda prestar el servicio de monitoreo permanente.
- La Central de Monitoreo debía encontrarse en las instalaciones del edificio matriz de la EMAAP-Q, específicamente en las oficinas de la Unidad de Seguridad Física.

- La comunicación de la Central con las Agencias de Recaudación debía ser permanente, las 24 horas, los 365 días.

Para efectuar el Análisis del Sistema de Seguridad Electrónica para la EMAAP-Q, se lo dividió al mismo en dos fases que debían ejecutarse secuencialmente para cumplir la meta programada. Estas fueron:

- Reconocimiento visual y análisis de las dependencias de la EMAAP-Q sobre las cuales se implementará el proyecto, y
- Diseño y configuración de los equipos electrónicos en cada una de las instalaciones.

2.2 RECONOCIMIENTO FÍSICO DE LAS DEPENDENCIAS

Este reconocimiento se vuelve la base principal del proyecto, ya que del mismo nace la necesidad de elección de los equipos adecuados para cada dependencia, teniendo en cuenta variables propias de cada una de ellas como lo son la función de trabajo que cumpla, la cantidad de personal laborando en la misma, y el flujo diario de particulares que la visiten.

Las dependencias a considerar en el Proyecto de Seguridad Electrónica son:

- Agencia de Recaudación 12 de Octubre
- Agencia de Recaudación Atahualpa
- Agencia de Recaudación Iñaquito
- Agencia de Recaudación La luz
- Agencia de Recaudación Mayorista
- Agencia de Recaudación La Manzana
- Agencia de Recaudación Carapungo
- Agencia de Recaudación Quitumbe
- Agencia de Recaudación Aeropuerto
- Agencia de Recaudación Parque Inglés
- Agencia de Recaudación Ipiales del Sur

- Agencia de Recaudación Chiriyacu
- Agencia de Recaudación Camal Metropolitano
- Agencia de Recaudación San José Noroccidente
- Agencia de Recaudación Chimbacalle

Antes de empezar a describir el estado actual en cuanto se refiere a la seguridad física de cada una de las agencias mencionadas anteriormente, cabe mencionar que una de las características que cumple toda Agencia de Recaudación es que la instalación cuenta con el servicio de energía eléctrica de la Empresa Eléctrica Quito S.A., además, posee un sistema eléctrico de emergencia UPS de 1,5 [KVA].

2.2.1 AGENCIA DE RECAUDACIÓN 12 DE OCTUBRE

La Agencia 12 de Octubre está ubicada en la Av. 12 de Octubre y Juan Montalvo 15-156, Barrio El Dorado, Parroquia Santa Prisca, Quito – Ecuador. Como se puede observar en la Figura 2.1, esta agencia consta de tres cubículos de los cuales dos son de recaudación y el sobrante de facturación.

Figura 2.1 *Atención al cliente, Agencia 12 de Octubre*

2.2.1.1 Características de Seguridad Física

- El único acceso a la dependencia es por una puerta metálica tipo lanfor.

- La Agencia de Recaudación posee ventanales protegidos por recubrimientos metálicos lanfor, pero su diferencia radica en que las mismas nunca son abiertas.

- Posee puerta y ventanillas pertenecientes al área interior (también denominada como bunker) blindadas. (Figura 2.2)

Figura 2.2 *Interior de la Agencia de Recaudación 12 de Octubre*

- Dos guardias de seguridad protegiendo la instalación de 8 de la mañana a 4 de la tarde.

- Posee dos cámaras de seguridad pertenecientes a su sistema local de CCTV.

2.2.2 AGENCIA DE RECAUDACIÓN ATAHUALPA

La Agencia de Recaudación Atahualpa (Figura 2.3) está ubicada en la calle Juan Lagos, entre la Av. Maldonado y Pedro Carpio, en las afueras del centro comercial que lleva su nombre. Consta de tres cubículos de los cuales dos son de recaudación y el sobrante de facturación.

Figura 2.3 *Ingreso a la Agencia de Recaudación Atahualpa.*

2.2.2.1 Características de Seguridad Física

- Como se puede ver en la Figura 2.4, la puerta única de ingreso tiene un recubrimiento metálico tipo lanfor, y la única ventana de la dependencia tiene rejas metálicas además de la posibilidad de sellar la misma con recubrimiento lanfor.

Figura 2.4 *Ingreso a la Agencia de Recaudación Atahualpa. (Vista interior)*

- Posee ventanillas y puerta de acceso a las cajas con protección de blindaje antivandálico. (Figura 2.5)

Figura 2.5 *Puerta blindada. Ingreso al área resguardada*

- Posee sistema de Circuito Cerrado de Televisión local conformado por cuatro cámaras.

- Dos guardias de seguridad brindan protección a la misma de 8 de la mañana a 4 de la tarde.

2.2.3 AGENCIA DE RECAUDACIÓN IÑAQUITO

La Agencia Iñaquito está ubicada en la Av. Amazonas y Pereira N38 -112, en la Administración Zonal Norte del Municipio, Quito – Ecuador. Como muestra la Figura 2.6, en esta agencia existen tres cubículos de los cuales dos son de recaudación y el sobrante de facturación.

Figura 2.6 *Area de Atencion al Publico. Agencia Iñaquito*

2.2.3.1 Características de Seguridad Física

- No posee Circuito Cerrado de Televisión.

- Cuenta con un guardia de seguridad que trabaja en el horario de 8 a 16 horas. Cabe mencionar que adicionalmente, pose vigilancia extra perteneciente a la Administración zonal, la cual protege las instalaciones durante las 24 horas del día.

- Las ventanillas para atención al público y la puerta de acceso a las mismas no son blindadas. (Figura 2.7)

Figura 2.7 *Interior de la Agencia de Recaudación Iñaquito*

- Los ventanales con vista al patio interno de la Administración Zonal no poseen ningún tipo de protección. (Figura 2.8)

Figura 2.8 *Area posterior de la Agencia Iñaquito*

2.2.4 AGENCIA DE RECAUDACIÓN LA LUZ

La Agencia La Luz se encuentra ubicada en las calles Francisco Guarderas y Capitán Ramos (Figura 2.9), Sector La Luz, Quito - Ecuador. Esta instalación se encuentra rodeada del parque que se encuentra en esta zona residencial.

Figura 2.9 *Ingreso a la Agencia de Recaudación La Luz. (Vista exterior)*

La dependencia consta de un cerramiento de malla metálica y la guardianía que realiza la labor de vigilancia está compuesta por dos personas. Como muestra la Figura 2.10, posee tres cubículos, dos de recaudación y uno de facturación.

Figura 2.10 *Area de Atención al Público, Agencia La Luz*

2.2.4.1 Características de Seguridad Física

- Posee un sistema de Circuito Cerrado de Televisión que cuenta con cuatro cámaras de seguridad ubicadas estratégicamente para mostrar los lugares de conflicto de la agencia.

- Tiene guardianía de 8 a 18 horas, mediante dos guardias de seguridad armados.

- La Figura 2.11 muestra la ubicación física de la dependencia. Limita con un parque, separando ambas zonas únicamente por malla metálica. Por eso se considera el área crítica de la Agencia de Recaudación.

Figura 2.11 *Area critica Agencia La Luz*

- La puerta de acceso del personal a esta agencia es blindada. (Figura 2.12)

Figura 2.12 *Ingreso de personal EMAAP-Q a la Agencia*

- Las ventanillas de atención son blindadas, y además, poseen rejas metálicas para ejercer mayor seguridad. (Figura 2.13)

Figura 2.13 *Interior de la Agencia La Luz*

2.2.5 AGENCIA DE RECAUDACIÓN MERCADO MAYORISTA

La Agencia de Recaudación Mercado Mayorista se encuentra ubicada en la Av. Teniente Hugo Ortiz y Pasaje 20 (Figura 2.14), cercana al mercado que lleva su nombre. La agencia consta de tres cubículos, dos de recaudación y uno de facturación.

Figura 2.14 *Ingreso Agencia Mayorista*

2.2.5.1 Características de Seguridad Física

- Como muestra la Figura 2.15, el único acceso a la dependencia tiene protección de puerta tipo lanfor.

Figura 2.15 *Ingreso a la Agencia de Recaudación Mayorista. (Vista interior)*

- La única ventana de la dependencia posee una reja metálica interna que brinda protección extra a las lanfor colocada en su exterior. (Figura 2.16)

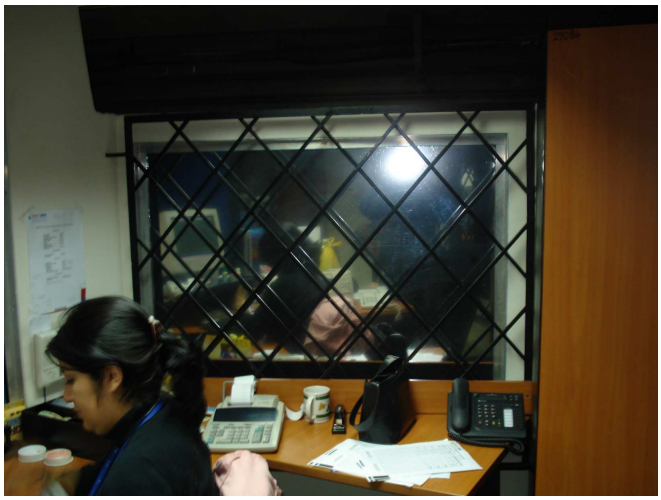


Figura 2.16 *Reja interna, Agencia Mayorista*

- La Figura 2.17 muestra las ventanillas de la agencia, que al igual que la puerta de ingreso del personal poseen blindaje a prueba de actos vandálicos.

Figura 2.17 *Ventanillas blindadas, Agencia Mayorista*

- Consta de un sistema de Circuito Cerrado de Televisión compuesto por cuatro cámaras de seguridad.

- Tiene guardianía de 8 a 16 horas, con dos guardias armados privados.

2.2.6 AGENCIA DE RECAUDACIÓN LA MANZANA

La Agencia de Recaudación La Manzana se encuentra ubicada en la Calle Venezuela y Bolívar, en el centro histórico de la ciudad de Quito, dentro del centro comercial que lleva su nombre.

2.2.6.1 Características de Seguridad Física

- Su ubicación estratégica es en el segundo piso de la edificación. El acceso único y principal está protegido por una puerta metálica corrediza. (Figura 2.18)

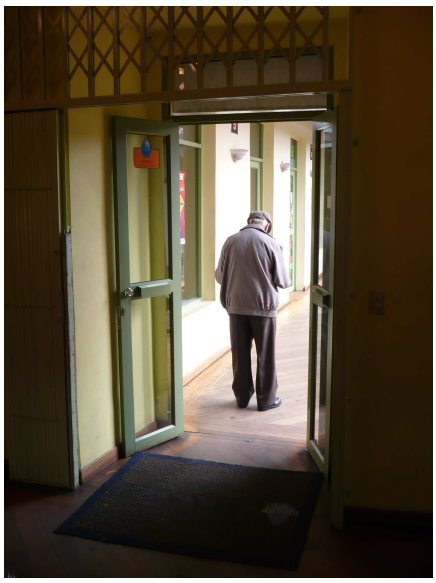


Figura 2.18 *Ingreso Agencia La Manzana. (Vista interior)*

- Consta de cuatro cámaras que conforman el sistema de Circuito Cerrado de Televisión local.

- Esta Agencia de Recaudación en especial posee un flujo de recaudación muy alto, superado únicamente por la Matriz de la empresa. Debido a esto, la misma trabaja continuamente desde las 8 hasta las 18 horas.

- Pese al grado de importancia comentado en el punto anterior, hay que destacar que las ventanillas de atención al cliente y la puerta de acceso a las cajas de recaudación no poseen protección ni blindaje alguno. (Figura 2.19)

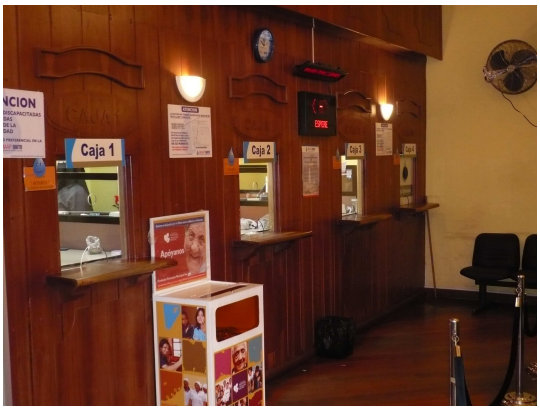


Figura 2.19 *Ventanillas de Atención al Cliente.*

- Las ventanas que rodean la instalación poseen rejillas de seguridad, tanto las que son accesibles al público en general así como aquellas que se resaltan por encontrarse en el segundo piso. (Figura 2.20)

Figura 2.20 *Rejillas de seguridad interna*

2.2.7 AGENCIA DE RECAUDACIÓN CARAPUNGO

La Agencia Carapungo está ubicada en el Pasaje No. 7 y Av. Luis Bacardi a las afueras de la ciudad, en la entrada del sector que lleva su nombre. (Figura 2.21)

Figura 2.21 *Ingreso Agencia de Recaudación Carapungo*

2.2.7.1 Características de Seguridad Física

- Como se observa en la Figura 2.22, la puerta principal de la agencia está protegida por un acceso metalico tipo lanfor.

Figura 2.22 *Ingreso Agencia Carapungo. (Vista interior)*

- Posee Circuito Cerrado de Televisión conformado por cuatro cámaras de seguridad.

- Dos guardias de seguridad brindan vigilancia en la instalación de 8 de la mañana a 4 de la tarde.

- Posee ventanillas y puerta de acceso a las cajas con blindaje. (Figura 2.23)

Figura 2.23 *Blindaje de puerta para acceso a cajas*

- Las ventanas de acceso a la dependencia están protegidas por rejas metálicas y accesos tipo lanfor (Figura 2.24)

Figura 2.24 *Agencia Carapungo*

2.2.8 AGENCIA DE RECAUDACIÓN QUITUMBE

La Agencia Quitumbe se encuentra ubicada en la Av. Quitumbe y Cóndor dentro de las instalaciones de la Administración Zonal Sur Quitumbe del Municipio, Sector Morán Valverde. Como parte activa del municipio, la EMAAP-Q recibió un lugar en el Balcón de Servicios para recaudar el dinero proveniente de los consumidores de agua de la zona.

Cabe mencionarse que a la fecha sobre la cual se trabajó en el análisis de seguridad, la agencia fue reubicada al balcón de servicios, por tal motivo, los

inmuebles que la conforman aún no se encuentran colocados en su interior en su totalidad.

Figura 2.25 *Agencia Quitumbe*

La dependencia posee un solo cubículo, mismo que realiza las actividades de recaudación y facturación.

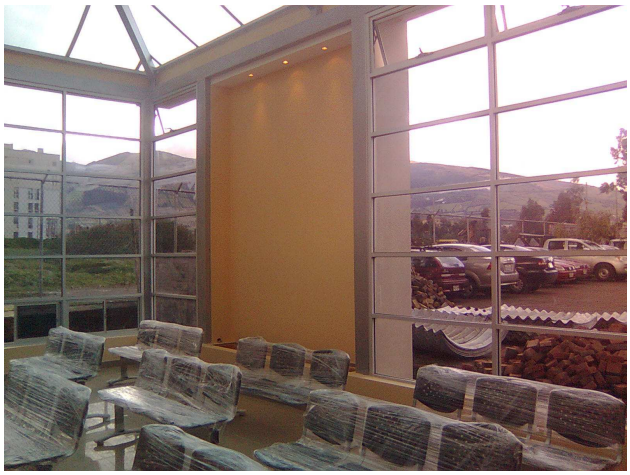


Figura 2.26 *Agencia Quitumbe*

2.2.8.1 Características de Seguridad Física

- El acceso al Balcón de Servicios está conformado por tres puertas de acceso, y el ingreso del personal de la EMAAP-Q a su cubículo está conformado por dos puertas consecutivas, estando la primera

constituida por un control de accesos con tarjetas magnéticas RFID. (Figura 2.27)

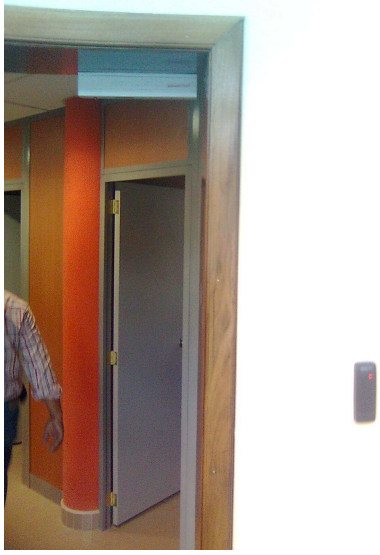


Figura 2.26 *Ingreso por tarjetas de acceso RFID*

- Las ventanillas y la puerta de acceso a las cajas no son blindadas.

- El Balcón de Servicios posee un sistema de Circuito Cerrado de Televisión conformada por 8 cámaras de seguridad.

- Tiene guardianía de 8 a 16 horas, la misma consta de un solo guardia armado contratado por la EMAAP-Q.

- Posee guardianía extra que brinda protección a toda la Administración Zonal.

2.2.9 AGENCIA DE RECAUDACIÓN AEROPUERTO

La Agencia de Recaudación Aeropuerto se encuentra ubicada en las calles Homero Salas y Av. La Prensa, en el interior del centro comercial que lleva su nombre. (Figura 2.28)

Figura 2.28 *Ingreso Agencia Aeropuerto*

La agencia Aeropuerto consta de cuatro cajas, solamente tres de ellas se encuentran en funcionamiento. Dos son de recaudación y una de facturación.

Figura 2.29 *Interior Agencia Aeropuerto*

2.2.9.1 Características de Seguridad Física

- Para el ingreso a la Agencia de Recaudación se tiene que atravesar una puerta de vidrio. Posee ventanales en los cuales no se tiene ninguna protección anti vandalismo.

- Tiene Circuito Cerrado de Televisión conformado por dos cámaras de seguridad. (Figura 2.30)

Figura 2.30 *CCTV Agencia Aeropuerto*

- La puerta de entrada a las ventanillas de atención al cliente es blindada.

- Las cuatro ventanillas de atención al cliente son blindadas.

- Posee dos guardias de seguridad que brindan vigilancia en la instalación de 8 de la mañana a 4 de la tarde.

2.2.10 AGENCIA DE RECAUDACIÓN PARQUE INGLÉS

La Agencia Parque Inglés se encuentra ubicada en la calle Antonio Villavicencio, Sector San Carlos al nor-occidente de la ciudad de Quito.

2.2.10.1 Características de Seguridad Física

- Esta agencia, como se observa en la Figuras 2.31 y 2.32, tiene una puerta de vidrio y ventanales de un considerable tamaño, los cuales, no poseen rejas ni ningún otro tipo de protección para evitar un ingreso no deseado a la dependencia.

Figura 2.31 *Ingreso Agencia Parque Inglés*

Figura 2.32 *Ventanales Agencia Parque Inglés*

- Posee Circuito Cerrado de Televisión conformado por cuatro cámaras de seguridad.

- La puerta de entrada a las ventanillas de atención al cliente es blindada.

- Las ventanillas de atención al cliente son blindadas.

- Posee dos guardias de seguridad que brindan vigilancia en la instalación de 8 de la mañana a 4 de la tarde.

2.2.11 AGENCIA DE RECAUDACIÓN IPIALES DEL SUR

Esta agencia de recaudación se encuentra ubicada en la Av. Morán Valverde, dentro del centro comercial que lleva su nombre, al sur de la ciudad de Quito. (Figura 2.33)

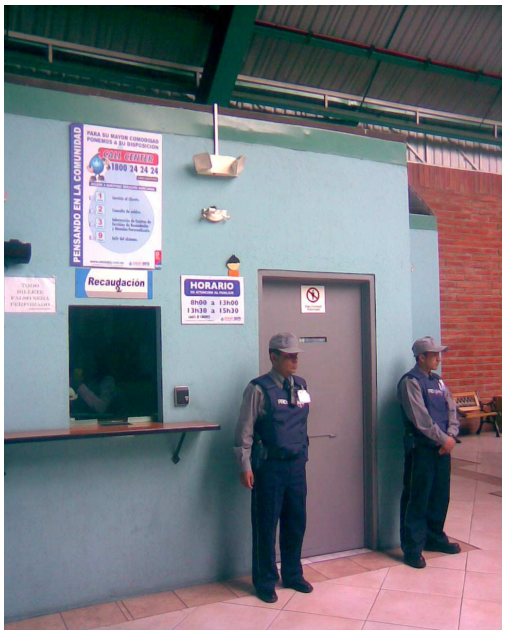


Figura 2.33 *Agencia Ipiales del Sur*

2.2.11.1 Características de Seguridad Física

- Posee sistema de Circuito Cerrado de Televisión conformado por cuatro cámaras de seguridad.

Figura 2.34 *Agencia Ipiales del Sur*

- La puerta de entrada a las ventanillas de atención al cliente es blindada.

- Las ventanillas de atención al cliente son blindadas.

- Posee dos guardias de seguridad que brindan vigilancia en la instalación de 8 de la mañana a 4 de la tarde.

Posee varios beneficios a más de sus protecciones propias, ya que la misma al encontrarse dentro del centro comercial está resguardada por guardianía privada extra a la contratada por la EMAAP-Q, y además, consta de un sistema de CCTV propio del centro comercial como se muestra en la Figura 2.34.

2.2.12 AGENCIA DE RECAUDACIÓN CHIRIYACU

Esta agencia se encuentra ubicada en Av. Gualberto Pérez, en el centro comercial del Antiguo Camal Metropolitano al sur de la ciudad de Quito.

2.2.12.1 Características de Seguridad Física

- La entrada a la Agencia de Recaudación está conformada por dos accesos metálicos tipo lanfor como se indica en la Figura 2.35.

Figura 2.35 *Acceso a la Agencia de recaudación. (Vista interior)*

- Posee Circuito Cerrado de Televisión conformado por cuatro cámaras de seguridad.

- La puerta de entrada a los cubículos de trabajo posee blindaje anti vandalismo.

- Las ventanillas de atención al cliente son blindadas. (Figura 2.36)

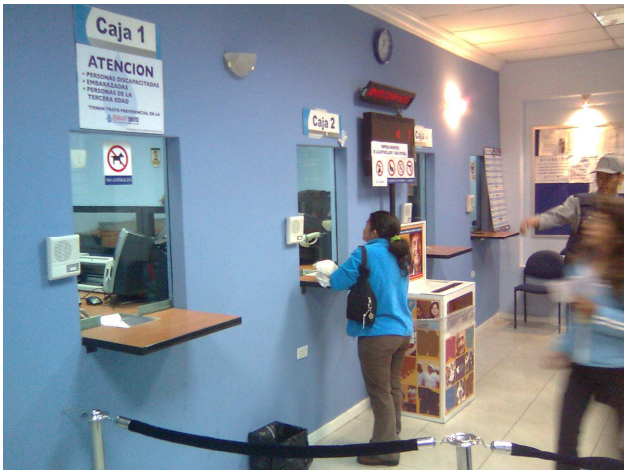


Figura 2.36 *Interior de la Agencia de Recaudación Chiriyacu.*

- Posee dos guardias de seguridad que brindan vigilancia en la instalación de 8 de la mañana a 4 de la tarde.

2.2.13 AGENCIA DE RECAUDACIÓN CAMAL METROPOLITANO

La Agencia de recaudación el Camal Metropolitano está ubicada al sur de la ciudad, dentro de las instalaciones municipales del camal. Consta de cuatro cubículos de los cuales solo uno brinda el servicio de recaudación y facturación.

Figura 2.37 *Exterior de la Agencia de Recaudación Camal Metropolitano.*

2.2.13.1 Características de Seguridad Física

- La entrada principal tiene protección de reja metálica, así como las ventanas que lo rodean. (Figura 2.38)

Figura 2.38 *Ingreso a la Agencia de Recaudación Camal Metropolitano.*

- Posee blindaje en las ventanillas y en la puerta de acceso a las cajas de recaudación. (Figuras 2.39 y 2.40)

Figura 2.39 *Ventanillas de la Agencia de Recaudación Camal Metropolitano.*

- La agencia trabaja en un horario de 8 a 4 de la tarde bajo la vigilancia de un solo guardia.

- Posee circuito cerrado de television con dos cámaras de seguridad.

Figura 2.40 *Puerta blindada para ingreso a cajas.*

2.2.14 AGENCIA DE RECAUDACIÓN SAN JOSÉ NOROCCIDENTE

La Agencia San José Noroccidente está ubicada en el segundo piso de una edificación que se encuentra aproximadamente a 200 metros de la Ave. Mariscal Sucre y Legarda en la Ciudad de Quito.

Figura 2.41 *Agencia de Recaudación San José Noroccidente*

2.2.14.1 Características de Seguridad Física

- No posee el sistema de circuito cerrado de televisión.

- Tiene guardianía de 8 a 16 horas, que consta de un solo guardia armado perteneciente a la empresa Guarpri.

- Los cubículos y la puerta de acceso principal a esta agencia son blindadas. (Figura 2.42)

Figura 2.42 *Interior de la Agencia de Recaudación San José Noroccidente*

- La ventana de esta agencia posee rejas metálicas de protección. (Figura 2.43)

Figura 2.43 *Ventana de la Agencia de Recaudación San José Noroccidente*

2.2.15 AGENCIA DE RECAUDACIÓN CHIMBACALLE

La Agencia Los Andes Chimbacalle se encuentra ubicada dentro del Mercado que lleva su nombre en la parte sur de la ciudad de Quito. Esta cuenta con cinco cubículos, de los cuales dos son de recaudación uno de facturación y los otros dos de atención al público, cabe mencionar que actualmente a los cubículos de atención al público no se los está dando uso alguno.

Figura 2.44 *Agencia de Recaudación Chimbacalle*

De los tres cubículos que brindan servicio de recaudación y facturación, solamente uno se encuentra trabajando, esto, debido a que el flujo de personas para disponer de este servicio es bajo.

Figura 2.45 *Agencia de Recaudación Chimbacalle*

2.2.15.1 Características de Seguridad Física

- No posee el sistema de circuito cerrado de televisión.

- Tiene guardianía de 8 a 16 horas, esta consta de un solo guardia armado. (Figura 2.45)

- Las ventanillas de los cubículos y la puerta de acceso a las cajas de esta agencia son blindadas. (Figura 2.46)

Figura 2.46 *Acceso blindado a cajas*

- La entrada única a esta dependencia se encuentra protegida por una puerta metálica tipo reja. (Figura 2.47)

Figura 2.47 *Acceso Principal a la Agencia*

2.3VULNERABILIDAD DE LAS AGENCIAS DE RECAUDACIÓN

El reconocimiento físico realizado sirvió para notar las fortalezas y debilidades de las 15 instalaciones dedicadas a recaudación de la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito, valiendo denotar sus falencias, ya que será sobre éstas que se deberá trabajar en el análisis necesario para determinación de los correctos dispositivos de vigilancia y monitoreo.

Las situaciones que se debe considerar para los grados de vulnerabilidad que poseen las agencias son la afluencia de gente que las visitan y la cantidad de dinero que se maneja en el horario de trabajo. Además de otras características físicas que se deben tomar en cuenta y así hacer la selección y posicionamiento de los dispositivos que constarán en el sistema de seguridad electrónica de alarmas.

Debido a que las agencias de recaudación no poseen el servicio de guardianía de seguridad privada las 24 horas del día los bienes de la empresa no están protegidos de ninguna forma aparte de puertas y ventanas como es normal; por esta razón el sistema de alarmas monitoreadas sería de gran utilidad para tener una protección continua durante las 24 horas.

Así también se debe tomar en cuenta las falencias físicas de las agencias como por ejemplo, la agencia de recaudación “La Manzana” es una de las mayores recaudadoras de dinero y la misma no posee puerta de ingreso a cajas blindadas y ventanillas de atención al cliente blindadas, dando así cierta inseguridad a los empleados de la agencia. Las agencias de recaudación “Aeropuerto” y Parque Inglés” por otro lado están propensas a mayores intentos vandálicos ya que las mismas cuentan con ventanales que pueden ser víctimas de algún incidente, además de que son más fáciles de romper en un intento de robo.

Aparte de estas falencias físicas han existido situaciones en las que el personal que trabaja para la empresa se ha contaminado con sustancias

tóxicas en el momento de recibir el dinero; en estas situaciones el personal no tiene la capacidad de reaccionar de alguna manera para evitar el robo o el atraco, mientras que con el sistema de alarmas monitoreadas se puede activar una alarma de pánico y otra de emergencia médica para que el personal pertinente acuda al sitio.

Otro de los puntos importantes a tomarse en cuenta con respecto a la vulnerabilidad de las agencias es el flujo de dinero que manejan, por esta razón en el cuadro siguiente se muestra la cantidad de dinero que circula por las agencias en el mes de Julio del 2008.

El cuadro indica que las Agencias con mayor flujo de dinero, y a la vez, baja seguridad son La Manzana, Mayorista, Atahualpa e Ipiales del Sur, por lo que necesitan protección que evite el robo o atraco.

EMPRESA METROPOLITANA DE ALCANTARILLADO Y AGUA POTABLE DE QUITO
UNIDAD DE RECAUDACION

AÑO	MES	AGENCIA	FACTURAS	USD	PROMEDIO FACT	PROMEDIO USD
2008	Julio	Manzana	27.066	628.517,06	873	20.274,74
		12 de Octubre	8.941	264.671,50	288	8.537,79
		Matriz	47.320	1.895.311,91	1.526	61.139,09
		Aereopuerto	10.562	315.948,40	341	10.191,88
		Chiriyacu	25.106	560.188,40	810	18.070,59
		Mayorista	17.304	352.887,83	558	11.383,48
		Iñaquito	7.658	324.879,44	247	10.479,98
		Tumbaco	9.228	212.864,28	298	6.866,59
		La Luz	11.299	367.763,88	364	11.863,35
		Los Chillos	8.916	181.612,01	288	5.858,45
		Carapungo	10.165	187.191,44	328	6.038,43
		Atahualpa	13.672	323.624,96	441	10.439,51
		Quitumbe	1.001	16.019,47	32	516,76
		Parque Ingles	6.206	127.684,60	200	4.118,86
		Ipiales Sur	12.298	196.513,83	397	6.339,16
		Condado	17.300	431.254,15	558	13.911,42
				6.386.933,16		

2.4 ANÁLISIS BÁSICO Y UBICACIÓN DE EQUIPOS

Como continuación al análisis físico realizado en las dependencias, se debe plantear las soluciones factibles de ser implementadas para fortalecer sus sistemas de seguridad, resumiendo sus inconvenientes y planteando soluciones a las mismas.

Cada Agencia de Recaudación presentó características especiales, así como características generales que pueden aportar al análisis y diseño del Sistema de Seguridad Electrónica con Alarmas Monitoreadas.

2.4.1 Características generales encontradas

A pesar que cada una de las doce dependencias posee características propias de su estructura física, variando principalmente su locación, ya sea dentro de un centro comercial, dentro de una administración zonal, o accesible al público en general a las afueras de una edificación, mantienen ciertas cualidades comunes, como lo son sus cajas de atención al público, ingreso al área resguardada de trabajadores EMAAP-Q (bunker) y la utilización de fuentes de energía abastecidas por UPS.

Partiendo del hecho que se debe resguardar un lugar plenamente comercial, y que se debe colocar dispositivos de alerta, se ha considerado que todas las instalaciones a trabajarse en el proyecto deban tener:

a) Botones de pánico en cada una de las cajas para alertar asaltos,

b) Sensores de movimiento para alertar un ingreso no deseado a la dependencia,

c) Magnéticos adhesivos para monitorear las puertas de ingreso a las áreas de atención al público y bunker,

d) Botones de pánico inalámbricos, mismos que poseerán los guardias de seguridad el momento de efectuar sus turnos de monitoreo en las agencias de recaudación,

e) Sirenas para alertar una emergencia,

f) Supresores de Transientes de 110 V para eliminar picos de voltajes no deseados, con el fin de que los equipos estén protegidos,

g) Teclado en español para facilidad el manejo por parte del usuario,

h) Un panel de control destinado al servicio comercial, que cumpla normativas UL para ser integrador, dedicado a sistemas de intrusión y que sea capaz de acoplar todos los dispositivos a detallarse,

i) Baterías de respaldo de 7amp/h para los paneles de control, y

j) Una interfaz capaz de acoplarse al panel de control para transmisión de los datos remotos.

Cabe mencionarse que a más de estos dispositivos comunes, las agencias tendrán otro tipo de dispositivos especiales, pero cada uno de estos se resaltará independientemente según la agencia a tratarse.

Ya que todas las dependencias tendrán paneles de control, los mismos serán colocados en un lugar estratégico, como lo es el área resguardada bunker, puesto que el ingreso al mismo se encuentra protegido con una puerta blindada y ventanillas de atención al cliente a pruebas de bala, dando así, una seguridad a la central de alarma de no ser alterada o manipulada por gente no autorizada. Las únicas excepciones de este tipo serán las agencias La

Manzana, Iñaquito y Quitumbe, ya que las mismas no poseen blindaje en puertas de ingreso o ventanillas; estos casos serán tratados individualmente.

Los teclados para activación o desactivación de zonas o sistema total, serán colocados dentro del cuarto de las ventanillas de atención al cliente; esto, debido a que sólo la persona encargada de la seguridad de esta dependencia tendrá la capacidad y responsabilidad de manipular el dispositivo.

Los botones de pánico inalámbricos serán otorgados a cada uno de los guardias de seguridad privada, teniendo como deber utilizar el mismo en caso de que se produzca algún evento inesperado.

Por último, para proteger a los equipos que se van a utilizar en estas agencias, es conveniente utilizar un Supresor de Transientes para que la energía usada sea adecuada y no se tenga problemas con los sobre voltajes transitorios para que los equipos trabajen en óptimas condiciones y no haya pérdidas de datos en el sistema.

2.4.2 Características específicas encontradas

Aquí se toma en cuenta el factor de locación y estructura interna de la dependencia, para lograr determinar el tipo de dispositivo electrónico que sea capaz de monitorear una variable que pueda alertar cualquier tipo de emergencia surgida en la instalación.

Todas las agencias visitadas necesitan los siguientes dispositivos para el funcionamiento del sistema de alarmas monitoreadas:

- Un panel de control que será colocado en un lugar estratégico, como lo es el área resguardada bunker.

- Un transmisor de información, el cual desempeñará la misión de transmitir los datos del panel de control a la central de monitoreo en la

matriz de la EMAAP-Q, se deberá colocar junto al panel de control para evitar inconvenientes.

- La sirena, medio auditivo de alarma, estará ubicada en la parte externa de la dependencia con su respectivo gabinete de protección, y además, deberá contar con la respectiva seguridad de tamper y conexiones seguras a prueba de sabotajes.

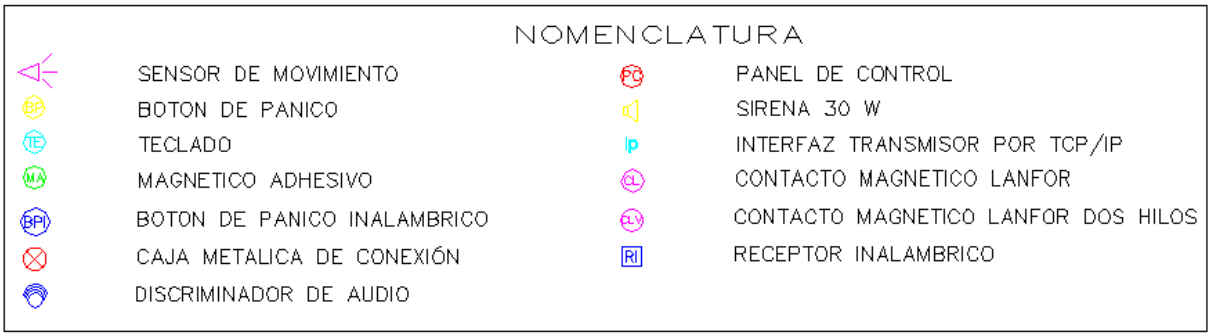
- Un contacto magnético para puertas metálicas tipo lanfor colocado en la puerta del acceso principal a la dependencia, el cual cumple con todas las especificaciones y normativas de seguridad eléctrica que le corresponden.

- Un sensor de movimiento que se colocará con una doble funcionalidad: la de sensar el espacio físico de atención al público y la de ser un control redundante de la agencia en caso de que el sensor colocado en la puerta de ingreso falle o sea saboteado.

- Un contacto magnético adhesivo en la puerta para tener el conocimiento de las veces que se abre la puerta blindada en el bunker.

- Los cables de alimentación para los diferentes dispositivos como son sensores de movimiento, botones de pánico, teclados, etc. serán cable UTP categoría 5e e irán por canaletas plásticas dentro del bunker y por tubería metálica fuera del mismo como se muestra en los planos.

La nomenclatura usada para la ubicación de los elementos es la siguiente:



2.4.2.1 Agencia de Recaudación 12 de Octubre

Realizando un análisis del espacio físico que le corresponde a esta agencia, que es de 47,95m^2, y de la disposición de la misma, se procedió a distribuir los dispositivos electrónicos que se consideran necesarios para esta dependencia.

Estos dispositivos han sido diseñados para ser colocados estratégicamente, con el único fin de que brinden un monitoreo eficaz de la dependencia, y además, que sean capaces de cumplir normas internacionales en cuanto a instalación y desempeño.

En esta dependencia se colocarán los siguientes dispositivos; según lo indica la Figura 2.48.

- 1 Panel de Control

- 1 Transmisor IP

- 1 Teclado

- 1 Sirena (con su respectivo gabinete)
- 1 Contacto Lanfor

- 1 Contacto Magnético Adhesivo

- 3 Botones de Pánico tipo palanca

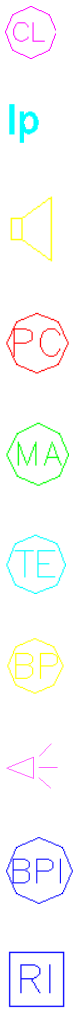
- 1 Sensor PIR (de movimiento)
- 1 Botón de Pánico Inalámbrico

- 1 Receptor Inalámbrico

2.4.2.2 Agencia de Recaudación Atahualpa

El área de esta agencia es de 94.05m^2, y de los dispositivos a colocarse serán; según lo indica la Figura 2.49.

- 1 Contacto Magnético Lanfor
- 1 Transmisor TCP/IP
- 1 Sirena 30w
- 1 Panel de Control
- 1 Contacto Magnético Adhesivo
- 1 Teclado
- 3 Botones de Pánico
- 1 Sensor PIR (de movimiento)
- 1 Botón de Pánico inalámbrico
- 1 Receptor inalámbrico



Sobre la Agencia Atahualpa se ha planificado colocar solamente un contacto magnético adhesivo, el mismo que se instalará en la puerta de ingreso al área protegida bunker. La idea es mantener un control eficaz de las acciones que se realizan dentro de la agencia, además de saber el momento que se suscite algún incidente vandálico o se irrumpa el área protegida.

2.4.2.3 Agencia de Recaudación Iñaquito

Luego del reconocimiento visual que se realizó en esta agencia de recaudación, podemos decir que el espacio físico es pequeño: 11,12m^2 y, debido a esta disposición, en esta agencia se colocarán los siguientes dispositivos; según lo indica la figura 2.50.

- 1 Panel de Control
- 1 Transmisor TCP/ IP
- 1 Teclado
- 1 Sirena
- 1 Contacto Magnético Adhesivo
- 3 Botones de Pánico
- 1 Sensor PIR (de movimiento)
- 1 Botón de Pánico Inalámbrico
- 1 Receptor Inalámbrico
- 1 Discriminador de Audio

En esta dependencia se colocará un discriminador de audio debido a que en la parte trasera de la dependencia existe un ventanal que puede ser destrozado en un intento de robo o acto vandálico. Su fin será alertar a la central de monitoreo alguna emergencia que pondría en riesgo a los empleados y a los bienes materiales de la EMAAP-Q, por tal motivo este discriminador de audio enviará una señal en el momento en que esto suceda.

Se colocará un sensor de movimiento en el interior del cubículo de atención al cliente, debido a que su exterior es monitoreado permanentemente las 24 horas por guardianía de la Administración Zonal.

2.4.2.4 Agencia de Recaudación La Luz

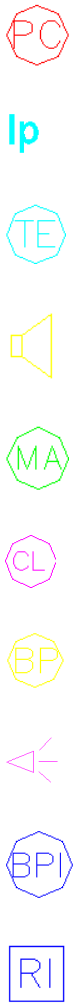
El área de la agencia es de 86,9m^2, y en esta agencia se colocarán los siguientes dispositivos; según lo indica la Figura 2.51.

- 1 Panel de Control
- 1 Transmisor TCP/ IP
- 1 Teclado
- 1 Sirena
- 1 Contacto Magnético Adhesivo
- 3 Botones de Pánico
- 1 Sensor PIR (de movimiento)
- 1 Botón de Pánico Inalámbrico
- 1 Receptor Inalámbrico

2.4.2.5 Agencia de Recaudación Mayorista

El espacio físico que le corresponde a esta agencia es de 58,24m^2, y en esta agencia se colocarán los siguientes dispositivos; según lo indica la Figura 2.52.

- 1 Panel de Control
- 1 Transmisor TCP/ IP
- 1 Teclado
- 1 Sirena
- 1 Contacto Magnético Adhesivo
- 1 Contacto Magnético Lanfor
- 3 Botones de Pánico
- 1 Sensor PIR (de movimiento)
- 1 Botón de Pánico Inalámbrico
- 1 Receptor Inalámbrico



2.4.2.6 Agencia de Recaudación La Manzana

El área de esta agencia es de 103,36m^2, y de los dispositivos a colocarse serán; según lo indica la Figura 2.53.

- 1 Panel de Control
- 1 Transmisor TCP/ IP
- 1 Teclado
- 1 Sirena
- 2 Contacto Magnético Adhesivo
- 5 Botones de Pánico
- 1 Sensor PIR (de movimiento)
- 1 Botón de Pánico Inalámbrico
- 1 Receptor Inalámbrico
- 1 Discriminador de Audio

En esta dependencia se recomienda la instalación de un discriminador de audio, debido a que en la parte frontal de la misma (ingreso), existen ventanas que pueden ser trisadas en un intento de robo, poniendo en riesgo los bienes materiales de la empresa. En este caso se sugiere la colocación de dos contactos magnéticos adhesivos, los cuales se encuentran: uno en la puerta de ingreso a la agencia, y el otro, en la puerta de ingreso a las ventanillas, así, se lograra mantener un control eficaz sobre las acciones que se realizan dentro de la dependencia.

El diseño de las instalaciones eléctricas de los equipos que se usarán en esta agencia consta de cableado a través de tubería metálica debido a que esta agencia no posee en el bunker ni puerta ni ventanillas blindadas.

2.4.2.7 Agencia de Recaudación Carapungo

El área de esta agencia es de 59,39m^2, y los dispositivos a colocarse serán; según lo indicado en la Figura 2.54.

- 1 Panel de Control
- 1 Transmisor TCP/ IP
- 1 Teclado
- 1 Sirena
- 1 Contacto Magnético Adhesivo
- 1 Contacto Magnético Lanfor
- 3 Botones de Pánico
- 1 Sensor PIR (de movimiento)
- 1 Botón de Pánico Inalámbrico
- 1 Receptor Inalámbrico

2.4.2.8 Agencia de Recaudación Quitumbe

Debido a que esta agencia de recaudación fue recientemente reubicada, no se posee planos oficiales de las instalaciones; es así, que dadas las circunstancias, se hizo la visita a la agencia para determinar visualmente la ubicación de los diferentes dispositivos electrónicos en la misma.

Para esta agencia de recaudación se recomienda la utilización de los siguientes dispositivos; según lo indica la Figura 2.55.

- 1 Panel de Control
- 1 Transmisor TCP/ IP
- 1 Teclado
- 1 Sirena
- 2 Contacto Magnético Adhesivo
- 2 Botones de Pánico
- 1 Sensor PIR (de movimiento)
- 1 Botón de Pánico Inalámbrico
- 1 Receptor Inalámbrico

La distribución de los mismos deberá cubrir todos sus puntos considerados críticos al responder o mantener una emergencia.

Debido a que el área interna de ventanillas no posee blindaje, pero si posee sistema de control de accesos, se planificó instalar el panel de control dentro de la misma.

2.4.2.9 Agencia de Recaudación Aeropuerto

El espacio físico de esta agencia es de 62,83m^2, y tomando en cuenta que está dentro del centro comercial se colocarán los siguientes dispositivos; según lo indicado en la Figura 2.56.

- 1 Panel de Control
- 1 Transmisor TCP/ IP
- 1 Teclado
- 1 Sirena
- 3 Contacto Magnético Adhesivo
- 3 Botones de Pánico
- 1 Sensor PIR (de movimiento)
- 1 Botón de Pánico Inalámbrico
- 1 Receptor Inalámbrico
- 1 Discriminador de Audio

Para Agencia Aeropuerto se ha planificado colocar tres contactos magnéticos adhesivos, dos de los cuales se colocaran en la puerta de ingreso a la agencia y el otro en la puerta de ingreso al bunker, para tener así, el conocimiento de las veces que se abren las mismas. La idea es mantener un control eficaz de las acciones que se realizan dentro de la agencia, además de que en algún incidente vandálico se conozca el momento en el que se está irrumpa el área blindada. En esta dependencia se colocará un discriminador de audio debido a que en la parte de la entrada de la dependencia existe un ventanal muy grande que puede ser destrozado en un intento de robo, hecho que, pondría en riesgo los bienes materiales de la empresa.

2.4.2.10 Agencia de Recaudación Parque Inglés

Realizando un análisis del espacio físico que le corresponde a esta agencia, que es de 86,4m^2, y de la disposición de la misma se colocarán los siguientes dispositivos; según lo indica la Figura 2.57.

- 1 Panel de Control
- 1 Transmisor TCP/ IP
- 1 Teclado
- 1 Sirena
- 3 Contacto Magnético Adhesivo
- 3 Botones de Pánico
- 1 Sensor PIR (de movimiento)
- 1 Botón de Pánico Inalámbrico
- 1 Receptor Inalámbrico
- 1 Discriminador de audio

Esta agencia se encuentra ubicada dentro del centro comercial Parque Inglés en el Patio de Comidas localizado en el Sector Parque Inglés, se recomienda ubicar la sirena en la parte externa de la agencia con su respectivo gabinete de protección y que cuente con la respectiva seguridad de tamper y conexiones seguras a prueba de sabotajes. Debido a que en la entrada a la agencia existen algunos ventanales se ha visto la necesidad de colocar un discriminador de audio, puesto que los mismos pueden ser destrozados en un intento de robo, poniendo en riesgo los bienes materiales de la empresa.

En este caso se han colocado tres contactos magnéticos adhesivos, dos de los cuales están en la puerta de ingreso a la dependencia y el otro en la puerta de ingreso al bunker, todo esto con el fin de obtener la información de cuantas veces se abre la misma, y a la vez, tener el conocimiento de un acto emergente tratar de irrumpir en el bunker.

2.4.2.11 Agencia de Recaudación Ipiales del Sur

El área de esta agencia es de 69,59m^2, y en la misma se colocarán los siguientes dispositivos; según lo indicado en la Figura 2.58.

- 1 Panel de Control
- 1 Transmisor TCP/ IP
- 1 Teclado
- 1 Sirena
- 1 Contacto Magnético Adhesivo
- 3 Botones de Pánico
- 1 Sensor PIR (de movimiento)
- 1 Botón de Pánico Inalámbrico
- 1 Receptor Inalámbrico

Ipiales del Sur poseerá al igual que la Agencia Iñaquito un sensor de movimiento en el interior de la zona de trabajadores EMAAP-Q, esto debido a que el área exterior mantiene continúo flujo de personas debido a ser un centro comercial.

2.4.2.12 Agencia de recaudación Chiriyacu

El área que le corresponde a esta agencia es de 78,75m^2, y se procederá a la colocación de los siguientes dispositivos; según lo indica la Figura 2.59.

- 1 Panel de Control
- 1 Transmisor TCP/ IP
- 1 Teclado
- 1 Sirena
- 1 Contacto Magnético Adhesivo
- 2 Contacto Magnético Lanfor
- 4 Botones de Pánico
- 1 Sensor PIR tecnología
- 1 Botón de Pánico Inalámbrico
- 1 Receptor Inalámbrico
- 2 Discriminadores de Audio

Debido a que en esta agencia se tienen dos ingreso y cada uno cuenta con su respectiva puerta metálica tipo lanfor, se colocarán contactos magnéticos comerciales para tener el monitoreo de las entradas en caso de que algún incidente vandálico se presente en la dependencia.

Ya que en la parte posterior de la agencia existen varias ventanas, se ha visto la necesidad de usar dos discriminadores de audio, ya que estas ventanas

pueden ser destrozadas en un intento de robo, o amenazadas en alguna emergencia que pondría en riesgo a los empleados y a los bienes materiales de la empresa.

2.4.2.13 Agencia de recaudación Camal Metropolitano

El área que comprende esta agencia es de 77,46m^2, y se procederá a la colocación de los siguientes dispositivos; según lo indica la Figura 2.60.

- 1 Panel de Control
- 1 Transmisor TCP/ IP
- 1 Teclado
- 1 Sirena
- 2 Contacto Magnético Adhesivo
- 2 Botones de Pánico
- 1 Sensor PIR tecnología
- 1 Discriminador de Audio
- 1 Botón de Pánico Inalámbrico
- 1 Receptor Inalámbrico

Como se puede observar en el plano no se ha colocado botones de pánico en las ventanillas de atención, que se encuentran en los extremos, debido a que las mismas se encuentran inhabilitadas, y se conoce que nunca van a ser abiertas.

2.4.2.14 Agencia de recaudación San José Noroccidente

El área que le corresponde a esta agencia es de 44,93m^2, y se procederá a la colocación de los siguientes dispositivos; según lo indicado en la Figura 2.61.

- 1 Panel de Control
- 1 Transmisor TCP/ IP
- 1 Teclado
- 1 Sirena
- 2 Contacto Magnético Adhesivo
- 3 Botones de Pánico
- 1 Sensor PIR tecnología
- 1 Botón de Pánico Inalámbrico
- 1 Receptor Inalámbrico

2.4.2.15 Agencia de Recaudación Chimbacalle

El área que le corresponde a esta agencia es de 101m^2, y se procederá a la colocación de los siguientes dispositivos; según lo indicado en la Figura 2.62.

- 1 Panel de Control
- 1 Transmisor TCP/ IP
- 1 Teclado
- 1 Sirena
- 2 Contactos Magnéticos Adhesivos
- 2 Botones de Pánico
- 1 Sensor PIR tecnología
- 1 Botón de Pánico Inalámbrico
- 1 Receptor Inalámbrico

2.5 DISEÑO DE INSTALACIONES ELÉCTRICAS PARA EL SISTEMA DE SEGURIDAD ELECTRÓNICA.

Debido a que todas las dependencias que se han tratado antes ya tienen una instalación eléctrica general (iluminación y tomas corrientes) instalada, lo que se pretende es analizar el tipo de cableado y de conexiones que se necesitan para la instalación de los diferentes dispositivos electrónicos que se van a utilizar en las agencias de recaudación.

Lo que se necesita es un toma corriente para obtener la energía eléctrica entregada por la Empresa Eléctrica Quito S.A. En este toma corriente se conectará un UPS que a su vez se conectará a un transformador que entregue la energía necesaria al panel de control de las alarmas. Y como todos los dispositivos electrónicos que se quiere instalar en las agencias están conectados a este panel, reciben del mismo la energía necesaria para su funcionamiento.

El cable que se utilizará para estas conexiones será un cable UTP categoría 5e, el cual será trasladado por tubería metálica EMT en lugares vulnerables o de fácil acceso al público y canaletas plásticas donde el acceso se vuelve difícil o muy limitado.

Se utilizará canaletas plásticas y tubería corrugada plástica cuando se traslade el cable dentro de la habitación que corresponde a las cajas (bunker) ya que como la mayoría de las agencias tienen puerta y ventanillas blindadas, el acceso al cableado será mucho más complicado y difícil. Además de que se pretende que la tubería plástica corrugada no sea visible y que la misma sea instalada por encima del techo falso.

Todo empalme tubería EMT – tubería EMT, tubería EMT - canaleta, canaleta - manguera corrugada, deberá atravesar una caja metálica estándar de revisión, misma que servirá como una herramienta práctica a la realización de

mantenimientos y permitirá unificar los diferentes tipos de material utilizado para canalizar el cableado UTP.

Todo dispositivo utilizará su propio UTP, es decir, a pesar de poseer cuatro pares, si los mismos sobran, se mantendrán como un futuro respaldo a la transmisión de eventos.

Se deberá procurar canalizar toda tubería EMT al ras del piso, así como toda canaleta plástica lo mas cercana al cielo raso, y manguera corrugada plástica sobre el techo falso.

La alimentación de cada dispositivo será brindada por el propio panel de la instalación, misma que cumplirá el requerimiento de ser regulada y permanente por poseer energía de respaldo a través de baterías propias del sistema y alimentadores UPS.

Se verificó que los UPS se acoplen a toma corrientes que se encuentren alimentados con conductores número 12 AWG tipo TW, en caso de no encontrarse el mismo se procurará optimizar la toma de energía realizando un cableado nuevo desde la caja de breakers hasta un toma corrientes nuevo.

Debido a que en las quince agencias analizadas no se encontró ningún tipo de protección a tierra; se recomienda a la empresa EMAAP-Q la implementación de la misma.

2.6 FUNCIONAMIENTO GENERAL DEL SISTEMA DE SEGURIDAD MONITOREADA

Luego de que se ponga en marcha el sistema, el mecanismo del mismo trabaja de la siguiente manera: En el momento que ocurra un incidente, uno o varios de los sensores instalados será accionado por parte del personal que labora en la agencia. La señal que se produce se dirige de inmediato al panel

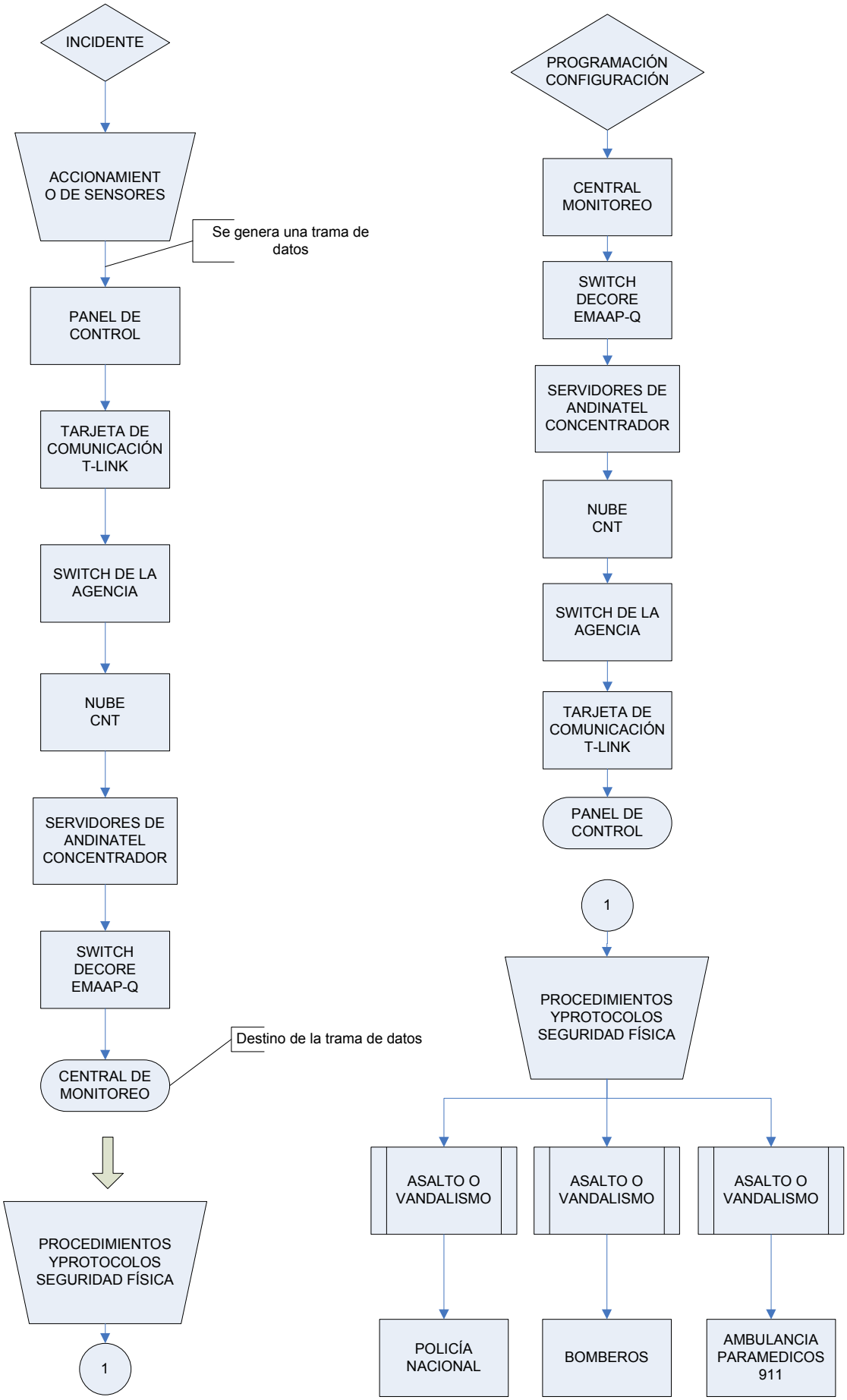
de control comunicándose a su vez con la tarjeta de comunicación en este caso la tarjeta llamada T-LINK.

La T-LINK codifica los datos recibidos y los envía al SWITCH (equipo perteneciente al Departamento de Recursos Informáticos de la EMAAP-Q). Este SWITCH se conecta a la red de la CNT introduciendo la información a una nube general donde llega toda la información, luego se dirige a los servidores de ANDINATEL que se conocen como “Concentrador”.

Del Concentrador de ANDINATEL la trama de datos se dirige a un SWITCH principal llamado DECORE en la EMAAP-Q, los datos ingresan a la red interna de la matriz de la empresa dirigiéndose estos datos al computador de la Central de Monitoreo que se encuentra en el Departamento de Seguridad Física y Radio Comunicaciones, mostrándose en el computador de la Central de Monitoreo que clase de alarma fue activada.

Toda la transmisión de datos se demora en ser receptada por la Central de Monitoreo en una fracción de segundo lo cual hace que los procedimientos y protocolos que se realizan por parte del Departamento de Seguridad Física sean efectivos. Estos procedimientos varían de acuerdo a la alarma que fue activada por ejemplo si se produce una emergencia médica lo que se hace es llamar al 911, paramédicos o una ambulancia; por otro lado si se presenta una emergencia de tipo vandálico o asalto se llama a la Policía Nacional; o si se da un incendio en las instalaciones o cercano se llama a los bomberos. Todos estos procedimientos vienen acompañados por protocolos propios del Departamento de Seguridad Física.

Aparte de todo esto se debe recalcar también que la comunicación que se tiene entre la matriz y las diferentes agencias es bidireccional, es decir que la de la Central de Monitoreo como el Panel de Control ubicado en las diferentes agencias pueden recibir o enviar información dependiendo de la necesidad. Ya que de ser el caso desde la matriz también se pueden enviar ciertos datos de programación o configuración a los distintos paneles de control.


INCIDENTE
ACCIONAMIENTO DE SENSORES
Se genera una trama de datos
PANEL DE CONTROL
TARJETA DE COMUNICACIÓN T-LINK
SWITCH DE LA AGENCIA
NUBE CNT
SERVIDORES DE ANDINATEL CONCENTRADOR
SWITCH DECORE EMAAP-Q
CENTRAL DE MONITOREO
Destino de la trama de datos
PROCEDIMIENTOS YPROTOCOLOS SEGURIDAD FÍSICA
1
PROGRAMACIÓN CONFIGURACIÓN
CENTRAL MONITOREO
SWITCH DECORE EMAAP-Q
SERVIDORES DE ANDINATEL CONCENTRADOR
NUBE CNT
SWITCH DE LA AGENCIA
TARJETA DE COMUNICACIÓN T-LINK
PANEL DE CONTROL
1
PROCEDIMIENTOS YPROTOCOLOS SEGURIDAD FÍSICA
ASALTO O VANDALISMO
ASALTO O VANDALISMO
ASALTO O VANDALISMO
POLICÍA NACIONAL
BOMBEROS
AMBULANCIA PARAMEDICOS 911

CAPÍTULO 3. DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA

3.1 CRITERIOS GENERALES

Como paso fundamental en el desarrollo de este proyecto, y teniendo en cuenta el análisis desarrollado en cada una de las dependencias, se ha considerado necesario definir ciertos criterios generales en cuanto a:

- Determinación de enlace para comunicación de los paneles de control a central de monitoreo y,

- Correcto procedimiento sobre instalación de equipos y uso de materiales.

3.1.1 DETERMINACIÓN DE ENLACE

El enlace entre Panel de Control – Central de Monitoreo debe ser un factor de suma importancia en el desarrollo de este tipo de proyectos, simplemente se puede resumir al mismo como la comunicación capaz de alertar una emergencia o una necesidad en tiempo real del sitio o lugar a establecer un control permanente de seguridad.

Comúnmente, en el monitoreo de alarmas, dicho enlace es establecido con la utilización de una línea telefónica o un enlace GPRS. Esto se determina según las características de la locación donde se pretenda implementar un sistema de seguridad electrónica monitoreado.

En el caso de las agencias de recaudación de la EMAAP-Q, y teniendo en cuenta que el principal fin de implementar este proyecto es ahorrar en gastos suprimiendo o reduciendo las horas laborables de los guardias de seguridad, se debía partir que el enlace a establecerse debía desempeñar a cabalidad

con su fin, y al mismo tiempo, economizar los gastos de la empresa inversionista.

Siendo así, surgió la idea de enlazar las dependencias a la Matriz de la Empresa de Agua Potable y Alcantarillado de Quito utilizando una comunicación ya pre establecida entre las mismas: enlace ADSL permanente de 64 Kbps.

3.1.1.2 Enlace ADSL

ADSL o Asymmetric Digital Subscriber Line (Línea de Suscripción Digital Asimétrica) se caracteriza por ser una tecnología capaz de transmitir datos digitales utilizando como vía la línea telefónica convencional.

La forma en que la misma se desempeña es modulando los datos a altas velocidades sobre el par trenzado de cobre, siempre y cuando el tendido del mismo no sobrepase los 5,5 km desde el abonado hasta la central telefónica. Esta modulación debe cumplir la función de utilizar una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales (300-3.800Hz) para no interferir en la misma.

Se caracteriza por ser asimétrica debido a que la velocidad de subida no es la misma que la de bajada, en otras palabras, puede alcanzar velocidades altas hacia el abonado pero velocidades bajas desde el abonado a la central.

Su funcionamiento se basa en colocación de dos módems, uno a la salida de la central telefónica y otro donde el usuario final. Esta conexión crea tres canales de información:

- Canal de Alta velocidad: Desde la red al usuario.
- Canal de Media velocidad: Canal Dúplex para transmisión de información en ambas direcciones.
- Canal telefónico convencional.

Debido a la creación de todos estos canales, es necesario implementar un dispositivo que pueda filtrar los mismos para evitar distorsiones entre los datos; este filtro es conocido comúnmente como *splitter.*

3.1.1.3 Enlace Agencias – Matriz

El enlace ADSL que poseen las Agencias con su Matriz se dedica neta y completamente a monitorear las transacciones efectuadas en cada una de estas dependencias, y es de aquí que surgió la idea de utilizarlo para transmitir paralelamente la información perteneciente a los paneles de control.

Ya planteada la idea, se debía dar inicio a un estudio para determinar la factibilidad de la misma, el cual debía responder si la transmisión efectuada por las agencias ocupaban en su totalidad los 64 Kbps, y en caso que la respuesta a esta pregunta sea NO, plantear dos inquietudes más: ¿cuál era la cantidad de banda que utilizan las agencias de recaudación?, y ¿cuál era la cantidad de banda que necesitaban los paneles de control para su transmisión?

3.1.1.4 Enlace vía ADSL

Las pruebas de comunicación fueron realizadas el miércoles 26 de marzo del 2008, utilizando equipo y software provisto por la empresa ACTICA, y el conocimiento y facilitación de ingreso a la red de la empresa por parte del Departamento de Recursos Informáticos de la EMAAP-Q.

El enlace de prueba fue efectuado entre la Agencia de Recaudación La Manzana localizada en el centro histórico de la ciudad y el Nuevo Edificio Matriz de la EMAAP-Q, localizado en la Av. Mariana de Jesús e Italia.

En este último, se armó una central de monitoreo de seguridad capaz de monitorear y administrar centrales de alarma, misma que fue instalada en un computador del Departamento de Seguridad Física y Radio Comunicaciones.

El software utilizado fue un emulador de la central DSC POWER 864 (Figura 3.1), capaz de administrar la central de alarma La Manzana.

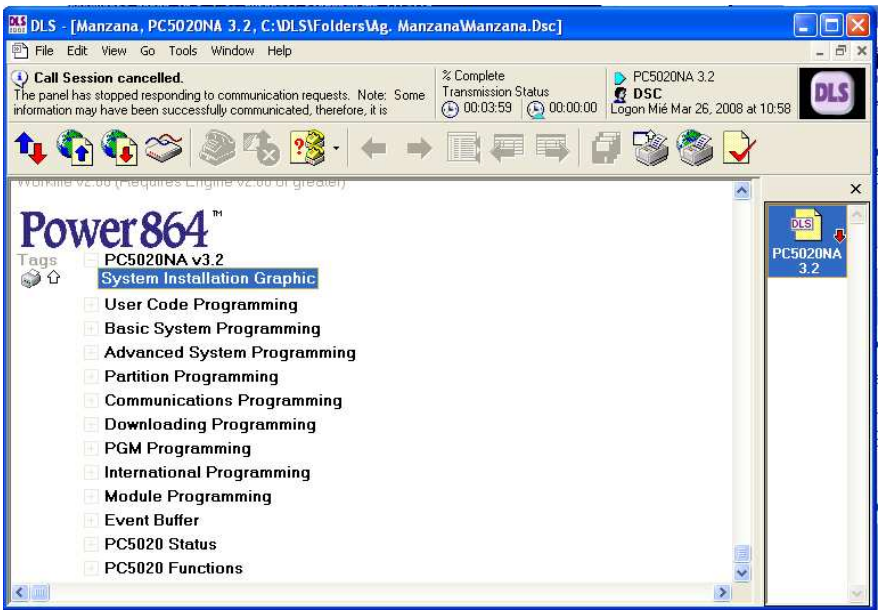


Figura 3.1 *Emulador Power 864*

Como se puede observar en la figura 3.1, el emulador Power 864 presenta todas las características de administración y programación a larga distancia sobre una central de alarma colocado en un lugar específico; este punto permitió una configuración total de los equipos colocados en la Manzana, (Figura 3.2) la misma que se efectuaba simultáneamente a la recepción de datos, en otras palabras, mientras se mantuvo el enlace de datos el emulador enviaba y recibía información.

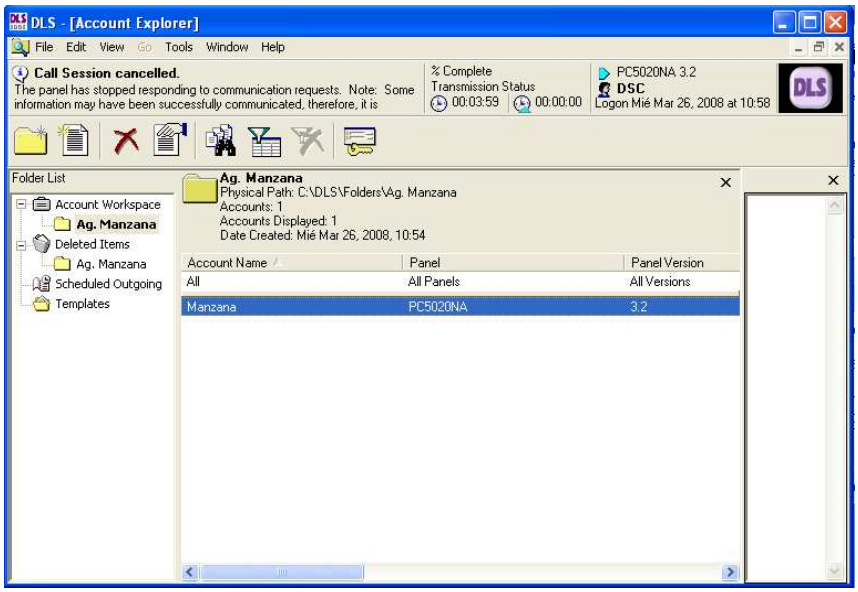


Figura 3.2 *Explorador de Usuarios*

Una de sus principales características presentadas, y que serán tomadas en cuenta el momento de definir la central de monitoreo a adquirir por parte de la EMAAP-Q, es la capacidad de mostrar en pantalla todos los eventos suscitados en tiempo real de una dependencia, programada previamente en su base de datos, como lo fué en este caso el panel de control de la agencia de recaudación La Manzana. (Figura 3.3)

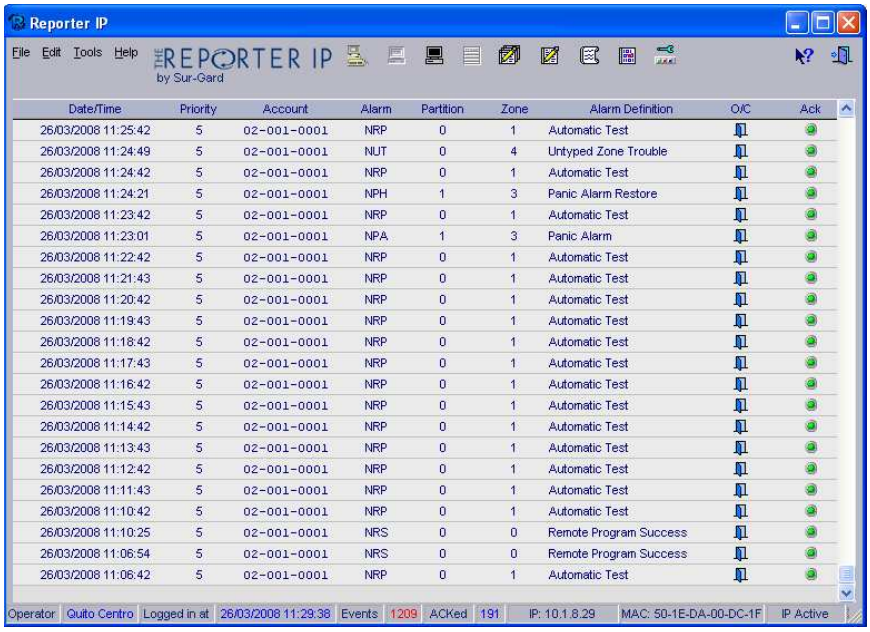


Figura 3.3 *Reportes de eventos*

En la prueba se simularon eventos de tipo:

- Programación remota
- Alarma de pánico
- Intrusión
- Alarma de Incendio
- Activación de la central
- Desactivación de la central
- Respuesta de vida

a. Programación remota

Capaz de establecer una conexión entre la central de monitoreo y la central de alarma para efectuar una configuración del sistema remoto. (A través del software DLS 2002)

26/03/2008 11:10:25	5	02-001-0001	NRS	0	0	Remote Program Success
26/03/2008 11:06:54	5	02-001-0001	NRS	0	0	Remote Program Success

b. Alarma de pánico

Se presenta al ser pulsado un botón de pánico, el mismo que cumple la función de alertar al personal de monitoreo de un asalto en proceso.

26/03/2008 11:24:21	5	02-001-0001	NPH	1	3	Panic Alarm Restore
26/03/2008 11:23:42	5	02-001-0001	NRP	0	1	Automatic Test
26/03/2008 11:23:01	5	02-001-0001	NPA	1	3	Panic Alarm

c. Intrusión

Detalle de evento el cual muestra un ingreso no autorizado al sector monitoreado en cuestión.

26/03/2008 11:26:21	5	02-001-0001	NBH	1	2	Burglary Alarm Restore
26/03/2008 11:26:21	5	02-001-0001	NCR	1	0	Recent Closing
26/03/2008 11:26:18	5	02-001-0001	NBA	1	2	Burglary Alarm
26/03/2008 11:26:01	5	02-001-0001	NCL	1	40	Closing Report

d. Alarma de Incendio

En el caso de colocarse un sensor para dicho propósito, la central de alarma es capaz de enviar un aviso a la central de monitoreo sobre dicha emergencia.

26/03/2008 11:25:46	5	02-001-0001	NFJ	0	0	Fire Trouble Restore
26/03/2008 11:25:42	5	02-001-0001	NRP	0	1	Automatic Test

e. Prueba de vida

En la prueba realizada se programó al equipo de la agencia para que cada minuto envíe una prueba de vida a la central de monitoreo, la misma que cumple la función de alertar al usuario que se encuentra funcionando perfectamente y sin ningún inconveniente.

Este evento tenía que ser reconocido por el monitor del sistema, siendo indicado el mismo por color azul cuando aún no ha sido reconocido, y cambiando a color blanco cuando ya se ha efectuado dicho control.

26/03/2008 12:41:39	5	02-001-0001	NRP	0	1	Automatic Test
26/03/2008 12:40:38	5	02-001-0001	NRP	0	1	Automatic Test
26/03/2008 11:27:04	2	02-001-0001	NFT	0	0	Fire Trouble
26/03/2008 11:24:49	2	02-001-0001	NFT	0	0	Fire Trouble

A más de todos estos detalles de eventos que se probaron, existe una cantidad muy grande de eventos programables dentro de la base de datos, capaces de ser utilizados en aplicaciones de mayor precisión.

3.1.1.5 Tiempos de respuesta del enlace

La Matriz de la EMAAP-Q al encontrarse en continua comunicación con la agencia de recaudación la Manzana, administra todo el envío de datos realizado desde esta dependencia hacia el Departamento de Recursos Informáticos y viceversa.

En la prueba de comunicación efectuada se procedió a transmitir la información necesaria para el envío de datos de la central de alarma sobre la red actual de la empresa, razón por la cual la congestión que se podía producir sobre la misma y la demora de tiempo en el tránsito normal de datos eran factores muy importantes a tener en cuenta.

Fue así que simultáneamente al envío normal de datos, se monitoreo constantemente el tiempo de respuesta (Figuras 3.4 y 3.5) al enlace establecido, cuidando que el mismo no se caiga en ningún momento y que no presente dificultades en la comunicación.

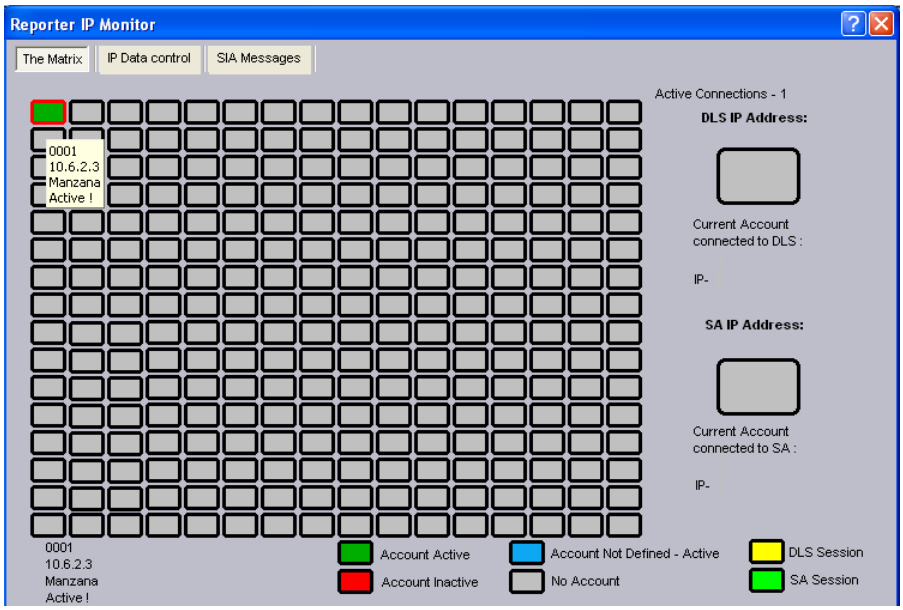


Figura 3.4 *Monitor del enlace*

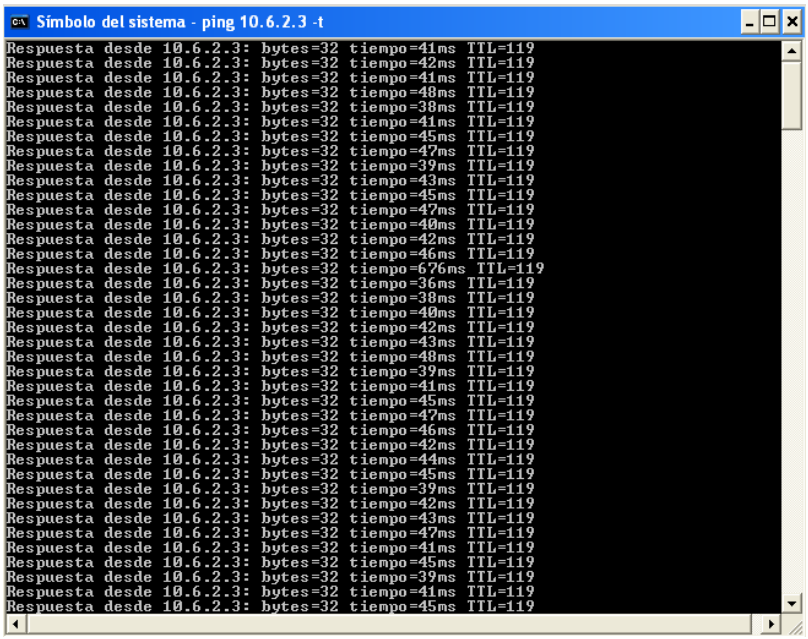


Figura 3.5 *Tiempos de respuesta*

La EMAAP-Q tiene contratado para las agencias un servicio de ancho de banda máximo de 64 kbps, este es un valor fijo no compartido. En lo que se refiere al consumo de ancho de banda en las agencias, este valor varía dependiendo de la afluencia de gente que acude a las mismas, un dato aproximado de consumo de ancho de banda es un pico de 16 kbps que se registró en la Agencia La Manzana por ser la más concurrida y donde más transacciones de dinero se realizan.

Teniendo en cuenta que la información a transmitir en el sistema a diseñarse consumirá un ancho de banda de 128 bits, teniendo esta trama de datos una encriptación propia del fabricante para asegurar el flujo seguro de la información. Se puede concluir entonces que el ancho de banda que tiene contratado la EMAAP-Q es suficiente se puede afirmar que no se tendrá ningún tipo de inconveniente en la implementación del enlace ADSL para este proyecto.

3.1.2 PROCEDIMIENTOS PARA INSTALACIÓN DE EQUIPOS Y CORRECTO USO DE MATERIALES

Dentro de los criterios generales para la instalación del Sistema de Seguridad Electrónica, se puede mencionar que primordialmente, todo el cableado a utilizarse sin importar su funcionalidad final deberá cumplir todas las normas de seguridad eléctrica necesarias, refiriéndose precisamente a que los mismos deben soportar el amperaje y diferencia de voltaje para la función que van a cumplir, respetando los códigos NEC para aplicaciones de fines generales, en tuberías verticales y techos falsos, resistentes a humedad y abrasión, aprobaciones UL, y también, todos los empalmes y conexiones deberán efectuarse con terminales adecuados para la mencionada función.

Los cables de alimentación y señales deben ser conectados a los equipos con sus propios terminales; todos estos cables y equipos deben ser debidamente instalados, identificados y ordenados. Los cables de datos deberán ser del tipo UTP, categoría 5e, no genéricos.

Teniendo en cuenta que los mantenimientos del sistema tras haber sido instalado serán mensuales, se consideró que lo mas práctico será que los cables de datos sean etiquetados cada 5 metros iniciando desde uno de sus extremos, además del extremo final del mismo el momento de llegar al equipo o dispositivo en cuestión, todo con la finalidad de facilitar mantenimientos correctivos en el caso de ser necesarios.

Especificando un poco más las áreas de las instalaciones sobre las cuales se trabajará, se ha dividido las mismas por sus sectores básicos, es decir, tomando una Agencia de Recaudación se obtiene dos áreas independientes a cubrir: área de atención al público y área de trabajadores EMAAP-Q.

3.1.2.1 Área de Atención al Público

Como su nombre lo dice, el área de atención al público se dedica plenamente a la recepción de los clientes, todo con el fin de que los mismos cancelen el servicio prestado de agua potable y alcantarillado que la EMAAP-Q ofrece a la población quiteña. Esta área es amplia en la mayoría de dependencias, posee sillones de descanso y está siendo vigilada continuamente por al menos un guardia que ayuda y guía a los clientes dentro de la agencia.

Siendo así, se ha tomado las siguientes precauciones referidas a la instalación de los implementos en esta área:

- Todo el cableado que deberá atravesar el área de atención al público deberá ser canalizado por tubería metálica conduit tipo EMT de 1 pulgada, las uniones y empalmes serán roscados, utilizándose cuplas, tuercas y/o boquillas.
- Las diferentes conexiones que conforman el sistema integrado de seguridad, no deberán tener cables vistos.

3.1.2.2 Área de funcionarios EMAAP-Q

El área donde se encuentra el personal de la empresa de agua potable se podría considerar el lugar primario a proteger, esto debido a que el dinero recaudado se encuentra repartido en cada una de las cajas de atención al cliente. En la mayoría de las doce agencias, este sector es blindado, pero uno de los afanes de la Empresa de Agua potable es que las mismas posean un grado de seguridad más alto, que sean capaces de transmitir al público en general el interés de la Empresa por mantener el orden y resguardar los bienes municipales.

Siendo así, se ha tomado las siguientes precauciones referidas a la instalación de los implementos en esta área:

- Todo el cableado que recorrerá el área resguardada del bunker deberá ser canalizado por canaletas plásticas, esto, debido a que el acceso a este sector es restringido por puertas de acceso y ventanillas que en su mayoría poseen blindaje anti actos vandálicos, razón por la cual, se puede abaratar costos no utilizando tubería EMT.

- Las diferentes conexiones que conforman el sistema integrado de seguridad, no deberán tener cables vistos, al igual que en el área de atención al público.

3.2 DETERMINACIÓN DE ZONAS

Una zona es el lugar de determinación de un evento específico, denotando con detalle cual es el sensor o dispositivo activado por un acto deseado o no, mientras el elemento se encontraba en vigilia. La determinación de una zona brinda a la persona encargada de monitoreo la facultad de discernir la localización precisa del evento en una instalación, en este caso: una de las agencias de recaudación.

La mayoría de paneles de control en el mercado ofrecen ocho zonas básicas, con capacidad de expandir las mismas en el caso de considerarlo necesario, por tal razón, se utilizará dicho planteamiento como base de diseño. A continuación se desglosará un cuadro, el mismo que detalla cada uno de los equipos que poseerá cada una de las quince instalaciones de la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito.

Cantidad de equipos y distribución de zonas para las 15 Agencias de recaudación

AGENCIAS DE RECAUDACION															
Equipos	**12 de Octubre**	**Atahualpa**	**Iñaquito**	**La Luz**	**Mayorista**	**Chiriyacu**	**Ipiales del Sur**	**Quitumbe**	**Parque Ingles**	**Aeropuerto**	**La Manzana**	**Carapungo**	**Camal Met.**	**San José**	**Chimbacalle**
Contacto Lanfor	1	1	0	0	1	2	0	0	0	0	0	1	0	0	0
Transmisor TCP/IP	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Sirena 30 w	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Gabinete sirena *	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Panel de control	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Magnético Adhesivo	1	1	1	1	1	1	1	2	3	3	2	1	2	2	2
Teclado	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Botón Pánico Recaudación	2	2	2	2	2	3	2	1	2	2	3	2	1	2	1
Botón Pánico Facturación	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1
Sensor PIR	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Discriminador Audio	0	0	1	0	0	2	0	0	1	1	1	0	1	0	0
Botón Pánico Inalámbrico	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Receptor Inalámbrico	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Gabinete de sirena presenta sensor tipo tamper *

Los dispositivos a generar zonas son los sensores, por tal razón y tras analizar las agencias de recaudación se ha obtenido el siguiente resultado preliminar:

AGENCIAS DE RECAUDACION															
	12 de Octubre	**Atahualpa**	**Iñaquito**	**La Luz**	**Mayorista**	**Chiriyacu**	**Ipiales del Sur**	**Quitumbe**	**Parque Ingles**	**Aeropuerto**	**La Manzana**	**Carapungo**	**Camal Met.**	**San José**	**Chimbacalle**
ZONAS	8	8	8	7	8	12	7	7	10	10	11	7	8	8	7

Se toma como referencia un panel de ocho zonas y al verificar los resultados preliminares sobre cantidad de equipo requerido, se puede notar que existen dependencias que superan dicho valor, lo que acarearía un problema, ya que para dar solución a esto se deberá eliminar equipo, comprar un expansor de zonas u optimizar recursos. En este caso y valiéndose que la opción de eliminar dispositivos es inaceptable, y comprar un expansor de zonas resultara caro, se procederá a optimizar los recursos actuales.

3.2.1 Optimización de Zonas

Para proceder a optimizar el resultado preliminar de zonas obtenidas se deben plantear las pautas a seguir:

- Utilizar máximo las ocho zonas que pueda brindar un panel de control comercial,
- Unificar ciertos elementos que traten o monitoreen puntos similares y,
- Elegir equipo que pueda trabajar en conjunto sobre una sola zona.

Continuando con las bases planteadas, y analizando específicamente las agencias: Chiriyacu (12 zonas), Parque Ingles (10 zonas), Aeropuerto (10 zonas) y la Manzana (11 zonas), se debe concluir los cambios que las mismas sufrirán por optimización

3.2.1.1 Agencia Chiriyacu

Esta Agencia posee dos ingresos independientes tipo puerta lanfor, mismos que en el análisis preliminar ocupan una zona cada uno. Como optimización se plantea independizar los mismos utilizando una única zona física, pero derivando la misma en dos direcciones, cuestión que solo puede llevarse acabo si se utiliza sensores magnéticos direccionables de 2 hilos.

Dado el caso que se debe seguir reduciendo zonas, se tendrá que conectar todos los botones de pánico del área de facturación y recaudación en una sola zona de monitoreo.

De esta manera, se ha rebajado el monitoreo de doce a ocho zonas sobre la agencia de recaudación Chiriyacu.

3.2.1.2 Agencia Parque Inglés

Esta Agencia posee un ingreso conformado por dos puertas abatibles, cada una posee un sensor magnético adhesivo. Como optimización se plantea unificar ambos elementos en una única zona física, esto debido a que los mismos cumplen la función en común de monitorear un ingreso en común.

Se conectará todos los botones de pánico del área de facturación y recaudación en una sola zona de monitoreo.

De esta manera, se ha rebajado el monitoreo de diez a ocho zonas sobre la agencia de recaudación Parque Inglés.

3.2.1.3 Agencia Aeropuerto

El Centro de Recaudación Aeropuerto posee una entrada compuesta por dos puertas de vidrio, sobre las cuales se colocará dos sensores magnéticos adhesivos respectivamente. La manera de optimizar la zona que ocuparían los dos magnéticos es la unificación de los mismos en una sola y única zona física.

Dado el caso que se debe seguir reduciendo zonas, se conectará todos los botones de pánico del área de facturación en una única zona, y de igual forma, se conectará todos los botones de pánico del área de recaudación en una sola zona de monitoreo.

De esta manera, se ha rebajado el monitoreo de diez a ocho zonas sobre la agencia de recaudación Aeropuerto.

3.2.1.4 Agencia la Manzana

Se conectará todos los botones de pánico del área de facturación en una única zona, y de igual forma, se conectará todos los botones de pánico del área de recaudación en una sola zona de monitoreo.

De esta manera, se ha rebajado el monitoreo de once a ocho zonas sobre la agencia de recaudación la Manzana.

De esta forma, y tras optimizar las zonas de las cuatro dependencias conflictivas, se concluye que las agencias de recaudación poseerán un análisis de zonas desglosado final:

	ZONAS PERTENECIENTES AL PANEL DE CONTROL							
AGENCIAS	**ZONA 1**	**ZONA 2**	**ZONA 3**	**ZONA 4**	**ZONA 5**	**ZONA 6**	**ZONA 7**	**ZONA 8**
12 DE OCTUBRE	Magnético Adhesivo	Sensor Movimiento	Botón de Pánico R-1	Botón de Pánico R-2	Botón de Pánico F.	Botón Inalámbrico	Tamper	Contacto Lanfor
ATAHUALPA	Magnético Adhesivo	Sensor Movimiento	Botón de Pánico R-1	Botón de Pánico R-2	Botón de Pánico F.	Botón Inalámbrico	Tamper	Contacto Lanfor
IÑAQUITO	Magnético Adhesivo	Sensor Movimiento	Botón de Pánico R-1	Botón de Pánico R-2	Botón de Pánico F.	Botón Inalámbrico	Tamper	Discriminador de Audio
LA LUZ	Magnético Adhesivo	Sensor Movimiento	Botón de Pánico R-1	Botón de Pánico R-2	Botón de Pánico F.		Tamper	Botón Inalámbrico
MAYORISTA	Magnético Adhesivo	Sensor Movimiento	Botón de Pánico R-1	Botón de Pánico R-2	Botón de Pánico F.	Botón Inalámbrico	Tamper	Contacto Lanfor
CHIRIYACU	Discriminador de Audio 2	Sensor Movimiento	Botones de Pánico R y F	Magnético Adhesivo	Discriminador de Audio 1	Botón Inalámbrico	Tamper	2 Contactos lanfor direccionables
IPIALES DEL SUR	Magnético Adhesivo	Sensor Movimiento	Botón de Pánico R-1	Botón de Pánico R-2	Botón de Pánico F.		Tamper	Botón Inalámbrico
QUITUMBE	Magnético Adhesivo 2	Sensor Movimiento	Botón de Pánico R.	Botón de Pánico F.	Magnético Adhesivo 1		Tamper	Botón Inalámbrico
PARQUE INGLES	Magnético Adhesivo 2 y 3	Sensor Movimiento	2 Botones de Pánico R.	Botón de Pánico F.	Magnético Adhesivo 1	Botón Inalámbrico	Tamper	Discriminador de Audio
AEROPUERTO	Magnético Adhesivo 2 y 3	Sensor Movimiento	2 Botones de Pánico R.	Botón de Pánico F.	Magnético Adhesivo 1	Botón Inalámbrico	Tamper	Discriminador de Audio
LA MANZANA	Magnético Adhesivo 2	Sensor Movimiento	3 Botones de Pánico R.	Botón de Pánico F-1	Magnético Adhesivo 1	Botón Inalámbrico	Tamper	Discriminador de Audio
CARAPUNGO	Magnético Adhesivo	Sensor Movimiento	Botón de Pánico R-1	Botón de Pánico R-2	Botón de Pánico F.	Botón Inalámbrico	Tamper	Contacto Lanfor
CAMAL METROPOLITANO	Magnético Adhesivo 1	Magnético Adhesivo 2	Sensor Movimiento	Botón de Pánico R.	Botón de Pánico F.	Botón Inalámbrico	Tamper	Discriminador de Audio
SAN JOSE NOROCCIDENTE	Magnético Adhesivo 1	Magnético Adhesivo 2	Botón de Pánico R-1	Botón de Pánico R-2	Botón de Pánico F.	Botón Inalámbrico	Tamper	Sensor de Movimiento
CHIMBACALLE	Magnético Adhesivo 1	Magnético Adhesivo 2	Sensor Movimiento	Botón de Pánico R.	Botón de Pánico F.	Botón Inalámbrico	Tamper	

Y resumiendo número de zonas:

AGENCIAS DE RECAUDACION															
	12 de Octubre	Atahualpa	Iñaquito	La Luz	Mayorista	Chiriyacu	Ipiales del Sur	Quitumbe	Parque Ingles	Aeropuerto	La Manzana	Carapungo	Camal Met.	San José	Chimbacalle
ZONAS	8	8	8	7	8	8	7	7	8	8	8	8	8	8	7

3.3 ESPECIFICACIONES TECNICAS

Independientemente que cada instalación poseerá cierto tipo de equipos según sus necesidades, muchas de ellas deberán compartir características similares.

Como primera característica general, el Sistema Integrado de Seguridad deberá permitir su integración con los sistemas actuales de control de accesos que posee la EMAAP-Q en varias de sus instalaciones, dichos sistemas pertenecen a la marca American Auto - Matrix de la línea Key Master.

En referencia a la línea Key Master, se debe mencionar como característica de especificación técnica que sus lectoras RFID deberán ser compatibles con los paneles de control a adquirir, en otras palabras, los paneles deberán trabajar con protocolo Wiegand.

Además, se debe especificar que los paneles de control deberán tener la facilidad de acoplarse en un futuro a video grabadoras digitales con cámaras de circuito cerrado de televisión, que la EMAAP-Q podría adquirir posteriormente, para una rápida y oportuna verificación por parte del personal de operadores de las grabaciones de los eventos capturados a través de las cámaras de video; en otras palabras, plantear la base de un sistema integrador.

3.3.1 Paneles de Control

Un panel de control como punto inicial, se debe dimensionar según el número de sensores o dispositivos a colocar en el mismo y en la distribución de zonas que se quiera tener para mantener un monitoreo efectivo.

A pesar que anteriormente se planificó el uso de 8 zonas máximo en cada una de las Agencias de Recaudación para optimizar equipos, se debe resaltar que

el Departamento de Seguridad Industrial de la EMAAP-Q planificó acoplar a futuro a los paneles de control sensores de humo y estaciones manuales de incendio, por tal razón, dentro de las especificaciones de los equipos se debe resaltar la posibilidad de expandir el número de zonas haciendo uso de tarjetas externas.

De acuerdo al análisis realizado, y teniendo en cuenta las necesidades de la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito, en sus especificaciones, el panel de control a más de ser dedicado a un Sistema de Intrusión deberá ser capaz de integrar sistemas de Circuito Cerrado de Televisión y Control de Accesos, ya que el deseo de la EMAAP-Q es unificar los mismos a futuro en una sola central.

El equipo deberá poseer salidas programables, que pueden cumplir funciones como activar una sirena, una luz estroboscópica, o cualquier dispositivo digital que pueda ser considerado como una ayuda en cuanto a monitoreo o acción de alerta al tener una emergencia.

Para optimización de comunicaciones, se resaltará que los paneles de control deberán poder trabajar con sensores de última tecnología, razón por la cual, se detallará que el mismo debe cumplir la facilidad de acoplamiento con dispositivos que trabajen a cuatro hilos (dos de alimentación y dos para transmisión de datos), dos hilos (dos hilos capaces de alimentar al sensor y transmitir por la misma vía la información que el mismo detalle), dispositivos inalámbricos comerciales con aprobación UL y, sensores que trabajen como normalmente abiertos o normalmente cerrados.

Deberá ser capaz de activar o desactivar zonas según programación vía ADSL, así como la facilidad de acoplarse a dispositivos que transmitan la mencionada información de Agencia a Edificio Matriz EMAAP-Q y viceversa.

En las Agencias de Recaudación pertenecientes a la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito se colocará el mismo tipo de panel.

Resumiendo lo anteriormente aquí detallado se ha desarrollado las especificaciones técnicas correspondientes:

- Panel de Control Comercial para Intrusión (no genérico)
- Alimentación a través de un transformador con salida de 16.5 VAC.
- Mínimo 8 zonas cableadas, capacidad de expansión hasta 128 zonas.
- Métodos de expansión a cumplir: convencional, direccionable (2 hilos) y dispositivos inalámbricos comerciales UL.
- Capacidad de registrar 500 eventos suscitados.
- Posibilidad de creación de 50 usuarios mínimo.
- 4 niveles de autoridad mínimo.
- Capacidad de integración con Control de Accesos (con protocolos Wiegand)
- Capacidad de integración con Sistemas de CCTV.
- Salida de sirena.
- 4 salidas programables como mínimo.
- Soporte de eventos calendarizados de armado / desarmado y control de automatización.
- Certificación de aprobación de robo: UL609, UL611/1610 Grades A, AA, Central Station y UL365 Grades A, AA Police Connect.
- Reducción de falsas alarmas.
- Soporta sensores normalmente abiertos y/o normalmente cerrados.
- Reporte de encendido y en actividad con tiempos y agendas.
- Capacidad de acoplarse a interfaces para transmisión de la información vía TCP/ IP y GPRS.
- Debe incluir su gabinete y transformador.

Algo que cabe denotarse es que en el análisis realizado en ciertas dependencias, se obtuvo como conclusión que algunas de ellas necesitan utilizar más de 8 zonas para obtener un control preciso en la ubicación de emergencias, pero las especificaciones del panel de control solo muestran 8 básicas, con capacidad de expandirse a 128 en el caso de considerarse

necesario, por tal razón, las especificaciones del teclado que funcionará como interfaz del panel deberá proveer de una zona extra, para ser capaz a futuro de expandir cierto requerimiento.

3.3.2 Teclado

Para la elección del teclado se debe tomar en cuenta algunos puntos que son determinantes en la manipulación de los equipos. Por ejemplo, se debe tener en cuenta que la manipulación diaria a la que van estar expuestos estos dispositivos por parte de los usuarios, ya sean de la empresa (recaudadores) o el guardia de seguridad, exigen que el teclado posea palabras fijas en español, con una pantalla LCD para un fácil manejo del mismo, ya que las personas que tratan con él no tienen un adiestramiento en la programación de equipos electrónicos.

Por el motivo expresado anteriormente, de que las personas que van a manipular estos dispositivos no tienen un conocimiento muy extenso en la programación de dispositivos electrónicos, se ha visto en la necesidad de capacitar a una de las personas que pertenezcan a la agencia en el manejo de este equipo. En este caso, la empresa EMAAP-Q con el Departamento de Seguridad Física y Radiocomunicaciones, tomarán la decisión de a qué persona se la capacitará para la manipulación del teclado. Esta capacitación será básica y exclusivamente para los fines necesarios.

Para no adquirir dispositivos o tarjetas de expansión de zonas para los paneles de control, se debe tomar en cuenta que existen teclados que poseen zonas extras, y debido a que todas las agencias necesitan un teclado y el beneficio en el costo se muestra claramente en adquirir un teclado que incluye cuatro zonas extras y un relé, se desglosa el precio aproximado de una tarjeta de expansión de 8 zonas, el cual es de USD 100 y el precio aproximado de un teclado con esta característica es de USD 147, entonces es más conveniente adquirir el teclado con las zonas extras que el teclado normal y aparte la tarjeta de expansión de zonas.

Una de las características más importantes que debe cumplir, es que debe ser compatible con el panel de control que se utilice, ya que por medio del teclado se utilizarán las zonas extras que se necesiten dependiendo de la agencia de recaudación.

Como el teclado no es un dispositivo al cual se lo esté vigilando continuamente, una característica que debe tener es la de poseer un parlante para que produzca pitidos o avisos audibles en caso de que exista algún problema en este equipo.

Además de la característica anterior, se han visto detalles del teclado que pueden ser útiles en la manipulación como lo es, poseer teclas de goma retroiluminadas.

Cabe mencionarse que en las Agencias de Recaudación pertenecientes a la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito se colocará el mismo teclado.

Resumiendo lo anteriormente aquí detallado se ha desarrollado sus especificaciones técnicas según el análisis efectuado en este tipo de dependencias:

- Compatible con los paneles de control tratados en el punto uno.
- Teclas de goma retro iluminadas.
- Teclado grande y fácil de utilizar con visor alfabético en español.
- Parlante con pitidos audibles para indicar el estado del sistema.
- 4 zonas en placa.
- 1 relé programable
- 4 teclas de función programables.

3.3.3 Transmisor Vía TCP/IP

Para realizar la transmisión sin ningún problema, se necesitan todos los dispositivos o tarjetas de comunicación para transmitir la información del panel de control hasta llegar a la red que utiliza la EMAAP-Q para transmitir vía IP los datos requeridos en la matriz.

Los equipos de transmisión que se vayan a usar deben ser compatibles con los paneles de control que se escogieran, para las funciones antes indicadas.

3.3.4 Sirena

Este será un dispositivo electrónico independiente de 30 vatios que utilizará una fuente de 6 a 12 voltios DC, rango que utilizan los paneles de control para la alimentación de sus dispositivos.

Otras de las características que deben tener estos dispositivos es tener un tono intermitente en el caso de que sea activado, y que para actos vandálicos, la sirena posea una placa anti-manipulación para proteger los cables de datos.

Resumiendo las especificaciones antes mencionadas podemos detallar lo siguiente:

- Sirena independiente de 30 vatios.
- 6 a 12 voltios DC y máximo 0.7 amperios.
- Un tono intermitente.
- Placa anti-manipulación para proteger los cables de ataques externos.

3.3.5 Gabinete de Protección para la Sirena

Este gabinete es para la protección de la sirena ya que en muchos de los casos las mismas estarán al aire libre y necesitan protección contra las inclemencias del tiempo.

Además deben tener una protección contra vandalismos como son intentos de abertura, barrenar o cincelar para dañar la sirena, por tal razón, constará de un tamper para alertar de un acto no deseado de manipulación.

3.3.6 Botones de Pánico

Su modo de trabajo es de enclavamiento, esto debido a que no se desea obtener falsas alarmas, por ende, para resetear los mismos, se debe requerir de una llave de desactivación.

Las características que deben cumplir estos dispositivos son:

- Botón de empuje de enclavar, demostraciones de la bandera cuando está presionado.
- Dos llaves de reseteo.
- Carcasa de alto impacto
- Switch de 1 Amp, 12VDC.

3.3.7 Baterías de Respaldo para los Paneles

Estas deben abastecer de energía al panel de control y a todos los dispositivos conectados al mismo en caso de que falle la energía eléctrica normal suministrada. Se recomienda una batería de respaldo de 12 VDC y 7 amperios para que el sistema siga en funcionamiento mientras se recupere la energía eléctrica.

Las características y especificaciones de estos dispositivos son:

- Batería de Respaldo a 12 VDC / 7 Ah
- Compatible con los paneles de control detallados en el punto uno y punto dos.
- Libre de mantenimiento.
- Proporciona una máxima corriente de 7 Amperios-Hora.
- Aplicación para fuentes de respaldo y paneles de alarma.

3.3.8 Discriminador de Audio

De acuerdo al análisis realizado, se vio la necesidad de la colocación de discriminadores de audio en las agencias que tienen ventanales para monitorear casos de actos vandálicos que puedan destruir estas estructuras.

Este dispositivo deberá realizar un procesamiento digital de la señal para que no procese falsas alarmas en caso de que exista algún ruido que no represente emergencia para la agencia.

Resumiendo sus especificaciones técnicas tenemos:

- Detección hasta 7 metros.
- Procesamiento digital de la señal para evitar falsas alarmas.
- Para todo tipo de vidrios: laminado, con alambre, templado e inastillable.
- Funcionamiento a 12VDC

3.3.9 Contacto Magnético para montaje en superficie

Estos dispositivos son recomendados para ubicarlos tanto en las puertas de acceso a las ventanillas de recaudación y facturación, puesto que son fáciles de instalar y son muy eficaces en su función, así como en ingresos a ciertas

agencias que poseen puertas del tipo abatible. Las características que deben cumplir estos contactos son las siguientes:

- Contacto magnético miniatura con imán para montaje sobre superficie.
- Para circuitos normalmente cerrados.
- Incluir cinta para cubrir los tornillos de los terminales.
- Montaje con tornillos utilizando pestañas laterales y con cinta adhesiva.

3.3.10 Contacto Magnético Lanfor Tecnología Direccionable 2 hilos

El contacto magnético direccionable a 2 hilos será usado en las puertas metálicas tipo lanfor de la Agencia Chiriyacu, esto debido a la optimización de zonas que requiere la dependencia. Para esto, el dispositivo mencionado debe cumplir con ciertas características que proporcionen más seguridad en el funcionamiento del equipo, ya que el mismo va a estar expuesto continuamente al tránsito del público.

Este dispositivo trabajará con una tecnología direccionable a dos hilos, es decir, se transmitirá información y se alimentará al mismo por la misma vía.

Las características más importantes que deben cumplir estos dispositivos se detallan a continuación:

- Contacto magnético para puerta superior compatible con los paneles de control indicados anteriormente.
- Funcionamiento con tecnología direccionable a dos hilos.
- Indicado para instalación en puertas abatibles.
- Soporte imantado en forma de L ajustable.
- Sellado epoxi para protección contra humedad e impacto.

3.3.11 Contacto Magnético Lanfor

Este dispositivo realizará las mismas funciones que el contacto mencionado en el punto anterior, pero no funcionará con la tecnología de funcionamiento direccionable a dos hilos.

Para este dispositivo las características a cumplirse serán las siguientes:

- Contacto magnético para puerta superior compatible con los paneles de control indicados en el punto uno de este anexo.
- Indicado para instalación en puertas abatibles.
- Soporte imantado en forma de L ajustable.
- Protección contra inmersión e impacto.
- Sellado epoxi para protección contra humedad e impacto.

3.3.12 Sensor de Movimiento

Estos sensores de movimiento deben ser capaces de cubrir toda el área de la agencia de recaudación; para esto es necesario revisar el alcance de los mismos para escoger el que más se ajuste a la necesidad de las instalaciones de la EMAAP-Q.

Otras de las características que se debe tomar en cuenta son las siguientes:

- Detector de Movimiento uso comercial.
- Alcance: 50 pies x 50 pies
- Funcionamiento a 12VDC
- Montaje en pared, esquina o cielorraso.
- Ajuste de sensibilidad de infrarrojo pasivo (PIR)
- No debe requerir de calibración de altura para su instalación.
- Diseño compacto para instalaciones residenciales.
- Compensación de temperatura.
- Debe tener sistema de anti enmascaramiento.

3.3.13 Botón de Pánico Inalámbrico

El botón de pánico que se piensa adquirir será de uso exclusivo de los guardias de seguridad. Su fin es alertar de una emergencia inmediatamente, sin necesidad de movilizarse.

Las características de estos dispositivos son:

- Dispositivo personal de tipo botón para situaciones de pánico.
- Accionamiento con un solo botón.
- Funcionamiento con batería capaz de ser reemplazada por el usuario.
- Para ser utilizado como colgante o con broche para el cinturón.
- Compatible con el receptor inalámbrico que se detalla a continuación.

3.3.14 Receptor Inalámbrico

Este dispositivo ayuda a que las señales del botón inalámbrico lleguen al panel de control, y su vez, enviar los datos a la central de monitoreo en la matriz de la EMAAP-Q.

La característica principal que necesita cumplir este receptor es el de ser compatible con el panel de control.

3.3.15 Computador para Soporte de Software de la Central de Monitoreo

Las características que debe tener el computador para manejar el software y la comunicación en el centro de monitoreo deben ser las siguientes:

Procesador:	Intel Core 2 Duo
Velocidad de Procesador:	2.13 Ghz
Memoria Caché:	2 MB cache L2

Memoria RAM:	4 Gb 667 Mhz DDR2
Disco duro:	160 GB SATA, 7200 rpm 3.0 Gbs
Tarjeta de red:	Ethernet 10/100/1000
Unidad óptica:	SATA DVD Rom/ CDRW Combo
I/O Puertos:	6 USB ver 2.0 1 puerto para teclado 1 puerto para Mouse 1 audio in, 1 audio out, 1 microphone in, 1 headphone/Line out 1 VGA monitor
Bahía de expansión:	1 interna de 3.5”; 1 externa de 3.5” y 1 externa de 5.25 “
Slots de expansión:	1 PCI convencional y 1 PCIe x16
Monitor:	TFT, color negro de 21”
Teclado:	Expandido en español tipo Windows
Mouse:	Scroll Mouse óptico – dos botones
Software:	Licencia de Windows XP (SP2) Profesional en Español o en su defecto MS Vista 32B Downgrade to XP32
Medios de soporte:	CD o diskettes del Hardware y Software instalados (si hubiera)
Accesorios:	Parlantes multimedia 100W

3.4 REQUERIMIENTOS DEL SOFTWARE

El sistema necesita un software de administración y gestión capaz de manejar la información de los quince distintos paneles de control que pertenecen a las agencias antes mencionadas que transmitirán la información pertinente del sistema de seguridad electrónica vía ADSL desde las dependencias de la EMAAP-Q hasta la Matriz de la mencionada Empresa localizada en la ciudad de Quito, Av. Mariana de Jesús e Italia.

El software de administración del sistema integrado de seguridad, permitirá al operador del centro de seguridad, mantener un control adecuado de sistemas de circuito cerrado de televisión, control de accesos e intrusión cuando estos sean implementados en su debido tiempo.

Permitirá interrelacionar las diferentes funciones y aplicaciones de los referidos sistemas, mediante programación “lógica”.

El software de administración y gestión del sistema integrado de seguridad, dispondrá de una licencia mínima de un año para 5 usuarios, deberá ser compatible con los datos transmitidos por los Paneles de Control detallados anteriormente vía TCP/IP.

Deberá tener la capacidad de instalarse sobre plataformas Windows XP y Windows Server 2003, además, capacidad de exportar un histórico de eventos a Excel.

Sobre sus capacidades y aplicaciones futuras, este software deberá ser capaz de enlazarse a un mínimo de 400 paneles de control con comunicación vía IP y 400 paneles de control con comunicación vía GPRS, valiendo recalcar, que para la comunicación vía GPRS se necesitará contratar los servicios de una empresa celular con un servicio de Ultima Milla.

Deberá tener la capacidad de informar eventos de alarmas por medio de correo electrónico, enviando la situación y tipo de alarma a un e-mail previamente programado sobre su sistema.

Su interfaz debe ser capaz de mostrar la información concerniente a número de evento, fecha y hora del evento, mensaje del evento, código del evento, descripción del evento, zona del evento y tipo de interfaz que envía el evento.

El mencionado software deberá tener la capacidad de funcionamiento sobre el computador con las características detalladas.

Como punto extra, en la adquisición del software, se recomienda a la EMAAP-Q que solicite a la empresa la cual proveerá este sistema, el costo adicional por licencia sobre un período especifico de tiempo, ya sea que el mismo varíe en el transcurso de un (1) año o sobre cualquier otro rango propuesto por la empresa proponente, así como, se deberá adjuntar el costo propuesto por mantenimiento anual del software presentado.

3.5 PRESUPUESTO REFERENCIAL

Ya con el conocimiento sobre el tipo de dispositivos y que características deben cumplir los mismos, se debe proceder a obtener un presupuesto referencial de cada uno de los elementos que conformarán el sistema de seguridad electrónica con alarmas monitoreadas para doce agencias de recaudación de la EMAAP-Q.

Para efectuar el análisis financiero, se debe plasmar las especificaciones técnicas en práctica, es decir, se debe buscar marcas de productos y modelos de equipos que cumplan lo requerido.

3.5.1 Elección de marcas referenciales

Dentro del sistema integral de seguridad electrónica a implementarse, tanto los paneles de control como su software de monitoreo plantean la elección de la marca referencial del proyecto, esto debido a que estas dos partes conforman la base principal del mismo.

Para tener una noción de las empresas que producen y distribuyen este tipo de equipos, se debe nombrar las marcas líderes, tanto en el mercado nacional y extranjero en cuanto a seguridad electrónica, estas son Honeywell y DSC.

Ambas marcas desarrollan equipos destinados a la automatización y control de ambientes, ya sean industriales, comerciales o residenciales. En nuestro

caso, y debido a que la EMAAP-Q posee referencias con equipos Honeywell, se ha elegido la misma para planificar la base de equipos de este proyecto.

3.5.2 Modelos de equipos

Honeywell maneja una gama de paneles de control muy extensa, ya sea para aplicaciones residenciales básicas o aplicaciones comerciales que exijan alto grado de complejidad, como lo es este caso, integración de sistema de alarmas, circuito cerrado de televisión y control de accesos.

La idea es encontrar modelos de equipos que sean fáciles de instalar, fáciles de usar y que desenvuelvan a total plenitud sus funciones programadas, todo esto considerando su valor económico en el mercado.

A continuación se procederá a detallar rápidamente los modelos de la línea ADEMCO VISTA, capaces de cumplir a plenitud las especificaciones técnicas solicitadas.

3.5.2.1 Panel de Control Vista 128FBP

Este panel de control combina funciones de incendio/ robo, además tiene la capacidad de integrarse a sistemas de acceso y CCTV de la propia línea ADEMCO VISTA. (Figura 3.6)

Figura 3.6 *Panel de control Vista 128FBP*

Debido a su robustez, cumple normativas UL 609 (Protección de grado A para establecimientos mercantiles y bóvedas mercantiles), UL611/1610 (Grados A y AA para estaciones centrales), UL365 (Grados A y AA para conexión policial) y UL864/NFPA 72 (estación local, central y remota para paneles dedicados a monitoreo de emergencias en situaciones de incendio)

Posee 8 zonas básicas con la opción de expandir las mismas a 128. Además de utilizar métodos de expansión convencional, V-Plex (dos hilos) y dispositivos inalámbricos UL.

Su costo referencial en el mercado ecuatoriano asciende a USD 902.60 sin IVA.

3.5.2.2 Teclado 6164 SP

Este modelo de teclado cumple con todas las especificaciones técnicas, presenta un teclado con iluminación posterior constante, un visor alfabético en español, 4 zonas en placa, 4 teclas de función programables y 1 rele programable tipo Forma C. (Figura 3.7)

Figura 3.7 *Teclado 6164 SP*

Su costo referencial en el mercado ecuatoriano asciende a USD 147.00 sin IVA.

3.5.2.3 Transmisores de información vía IP

Dentro de la gama Honeywell existe el equipo LPL con el modelo **LHOTCP IP**, el cual se adapta al modulo RS232 4100SM de Ademco, logrando transmitir vía IP información de cualquier central VISTA. Una pequeña topología del resultado final a obtenerse en el proyecto se presenta en la Figura 3.8

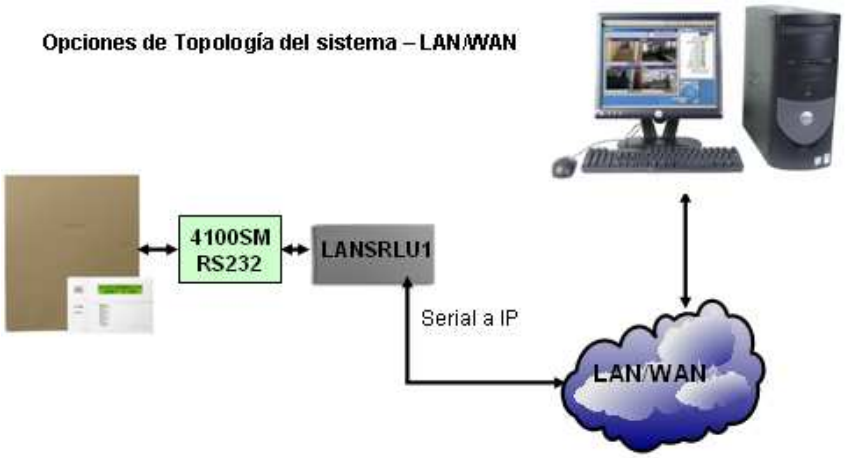


Figura 3.8 *Topología del Sistema*

Dentro de sus características principales se puede resaltar la programación remota de los paneles de alarma (Honeywell), monitoreo de línea telefónica, monitoreo del panel de alarma y monitoreo de la red TCP IP.

Su precio en el mercado ecuatoriano es de USD 450 sin iva.

3.5.2.4 Sirena

La sirena Honeywell 738, como lo muestra la figura 3.9, está diseñada para uso en interiores y exteriores, es de fácil instalación e incluye circuito tamper de protección.

Figura 3.9 *Sirena Honeywell 738*

Su precio en el mercado ecuatoriano es de USD 17.60 sin iva.

3.5.2.5 Gabinete para sirena

El gabinete para la sirena debe contener ciertas características especiales, entre ellas, su funcionalidad en exteriores y la capacidad de acoplar un seguro tamper al mismo.

El precio de este equipo en el mercado ecuatoriano es de USD 15 sin iva.

3.5.2.6 Botones de pánico

Un botón de pánico que cumple las especificaciones aquí expuestas es el modelo Honeywell 270R, con aprobación de norma UL636. Su precio en el mercado ecuatoriano es de USD 21.30 sin iva. Figura 3.10.

Figura 3.10 *Botón de Pánico.*

3.5.2.7 Baterías de respaldo

Una de las baterías encontrada en el mercado es la VIPERTEK VIP-712 , un dispositivo de este tipo cumple con las especificaciones detalladas anteriormente, y en el mercado se lo puede encontrar a un valor aproximado de USD 26sin iva.

Las principales características de esta batería son:

- Viper Tek Batteries
- VIP – 712
- 12 V 7 Ah / 20 Hr
- Voltaje Constante de Carga (25ºC)
- Ciclo de uso: 14.4 – 15.0 V
- Uso en pasivo: 13.5 – 13.8 V
- Corriente Inicial: menos de 2.10 A.

Figura 3.11 *Batería de respaldo 7 amp/ h*

3.5.2.8 Discriminador de Audio

Para este equipo en especial no se a tomado en cuenta un equipo Honeywell, sino DSC, ya que por especificaciones cumple con lo que este proyecto necesita y es más económico a la vez.

El modelo Acuity, mostrado en la Figura 3.12, es un discriminador de audio capaz de detectar el quiebre del mismo, captando dichos ruidos hasta una distancia de 7.6 metros. Posee un sistema capaz de procesar digitalmente la señal y evitar activaciones a causa de falsas alarmas.

Figura 3.12 *Discriminador de Audio Acuity*

Su precio en el mercado ecuatoriano es de USD 40.00 sin iva.

3.5.2.9 Contactos magnéticos para montaje en superficie

Contactos magnéticos adhesivos que cumplen con las características de especificaciones técnicas detalladas aquí pueden ser los Honeywell 945, de la Figura 3.13, mismo que tiene un costo de USD 5.00 sin iva en el mercado ecuatoriano.

Figura 3.13 *Contactos Magnéticos Adhesivos Honeywell*

3.5.2.10 Contacto Magnético Lanfor Tecnología Direccionable 2 hilos

El contacto direccionable Honeywell 4959sn, mostrado en la Figura 3.14, utiliza la tecnología de comunicación y alimentación por dos hilos, conocida dentro de la línea ADEMCO como tecnología V-Plex.

Figura 3.14 *Contacto lanfor V-Plex 4959SN*

Cumple con todas las especificaciones técnicas detalladas en este capítulo, su precio en el mercado ecuatoriano asciende a USD 42 sin IVA.

3.5.2.11 Contacto Magnético Lanfor

Un dispositivo que cumple con las características técnicas detalladas es el Honeywell 958, mostrado en la Figura 3.15. Este es un contacto que posee sus cables de conexión reforzados y soporte golpes en su estructura.

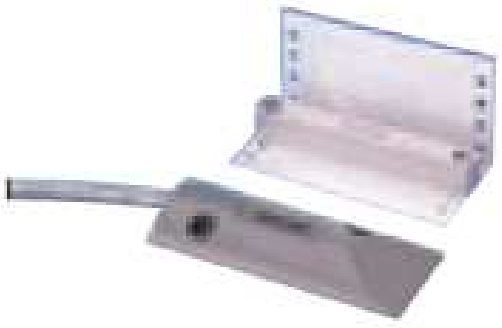


Figura 3.15 *Contacto Magnético Lanfor*

El costo de este dispositivo en el mercado ecuatoriano es de USD 21.00

3.5.2.12 Sensor de Movimiento

El sensor Honeywell IS2535 es del tipo PIR, en otras palabras: sensor infrarrojo pasivo. Posee la característica de cubrir un rango de distancia de 11 x 12m.

Como se observa en la Figura 3.16, posee la característica de tener doble cobertura por parte del sensor infrarrojo, es decir, la normalmente conocida en un sensor de movimiento y una inferior, capaz de cubrir toda el área directamente vertical al dispositivo.

Figura 3.16 *Sensor PIR IS2535*

Uno de sus requerimientos en cuanto a instalación es la altura, la cual según sus especificaciones, debe encontrarse en un rango de 2.3 a 2.7 metros.

Su costo en el mercado es de USD 16 sin IVA.

3.5.2.13 Botón de Pánico Inalámbrico y Receptor

Un kit de este tipo puede ser el Enkriptor, mismo que cumple las especificaciones técnicas y tiene un costo en el mercado de USD 38.00 sin IVA.

Figura 3.17 *Sensor PIR IS2535*

Este dispositivo posee un control remoto capaz de transmitir tres señales, las cuales, pueden ser definidas por el controlador inalámbrico.

3.5.2.14 Cuadro resumido de costos

Precios Equipos para Agencias			
Equipos	**Costo Unitario**	**Cantidad**	**Costo Total**
Contacto Lanfor direccionable	$ 42.00	2	$ 84.00
Contacto Lanfor	$ 21.00	4	$ 84.00
Sirena 30 w	$ 17.60	15	$ 264.00
Gabinete protección sirena	$ 12.00	15	$ 180.00
Panel de control, gabinete y transformador	$ 902.60	15	$ 13,539.00
Interfaz comunicación panel a serial RS232	$ 70.00	15	$ 1,050.00
Interfaz comunicación serial RS2323 a IP	$ 380.00	15	$ 5,700.00
Teclado	$ 147.00	15	$ 2,205.00
Magnético Adhesivo	$ 5.00	24	$ 120.00
Botones Pánico Recaudación y Facturación	$ 21.30	45	$ 958.50
Sensor de Movimiento	$ 16.00	15	$ 240.00
Discriminador Audio	$ 40.00	7	$ 280.00
Kit inalámbrico	$ 38.00	15	$ 570.00
Material eléctrico promedio por cada agencia de recaudación(UTP, gemelo, canaleta plástica, cajetines, etc)	$100.00	15	$ 1500.00
		Total	**$ 26,774.50**

Desglose de equipos para matriz

Equipos para la Matriz			
Equipos	**Costo Unitario**	**Cantidad**	**Costo Total**
Software	$ 5,704.00	1	$ 5,704.00
Central de recepción	$ 4,000.00	1	$ 4,000.00
Computador (server y administración a com. IP)	$ 1,449.00	1	$ 1,449.00
		Total	**$ 11,153.00**

Obteniendo un costo aproximado del proyecto de USD 37,927.50

3.6 IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD ELECTRÓNICA

La Empresa Metropolitana de Alcantarillado y Agua Potable de Quito, a pesar de tener su entera disposición y deseo por la implementación de este proyecto, se ha visto retardada en llevar el mismo a la realidad, esto debido a cuestiones netamente financieras, ya que al tiempo en el cual se finalizó el análisis y diseño del Sistema de Seguridad Electrónica, se procedió a preparar la partida presupuestaria y solicitud de bienes, pero dicho proceso se ha visto retrasado por falta de fondos destinados a este tipo de proyectos. Por esta razón, y debido a que la tesis aquí realizada exige el factor de implementación, se ha visto la necesidad de implementar los equipos de seguridad en una de las agencias de recaudación, y a la vez, comprobar su óptimo funcionamiento con la instalación de un software de control y monitoreo en una de las computadoras pertenecientes al Departamento de Seguridad Física y Radio Comunicaciones de la EMAAP-Q.

En este capítulo se procederá a detallar la parte de implementación, configuración y programación de los equipos asignados a la agencia de recaudación Ipiales del Sur, así como se procederá a realizar todas las pruebas necesarias en cuanto se refiere al funcionamiento de los equipos y del sistema en general, para así demostrar la factibilidad del proyecto que se ha venido detallando anteriormente.

3.6.1 EQUIPOS A UTILIZAR

Debido a que por parte de la EMAAP-Q no se obtendrán los fondos necesarios para la compra de equipos, se ha realizado un pequeño estudio de dispositivos, el mismo que tiene el fin de detallar elementos que resulten económicamente asequibles por nuestra parte como tesistas, y a la vez, que cumplan con todo lo detallado en el alcance de este proyecto.

3.6.1.1 Panel de Control DSC PC 5020

Su estructura básica esta comprendida de 8 zonas básicas, con una capacidad de ser expandido a 64 mediante el uso de tarjetas de acoplamiento. Debido a que el requerimiento de la agencia de recaudación Ipiales del Sur exige poseer 7 zonas, se cumple el primer factor que exige el diseño original: suficientes zonas según requerimiento de la dependencia.

La Figura 3.18 muestra el equipo DSC PC 5020, su estructura y componentes.

Figura 3.18 *Panel de Control DSC PC 5020*

3.6.1.2 Teclado DSC PK5500

El teclado DSC PK5500, mostrado en la Figura 3.19, posee la característica de brindar tres funciones simulando botones de pánico (alarma de incendio, médica o robo).

Figura 3.19 *Teclado DSC PK5500*

Este teclado posee una pantalla LCD para que el control del sistema sea más sencillo. Otra de las características importantes, es que tiene un zumbador piezoeléctrico el cual ayuda con sonidos de confirmación cuando se lo está manipulando. Este teclado utiliza un voltaje de 12 VDC.

3.6.1.3 Sirena de 122 db Chowsons International

Esta sirena trabaja a 12 VDC, tiene la característica de consumir hasta 1000 mA cuando se encuentra en funcionamiento.

Como se muestra en la Figura 3.20, la misma viene dentro de su caja de protección, a la cual se debe acoplar el dispositivo tamper de seguridad, capaz de alertar todo intento de manipulación indebida.

Figura 3.20 *Sirena con su gabinete*

En la Figura 3.21 se muestra el dispositivo tamper, este es un SECO LARM, modelo SS-072Q, para circuitos normalmente cerrados.

Figura 3.21 *Dispositivo tamper*

3.6.1.4 Transmisor vía TCP/IP

El transmisor de información vía TCP/IP a utilizarse, tal como lo muestra la Figura 3.22, es un T-Link, el cual, utiliza como software base de monitoreo el programa SG-Reporter IP.

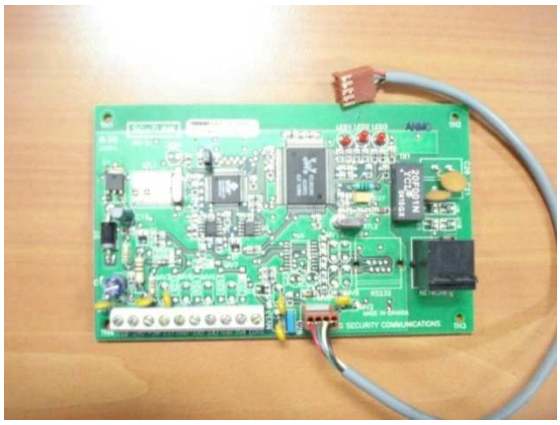


Figura 3.22 *Transmisor T-Link*

3.6.1.5 Dispositivos complementarios

El sensor de movimiento IS2535, los magnéticos adhesivos, los botones de pánico Sentrol 3045, la batería de respaldo y el kit inalámbrico Enkryptor a implementarse, son aquellos detallados anteriormente en el análisis económico del proyecto global, razón por la cual, no es necesario detallar más sobre las características del mismo.

3.6.2 RECONOCIMIENTO VISUAL

Antes de proceder a instalar los dispositivos, se procedió a realizar un reconocimiento previo a la dependencia, única y exclusivamente para mostrar por imágenes su exterior e interior previa la implementación.

3.6.2.1 Paneo exterior

Las imágenes a mostrarse simularan un paneo de la agencia, mismas que iniciaran con la Figura 3.23, mostrando el exterior principal de la dependencia.

Figura 3.23 *Agencia de recaudación Ipiales del Sur*

La Figura 3.24 detalla el ingreso a la instalación, denotando la puerta blindada de acceso.

Figura 3.24 *Acceso a la Agencia Ipiales del Sur*

La Figura 3.25 muestra el exterior de la agencia, específicamente el área superior de las ventanillas, denotando las esquinas superiores del lugar y la vigilancia permanente de esta área por monitoreo CCTV propio del centro comercial.

Figura 3.25 *Ventanillas y CCTV del centro comercial*

Continuando el paneo hacia la izquierda, la Figura 3.26 muestra la pared que recubre el área del baño de la agencia de recaudación. Sobre esta se encuentra el letrero de presentación de la agencia.

Figura 3.26 *Pared lateral izquierda*

Para finalizar el paneo izquierdo, la Figura 3.27 muestra la pared que termina de recubrir el área del baño de empleados de la EMAAP-Q.

Figura 3.27 *Pared exterior al área de baños de la agencia*

Ahora bien, para finalizar el paneo total de la dependencia, se deberán mostrar las imágenes pertinentes al sector colocado al lado derecho de la puerta de ingreso. La Figura 3.28 muestra el mencionado sector, específicamente la caja del área de facturación.

Figura 3.28 *Caja de facturación*

La última imagen del exterior de la dependencia se muestra en la Figura 3.29, misma que denota la pared que conforma el lado derecho de la caja de facturación.

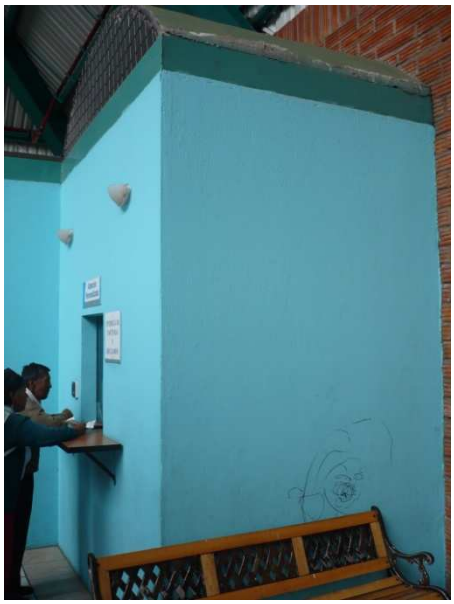


Figura 3.29 *Pared lateral derecha de la dependencia*

3.6.2.2 Paneo interior

Tal como se mostró en el diseño planteado anteriormente, se procedió a reconocer internamente los sectores sobre los cuales se instalarán los equipos, procedimiento el cual, se valió en la Figura 3.30, misma que representa el plano en formato dwg de la dependencia.

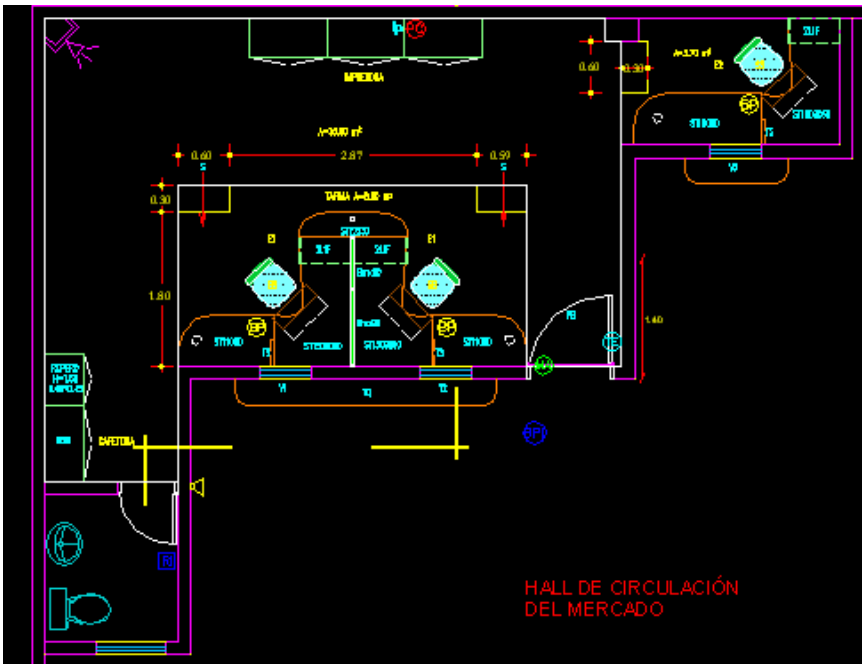


Figura 3.30 *Levantamiento de equipos en plano DWG Ipiales del Sur*

Siendo así, vale recordar uno por uno los lugares elegidos para implementación:

a. Al sensor de movimiento se lo planificó colocar en la esquina superior trasera izquierda de la dependencia, sobre la superficie de la viga metálica de soporte de la instalación, tal como lo muestra la Figura 3.31

Figura 3.31 *Sector de instalación del sensor de movimiento*

b. Al sensor magnético adhesivo se lo planificó colocar en la puerta de acceso al área blindada, tal como lo muestra la Figura 3.32

Figura 3.32 *Área de instalación del magnético adhesivo*

c. Los botones de pánico fueron planificados a ser colocados en la parte inferior de los escritorios de atención al cliente, tanto de recaudación como de facturación, tal como lo muestra la Figura 3.33

Figura 3.33 *Lugar destinado a los botones de pánico*

d. La sirena se planificó colocarla bajo el letrero de la agencia de recaudación, en la pared exterior izquierda de la dependencia, tal como lo muestra la Figura 3.34

Figura 3.34 *Sector predeterminado para la instalación de la sirena*

e. Para finalizar, el panel de control y el módulo de transmisión vía TCP/IP fueron planificados a ser colocados en la parte trasera central del interior de la agencia de recaudación, tal como lo muestra la Figura 3.35

Figura 3.35 *Sector de instalación de la caja del panel*

3.6.3 INSTALACIÓN DE DISPOSITIVOS

La instalación de todos los equipos requeridos por la Agencia Ipiales del Sur fue realizada los días martes 24 y miércoles 25 de marzo del 2009, y contempló el tendido del cableado, posicionamiento de equipo, configuración de dispositivos y puesta en marcha del panel de control.

3.6.3.1 Tendido del cableado

Para proceder a dimensionar la cantidad de cableado necesario para la dependencia, se utilizó parte de un rollo de cable UTP categoría 5e, tendiendo el mismo a través de la superficie de la dependencia y sumando a los extremos necesarios una distancia de 2 metros, planificada tanto para empalmes como para canalización.

Como lo muestra la Figura 3.36, todo el cableado UTP fue canalizado a través de manguera plástica corrugada de media pulgada, la cual pretende proteger la transmisión de información de humedad, calor y manipulación no deseada. Debido a que esta protección solo se contempla para el área interna de la agencia, no se consideró necesaria la utilización de tubería metálica tipo EMT, ya que por ser un sector blindado, solamente puede ingresar personal autorizado de la EMAAP-Q.

Figura 3.36 *Manguera plástica corrugada de media pulgada*

Como ya se tenía conocimiento de la localización de los elementos de seguridad electrónica deseados, se procedió a tender la manguera corrugada a través del techo falso de Ipiales del Sur.

Se planificó utilizar ocho cables UTP, mismos que tendrían que cumplir las siguientes funciones: (según orden en el que se fue tendiendo el cableado)

Primer cable UTP	Botón de pánico área de facturación
Segundo cable UTP	Teclado de armado y desarmado
Tercer cable UTP	Magnético adhesivo de la puerta
Cuarto cable UTP	Botón de pánico área de recaudación uno
Quinto cable UTP	Botón de pánico área de recaudación dos
Sexto cable UTP	Sensor de movimiento
Séptimo cable UTP	Alimentación y activación de sirena. Tamper
Octavo cable UTP	Receptor inalámbrico Enkriptor

En total, se realizaron cuatro tendidos de cableado, que fueron estructurados de la siguiente manera:

3.6.3.1.1 Primer tendido

La primera manguera tendida, tal como lo muestra la Figura 3.37, va a servir específicamente para canalizar el cable UTP del botón de pánico del área de facturación.

Figura 3.37 Primer cable UTP tendido. Botón de pánico área de facturación

Uno de los procedimientos del tendido a seguir, tanto para el primer cable UTP como para los restantes, tal como lo muestra la Figura 3.38, es ir colocando amarras plásticas capaces de templar la manguera corrugada. La idea es obtener una instalación que sea fácil de manejar, ya sea para proveer un mantenimiento futuro preventivo o correctivo del sistema en cuestión.

Figura 3.38 *Uso de amarras plásticas para sujetar la manguera corrugada*

El siguiente paso, mostrado en la Figura 3.39, fue canalizar las mangueras a través de las esquinas de la dependencia, procedimiento el cual tenía como fin recorrer de manera adecuada el perímetro de la agencia de recaudación.

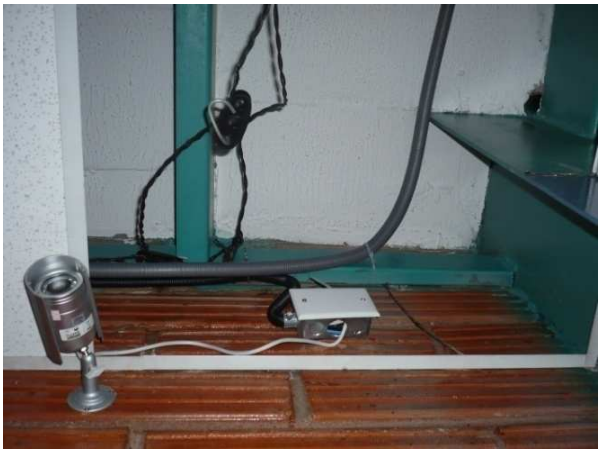


Figura 3.39 *Canalización de la manguera a través de las esquinas de Ipiales del Sur*

A continuación, se procedió a encaminar el cable UTP designado al botón de pánico de facturación por la canaleta plástica usada para la línea telefónica existente de la dependencia, tal como lo muestra la Figura 3.40

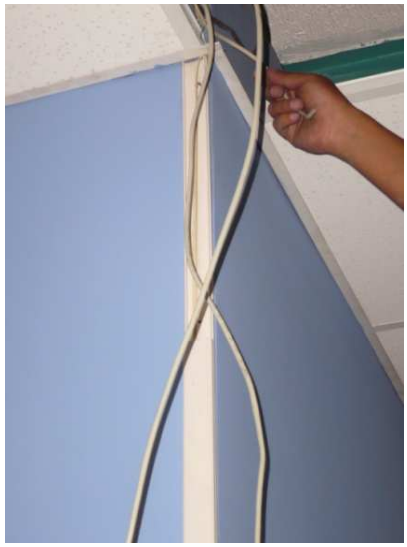


Figura 3.40 *Envió del cable UTP a través de la canaleta de la línea telefónica*

Ya en la parte inferior, se utilizó silicona caliente para encaminar el cable UTP por el filo posterior del mueble de la caja de facturación. Logrando así, dejar listo el cable para la instalación del botón de pánico, tal como lo muestra la Figura 3.41.

Figuras 3.41 *Sujetamiento del cable UTP*

3.6.3.1.2 Segundo Tendido

La Figura 3.42 muestra el inicio del tendido de la segunda manguera corrugada, misma que llevaría consigo el segundo y tercer cable UTP, los cuales, cumplirán la función de transmisión del estado del teclado y el magnético adhesivo de la puerta blindada. Dicho procedimiento fue similar al primer tendido realizado, enviando los UTP dentro de la manguera corrugada sobre el lugar donde se colocará el panel de control.

Figura 3.42 *Tendido de la segunda manguera corrugada*

La razón de que ambos cables atravesaran la misma manguera corrugada, se debió a que los dos deberán bajar conjuntamente por una de las esquinas de la agencia de recaudación, tal como se puede observar en la Figura 3.43.

Figura 3.43 *Bajada de los UTP para teclado y magnético adhesivo*

3.6.3.1.3 Tercer tendido

Sobre la tercera manguera corrugada, tal como se aprecia en la Figura 3.44, se atravesó el cuarto, quinto y sexto UTP, esto debido a que dos de ellos se destinarían a transmitir la información de los botones de pánico a colocarse en las dos cajas de recaudación continuas, y el tercero, a colocar sobre el área de cajas el receptor del sistema inalámbrico de botón de pánico.

Figura 3.44 *Tendido de la tercera manguera corrugada*

Al llegar al área superior de las cajas, se procedió a canalizar los dos cables UTP a través de una canaleta plástica, tal como se muestra en la Figura 3.45; posteriormente, al igual que en la instalación del primer botón de pánico, se sujeto los UTP a la parte posterior inferior de los escritorios con silicona caliente.

Figura 3.45 *Bajada de la manguera corrugada con los dos cables UTP para los dos botones de pánico para de las cajas*

3.6.3.1.4 Cuarto tendido

A través de la cuarta manguera, Figura 3.46, se atravesó el séptimo y el octavo cable UTP, teniendo como fin la transmisión de información proveniente del sensor de movimiento y la sirena.

Figura 3.46 *Inicio del cuarto tendido*

Debido a que la sirena se encontrará en un lugar totalmente aparte del sensor de movimiento, se tuvo que separar los cables utilizando un pequeño cajetín metálico, mismo que se muestra en la Figura 3.47

Figura 3.47 *Cajetín metálico*

La instalación de este cajetín, como se observa en la Figura 3.48, consistió en ingresar la cuarta manguera corrugada, y a su vez, separar de ésta dos mangueras más, una para la sirena y una que encamine el pequeño trayecto hacia el sensor PIR.

Figura 3.48 *Separación de las mangueras corrugadas a través del cajetín metálico*

A continuación, frente a la viga de la esquina, se sacó el sexto cable UTP para la conexión del sensor de movimiento, esto se muestra en la Figura 3.49.

Figura 3.49 *Cable UTP para conexión del PIR*

Después de esto, se continuó el cuarto tendido a través del techo falso de la dependencia para llegar al lugar de instalación de la sirena, mostrándose dicha actividad en la Figura 3.50.

Figura 3.50 *Tendido del cableado de la sirena a través del techo falso*

Debido a que la sirena será situada en el exterior de la dependencia, se debía llegar al baño de la instalación, atravesar la pared con un taladro y sacar de ahí el cable UTP, procedimiento mostrado secuencialmente en las Figuras 3.51 y 3.52.

Figura 3.51 *Tendido del cableado en el techo del baño*

Figura 3.52 *Salida del cable UTP bajo el letrero de la agencia de recaudación*

3.6.3.2 Posicionamiento de Equipo

Ya finalizado todo el tendido para la alimentación y transmisión de datos de los dispositivos, se procedió a la instalación de cada uno de los dispositivos de seguridad electrónica.

Cabe señalar, que para precautelar y asegurar la correcta transmisión de información proveniente de todos los dispositivos, se utilizará uno de los pares de cable UTP para simular una sola vía, es decir, cada pareja formará un solo cable. De esta forma, se asegura que si uno de los cables por individual fallara, el otro le serviría como respaldo.

La secuencia a seguir, en cuanto a instalación de los mismos, fue realizada secuencialmente según la forma en que se tendió el cableado UTP.

3.6.3.2.1 Instalación de Botones de Pánico

Los primeros dispositivos en instalarse fueron los botones de pánico, tanto de la caja de facturación como de las dos cajas de recaudación.

Se inició específicamente por la caja de recaudación, ya que fue ésta la que conformó el primer tendido de cableado.

Para esto, se tomó el botón tipo palanca, mostrado en la Figura 3.53, se lo destapó y se procedió a conectar el cable UTP a sus dos terminales, procedimiento expuesto en la Figura 3.54.

Figura 3.53 *Pánico tipo palanca*

Figura 3.54 *Pines de conexión*

A continuación se sujetó el botón de pánico en la parte inferior del escritorio mediante el uso de dos tornillos, precautelando que la posición del mismo sea cómoda para la activación de la palanca en caso de ser necesario. Dispositivo instalado mostrado en la Figura 3.55.

Figura 3.55 *Botón de pánico instalado*

Seguido, se repitió el mismo procedimiento para las dos cajas de recaudación, mostrando uno de estos resultados en la Figura 3.56.

Figura 3.56 *Botón de pánico – Caja de recaudación*

3.6.3.2.2 Instalación del teclado de control

El segundo dispositivo a instalarse fue el teclado de control. El procedimiento seguido para cumplir este fin, mostrado en la Figura 3.57, fue la colocación de una canaleta plástica adhesiva para la canalización de los UTP destinados al teclado de control y al magnético adhesivo.

Figura 3.57 *Teclado instalado.*

3.6.3.2.3 Instalación del magnético adhesivo

El magnético adhesivo fue el tercer dispositivo instalado. Parte de este procedimiento ya fue expuesto en el literal anterior, pero para complementarlo, se debe comentar la instalación de una canaleta plástica para canalizar individualmente el cableado del magnético adhesivo a través del marco superior de la puerta de acceso a la dependencia, procedimiento mostrado en la Figura 3.58

Figura 3.58 *Colocación de la canaleta plástica sobre el marco de la puerta*

A continuación, se preparó el magnético adhesivo, pegando una de las dos partes que lo conforman en el marco de la puerta, y el restante en la puerta en sí. Dicho procedimiento está expuesto en la Figura 3.59.

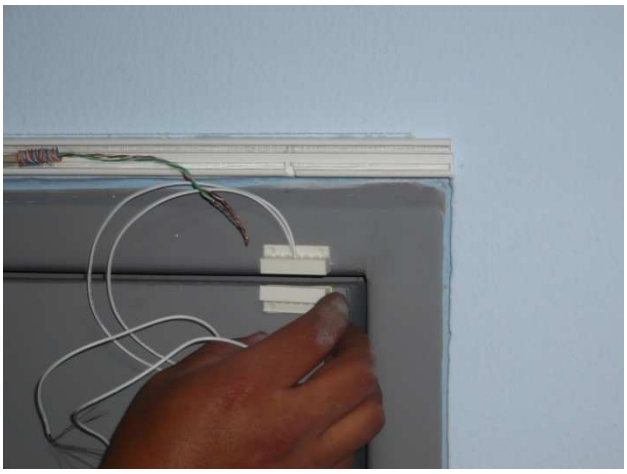


Figura 3.59 *Instalación del magnético adhesivo*

La Figura 3.60 muestra ya finalizada la instalación del teclado y el magnético adhesivo, denotando la colocación de las dos canaletas plásticas en sus respectivas posiciones.

Figura 3.60 *Finalización de instalación*

3.6.3.2.4 Instalación del sensor de movimiento PIR

Continuando con la implementación de los dispositivos, se procedió a instalar el sensor de movimiento en su lugar predeterminado. Para esto, al igual que al botón de pánico, se destapó el dispositivo, y se conectó al mismo cuatro pares de cable UTP. Dos de ellos brindarían la alimentación de 12 V necesaria, y los otros dos, la transmisión de información requerida para el monitoreo.

Para la sujeción del sensor se utilizó silicona caliente, asegurándose de esparcirla sobre toda su superficie para que no cause problemas posteriormente al desprenderse el sensor. La Figura 3.61 muestra como quedó el dispositivo tras su instalación.

Figura 3.61 *Sensor de movimiento instalado*

3.6.3.2.5 Instalación de la sirena

El quinto dispositivo instalado fue la sirena del sistema de seguridad electrónica. El procedimiento inició con la respectiva perforación de un agujero en la pared lateral izquierda de la dependencia, sobre el cual se pasaría el respectivo cable para alimentación de la sirena y transmisión de señal por parte del tamper.

A continuación, se sujetó la caja de la sirena a la pared con sus respectivos tornillos, asegurando la misma y conectando el sensor tamper. La Figura 3.62 muestra la forma en que quedó la mencionada implementación.

Figura 3.62 *Sirena instalada*

3.6.3.2.6 Instalación del receptor inalámbrico Enkriptor

A continuación de la instalación de la sirena, se procedió a colocar el receptor inalámbrico Enkriptor en una posición cómoda para la recepción de la señal del botón de pánico inalámbrico.

Figura 3.63 *Enkriptor instalado.*

Este receptor fue colocado en la parte superior a las cajas de recaudación uno y dos, frente a la pared principal que conforma la agencia de recaudación.

3.6.3.2.7 Instalación del panel de control y módulo T-Link

Por último, y no menos importante, se procedió a la instalación del panel de control DSC PC 5020 y el módulo para transmisión de datos vía TCP/IP T-Link.

Lo primero en realizarse, es un esquema gráfico del lugar donde se va a instalar todo el sistema. En este diagrama deben constar todos los dispositivos que se vayan a utilizar en este caso en la agencia de recaudación Ipiales del Sur. Como se observó previamente se tiene un plano de la agencia donde se encuentran ubicados los equipos que se van a utilizar.

Como siguiente paso, se debe asegurar el panel de control a la caja metálica, tal como lo muestra la Figura 3.64. La caja metálica junto con la central deben ser colocados en un lugar seco, cerca de un toma corriente y de una línea telefónica en el caso de que la transmisión de datos se la realice por medio de la línea de teléfono o cerca de un punto de red en el caso que se realice por vía TCP/IP como es nuestro caso.

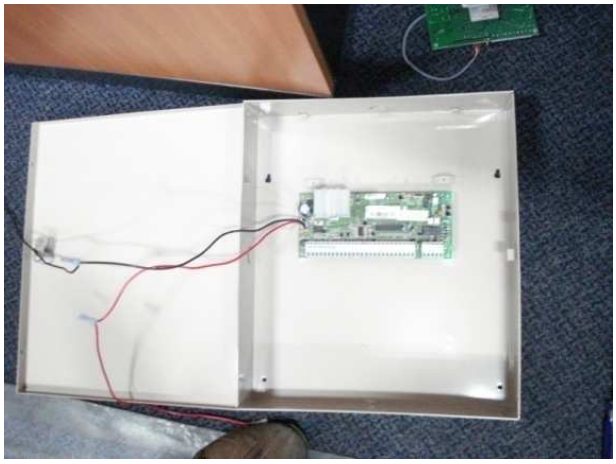


Figura 3.64 *Sujeción de tarjetas electrónicas*

La ubicación del panel de control, como se encuentra detallado anteriormente en el plano, está en el lugar donde el Departamento de Recursos Informáticos de la EMAAP-Q tiene instalados sus equipos de redes para la transmisión de sus datos, es por esta razón que el panel de seguridad se lo colocó cerca de

esta ubicación para tener cerca un punto de red y un toma corriente que es la alimentación necesaria para los mismos.

A continuación, se procedió a instalar el gabinete metálico en la pared posterior de la dependencia, procedimiento expuesto en la Figura 3.65

Figura 3.65 *Instalación del gabinete metálico*

3.6.3.3 Acoplamiento de los dispositivos electrónicos al panel de control

Al panel de control ya instalado se le deben acoplar el resto de dispositivos implementados. Antes de proseguir, es necesario mostrar en la Figura 3.66 el diagrama de conexiones del panel PC5020, esto, con el fin de visualizar los pines sobre los cuales se deberá realizar las respectivas conexiones, tanto de dispositivos sensores, así como, batería, sirena, T-Link, etc.

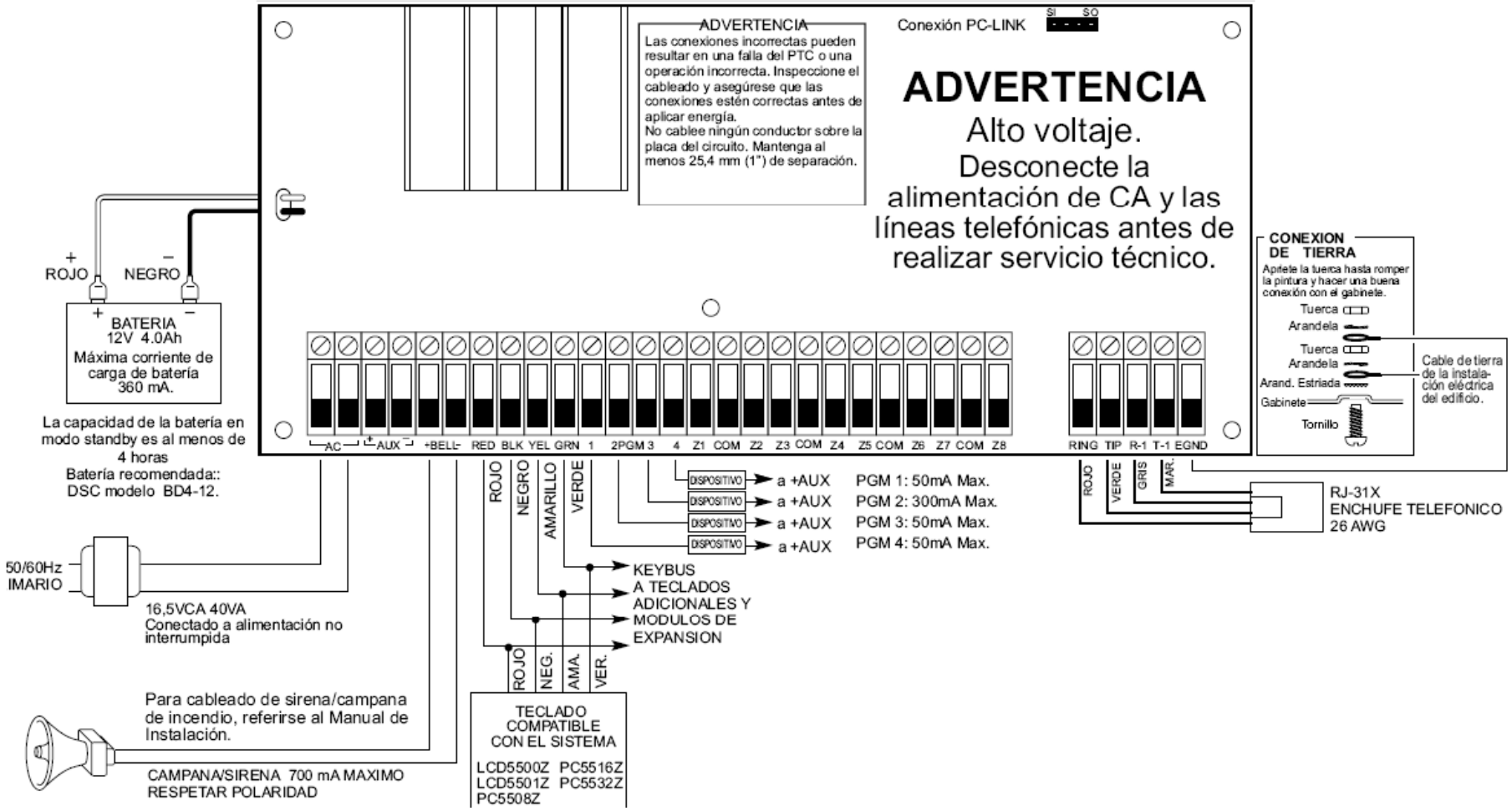


Figura 3.66 *Diagrama de conexionado*

DSC PC5020

Lo primero a realizarse, después de la respectiva instalación del equipo físico, es la conexión del Keybus del sistema, mostrado en la Figura 3.67. El Keybus es usado por el control para comunicarse con todos los módulos conectados y para que los módulos se comuniquen con el control. Las terminales Roja y Negra (RED, BLK) son usadas para proporcionar energía mientras que las terminales Amarilla y Verde (YEL, GRN) son para el reloj y datos.

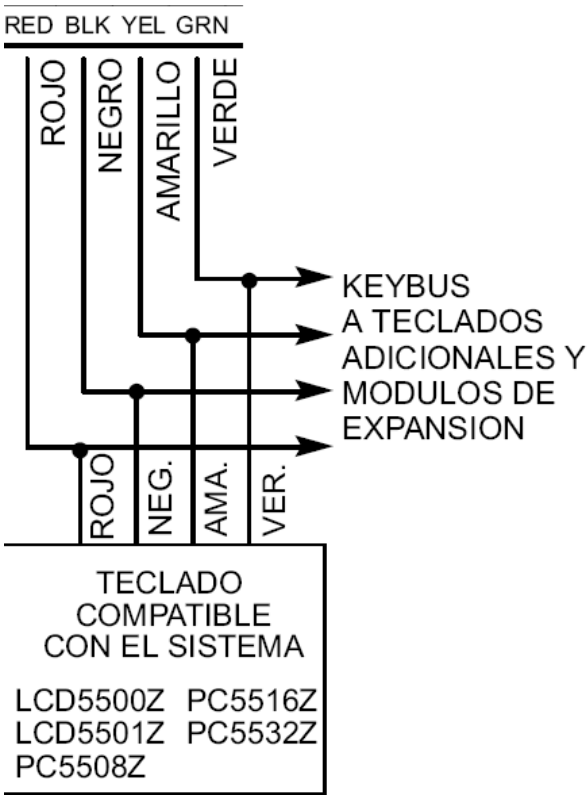


Figura 3.67 *Keybus del sistema*

En este sistema, los únicos módulos que necesitan la conexión del Keybus son el teclado y el T-Link, razón por la cual, se inicia con un pequeño resumen de este procedimiento.

3.6.3.3.1 Conexión del teclado

Como especificación de conexión propia del panel, se detalla que los módulos a conectarse sobre el Keybus pueden ser corridos al control, conectados en series, o pueden ser derivados T.

La conexión debe ser directa de cada uno de los cables entre el panel y el modulo, es decir, las 4 terminales Keybus del control deben ser conectadas a las 4 terminales o cables de Keybus en el teclado.

3.6.3.3.2 Conexión del T-Link

El T-Link debe acoplarse con el panel de control a través del Keybus y la entrada PC-LINK del PC5020, mostrado en la Figura 3.68.

Figura 3.68 *Conexión del módulo de comunicación IP*

El módulo PC-LINK permite la descarga de información, la cual, conlleva a la programación de todo el control vía una computadora o modem. Gracias a esto es que todas las funciones y características, cambios y estados, tales como condiciones de falla y zonas abiertas pueden ser vistas o programadas por la descarga de información.

3.6.3.3.3 Conexión de dispositivos sensores de monitoreo

Continuando con el procedimiento de conexiones, los segundos dispositivos a acoplarse al panel de control deberán ser los sensores que abarcarán las zonas de monitoreo. Antes de conectar los terminales de cada uno de estos, es necesario especificar dos cosas:

- Cual zona del panel corresponderá a los mismos y,
- Como acoplar los mismos al panel de control

Siendo así, y solucionando dichas inquietudes en su respectivo orden, se inicia determinando que zona debe ocupar cada sensor.

Para Ipiales del Sur

Zona 1	Magnético adhesivo de la puerta
Zona 2	Sensor de movimiento
Zona 3	Botón de pánico área de recaudación uno
Zona 4	Botón de pánico área de recaudación dos
Zona 5	Botón de pánico área de facturación
Zona 6	Botón de pánico inalámbrico
Zona 7	Sensor Tamper
Zona 8	Libre

Viendo un poco más de cerca, y concentrándonos en las 8 zonas de monitoreo, se puede ampliar el diagrama de conexiones con la imagen representada en la Figura 3.69.

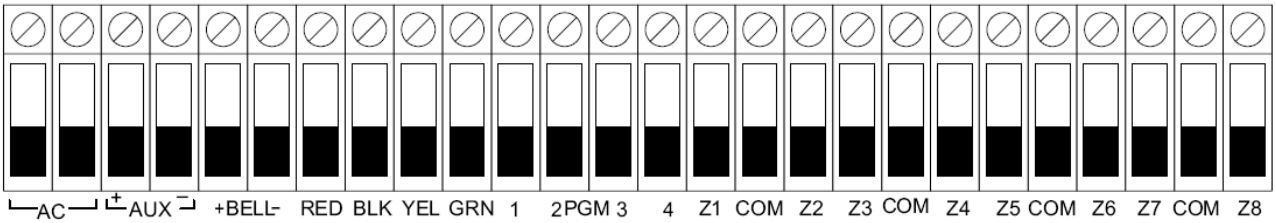


Figura 3.69 *Terminales de conexión*

Ya definido que dispositivo de monitoreo ocupará cada zona, se debe determinar cómo acoplar el mismo a la tarjeta electrónica. Para esto, se debe introducir el criterio si los sensores trabajaran como NO o NC (normalmente abierto o normalmente cerrado).

Los contactos normalmente abiertos conectan el circuito cuando el relé es activado; el circuito se desconecta cuando el relé está inactivo. Este tipo de contactos son ideales para aplicaciones en las que se requiere conmutar fuentes de poder para dispositivos remotos.

Los contactos normalmente cerrados desconectan el circuito cuando el relé es activado; el circuito se conecta cuando el relé está inactivo. Estos contactos

se utilizan para aplicaciones en las que se requiere que el circuito permanezca cerrado hasta que el relé sea activado.

Hay diferentes maneras en las cuales las zonas pueden ser conectadas, dependiendo de las opciones de programación que han sido seleccionadas. El control puede ser programado para supervisar circuitos normalmente cerrados, al final de la línea (EOL), o dobles al final de la línea (DEOL):

a) Resistores Singulares al Final de la Línea (EOL)

Se utiliza cuando los dispositivos de detección o contactos ya sea Normalmente Cerrados (NC) o Normalmente Abiertos (NO) están siendo usados.

b) Resistores Dobles (DEOL) al Final de la Línea

Los resistores dobles al final de la línea permiten al control determinar si la zona está en alarma, saboteada o con falla.

Ya sea utilizando el método EOL o DEOL, ambas deben ser activadas vía programación sobre el panel de control. En este caso, y para las funciones del sistema, se utilizará el método EOL, mostrado en diagrama de conexión en la Figura 3.70

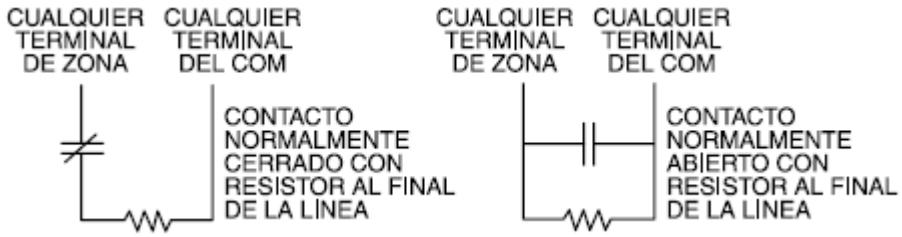


Figura 3.70 *Conexión con resistencia según NC o NO*

La función de la resistencia es, en circuito normalmente cerrado, crear una diferencia de voltaje que en el caso de abrirse el contacto se vuelve cero y, en un circuito normalmente abierto, al cerrarse, mostrar un voltaje cero debido a su implementación en paralelo al contacto.

A continuación se muestra un cuadro capaz de detallar la forma en que trabajan cada uno de los dispositivos contemplados en este proyecto

DISPOSITIVO DE MONITOREO	**NORMAL FUNCIONAMIENTO**
Tamper	NC
Sensor de movimiento	NC
Botón de pánico	NC
Dispositivo inalámbrico de activación	NO
Magnético Adhesivo	NC

Ya con el conocimiento de la forma en que trabajarán los dispositivos de monitoreo, se puede proseguir a la conexión de los mismos, utilizando para ello, resistencias de 5.6 KΩ recomendadas por el fabricante del panel.

3.6.3.3.4 Cableado de dispositivos secundarios

Después de conectar los dispositivos de monitoreo a la central de alarma PC5020, se debe proseguir con esta actividad pero aplicando la misma a equipos como sirenas, baterías de respaldo, módulos de comunicación, etc., es decir, el cableado de los dispositivos secundarios.

Para esto es necesario recordar el diagrama del equipo y reducirlo en las Figuras 3.71 y 3.72, que denoten los terminales del panel de control para la conexión de la sirena/ transformador y la batería de respaldo.

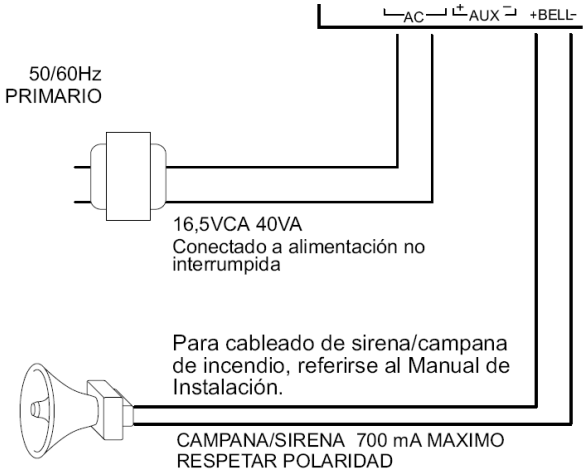


Figura 3.71 *Conexión de la sirena y el transformador*

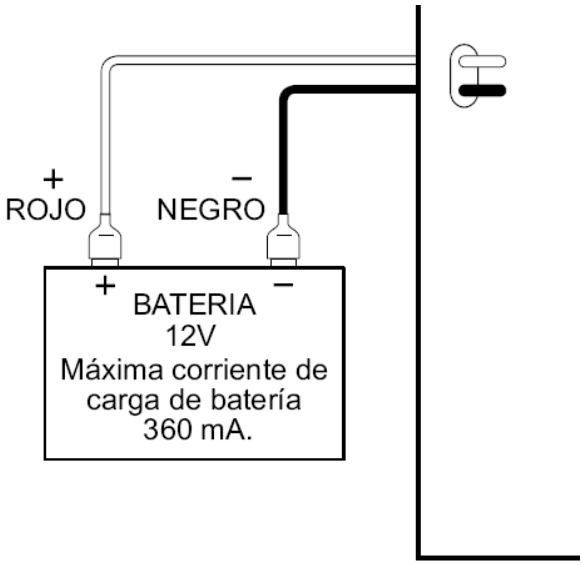


Figura 3.72 *Conexión de la batería de respaldo*

3.6.4 CONFIGURACIÓN DEL PANEL DE CONTROL

Finalizada toda la instalación de dispositivos, se debe proceder al encendido del panel de control para iniciar la configuración de cada uno de los equipos interconectados.

3.6.4.1 Asignación del teclado

Se tiene la capacidad de asignar hasta 8 teclados en el panel de control, en este caso, solamente se utiliza uno, el modelo PK5500. Los teclados deben ser asignados al sistema para ser supervisados propiamente.

El panel de control tiene pre asignado uno de los ocho espacios para los modelos de teclado, según esto, se confirmó que el 5511 tiene la asignación del espacio 1 de la PC5020.

3.6.4.2 Supervisión de los Módulos

En el momento de la instalación y programación del sistema se puede saber si todos los dispositivos están bien conectados o si el sistema está reconociendo todos los dispositivos conectados al panel de control. La supervisión está habilitada todo el tiempo para que el control pueda indicar una falla si un módulo es removido o no del sistema. Para chequear cuales módulos están actualmente conectados y supervisados se debe seguir el siguiente procedimiento

1. Presionar [*] [8] [Código del Instalador] para entrar a la Programación del Instalador.
2. Presionar [903] para mostrar todos los módulos.
3. El teclado LCD permitirá recorrer a través de los módulos

3.6.4.3 Programación básica

La programación básica del equipo se refiere a la configuración de las zonas a utilizarse en el panel de control. Previo a detallar este procedimiento, se resumirá los tipos de zonas más importantes que pueden ser configurados en un sistema de alarmas monitoreadas, tomando como referencia la Figura 3.69, obtenida de las “Hojas de Programación - panel DSC PC5020, sección 3: Programación básica, Definiciones de zonas, página 5.

00 Zona Nula (No Usada)	10 Zumbador Supervisor 24 Horas	20 Congelador 24 Horas
01 Demora 1	11 Robo 24 Horas	21 Sabotaje de 24 Horas Enganchado
02 Demora 2	12 Atraco 24 Horas	22 Armar por Interruptor de Llave Momentáneo
03 Instantánea	13 Gas 24 Horas	23 Armar por Interruptor de Llave Sostenido
04 Interior	14 Calefacción 24 Horas	24 Respuesta del LINKS
05 Interior, Presente / Ausente	15 Médica 24 Horas	25 Demora Interior
06 Demora, Presente / Ausente	16 Pánico 24 Horas	26 24 Horas Ninguna Alarma
07 Incendio de 24 Horas, Demorada (Cableado)	17 Emergencia 24 Horas	87 Incendio de 24 Horas con Demora (Inalámbrico)
08 Incendio de 24 Horas, Normal (Cableado)	18 Regadera 24 Horas	88 Incendio de 24 Horas, Normal (Inalámbrico)
09 Supervisor 24 Horas	19 Agua 24 Horas	

Figura 3.73 *Definiciones de zonas*

a) **Zona nula**

Este tipo de zona simplemente representa la zona que no se utilizará, o en otras palabras, no estará en funcionamiento debido a que no habrá ningún dispositivo acoplado a la misma.

b) **Zona de Demora 1**

Esta definición de zona aplica a las entradas monitoreadas de una instalación, en las cuales, deben permitir y dotar al usuario un tiempo predeterminado para desactivar el sistema, y evitar así, que se transmita una señal de emergencia al ser traspasadas.

Además, cabe señalar que el teclado emite un pitido que alerta al usuario que debe desactivar la alarma en cuestión, dándole como predefinido, un tiempo de 30 seg.

c) **Zona de Demora 2**

Trabaje de la misma forma que la Zona de demora 1, con la única diferencia que da un tiempo predefinido en su sistema de 45 seg.

d) **Zona Instantánea**

Como su nombre lo dice, si la zona es violentada, inmediatamente se transmite la señal de emergencia. Comúnmente utilizada para monitoreo de ventanas.

e) **Zona Interior**

La mejor forma de explicar el funcionamiento de este tipo de zona es con un ejemplo práctico. Esta se utiliza comúnmente en sensores de movimiento que deben activarse inmediatamente en caso de detectar un intruso ***sin la activación de una zona previa***, es decir, si el usuario abre su puerta de entrada se activará la zona de demora, si la zona de demora es activada el sensor de movimiento deberá esperar el mismo tiempo de espera programado para generar alarma. Si al contrario, si secuencialmente, antes de activarse el sensor de movimiento no existió alarma de zona de demora, deberá generarse la señal de emergencia.

f) **Zona de Incendio de 24 Horas con Demora**

Al violentarse la zona ocurren dos cosas claves: Primero, la salida de alarma se activa inmediatamente y, segundo, el comunicador demorará 30 segundos en transmitir la emergencia con el fin de confirmar si se pudo o no contener la situación. Si durante estos 30 segundos el usuario presiona cualquier botón del teclado, la salida de alarma y el comunicador serán demorados por 90 segundos adicionales.

Tras la demora de 90 segundos, si la zona sigue violentada, se repite el proceso detallado anteriormente, la salida se alarma se activa y se espera 30 segundos para transmitir la emergencia.

Esta zona comúnmente es utilizada para dispositivos detectores de humo que enganchan.

g) **Zona de Incendio Normal de 24 Horas**

A diferencia de la Zona de Incendio de 24 horas con demora, el comunicador transmite inmediatamente la emergencia suscitada. Esta zona es utilizada para dispositivos como estaciones manuales de incendio.

h) **Zona Supervisada de 24 Horas**

Ya sea que el sistema se encuentre armado o desarmado, si esta zona es violentada, el control reporta inmediatamente a la estación de monitoreo la emergencia. Esta zona se caracteriza porque proporciona una alarma silenciosa predefinida. Se lo utiliza comúnmente para dispositivos como botones de pánico.

i) **Zona de 24 Horas Supervisada por Zumbador**

Cuando este tipo de zona es violentada, ya sea que el control esté armado o desarmado, inmediatamente se engancha el encendido del zumbador del teclado. Esta alerta se mantiene hasta que se ingrese un código de acceso válido para desactivar la novedad, comunicándose de igual forma, a la estación central de monitoreo.

j) **Zona de 24 Horas Contra Robo**

Ya sea que el sistema se encuentre armado o desarmado, si esta zona es violentada, el control reporta inmediatamente a la estación de monitoreo la emergencia y activa la salida de alarma del panel de control.

Las siguientes definiciones de zona trabajan de igual forma que la Zona de 24 Horas Contra Robo, con las excepciones del tipo de salida del Evento del Sistema y algunos atributos propios de zona:

- Zona de 24 Horas Contra Atraco
- Zona de 24 Horas de Gas
- Zona de 24 Horas de Calefacción
- Zona Médica de 24 Horas
- Zona de Pánico de 24 Horas
- Zona de Emergencia de 24 Horas
- Zona de 24 Horas de la Regadera

- Zona de 24 Horas de Corriente de Agua
- Zona de 24 Horas del Congelador

Los pasos seguidos para realizar la programación de cada una de estas zonas en este proyecto fue:

1. Presionar [*] [8] [Código del Instalador] para entrar a la Programación del Instalador.
2. Presionar [001] para la programación de la sección 1 de zonas. (Existen cuatro secciones de zonas, cada una de ellas abarcan 16 zonas. Físicamente solo se tiene ocho zonas ya que no hay expansores, por tal razón y debido a que son secuenciales se programó en la sección 1)
3. Se digita la zona a trabajar. Ejemplo: [01]
4. Se ingresa a la definición de zona deseada. Ejemplo [01] (zona de demora 1)

3.6.4.4 Configuración del Módulo T-LINK

Antes de empezar a configurar el módulo T-LINK, se comienza igualando la hora y la fecha del equipo para sincronizar los equipos con los eventos que se produzcan, esto se lo realiza directamente en el teclado de cada agencia, los pasos son los siguientes:

1. Se procede en el teclado a presionar [*] [6] [1234]
2. Se presiona la tecla [1]
3. Por último, se procede a insertar la hora, los minutos, el día, el mes y el año.

Siguiendo con el proceso de la configuración del módulo de comunicación vía TCP/IP, se trabaja con el teclado donde se realiza los siguientes pasos:

1. Se ingresa a la configuración en el teclado del panel de control presionando [*] [8] [5555].

2. Como siguiente paso se ingresa en el campo de configuración del módulo T-LINK presionando [851].
3. Dentro de este campo se ingresa el campo [001] en el teclado que es el módulo IP, y es donde se procede a colocar la dirección IP que le corresponde al equipo.
4. Luego se ingresa en el campo [002] presionando las teclas, esta es la mascara de red, a continuación de esto se ingresa la máscara correspondiente que se vaya a usar.
5. Seguido de esto se pulsa en el teclado el campo [003] que es el receptor IP, a continuación de esto se procede a ingresar la dirección IP en donde se recibirán los datos, es decir en la estación central de monitoreo.
6. Como paso siguiente al procedimiento se presiona en el teclado el campo [004] que es la entrada del T-LINK es decir el “Gateway” y a continuación se pulsa el IP solicitado.
7. Para ingresar en el campo número de puerto de la fuente del T-LINK se pulsa en el teclado [007], el número que viene establecido de fábrica como el puerto es el [3060].
8. Para finalizar, se ingresa en el campo número de puerto de destino del T-LINK presionando en el teclado [008], en este el número de puerto que viene establecido por el fabricante es el [3061].

3.7 INSTALACIÓN DEL SOFTWARE

En este caso para realizar un control efectivo de las agencias de recaudación lo que se necesita es tener un software de monitoreo y otro para la configuración remota del sistema de alarma y de los dispositivos a instalarse, esto ayudará a que siempre se esté vigilando los equipos de alarma instalados y además que se pueda, mientras tanto, realizar la configuración de los dispositivos. Estas configuraciones remotas consisten en activar o desactivar el sistema de una agencia o sólo de un dispositivo, dar horarios de activación de un sistema o dispositivo, dar acceso al personal a las agencias, etc. Teniendo en cuenta que mientras se realizan todas las configuraciones

necesarias el sistema de alarmas sigue funcionando y sigue siendo monitoreado por el otro software; a pesar de que el software de monitoreo indica el estado en el que se encuentra la comunicación entre las Agencias y el Edificio Matriz el software de configuración es el que asegura esta conexión debido a que por medio de este software se da instrucciones ya sea al sistema o a los dispositivos.

3.7.1 SOFTWARE DE MONITOREO DE ALARMAS

Para realizar un control de las agencias de recaudación, es decir de los dispositivos de alarma que se van a instalar, es necesario contar con un software de monitoreo que permita visualizar las acciones que ocurren con cada uno de los dispositivos instalados y en general con el sistema de alarma instalado en cada agencia, de esta forma se podrá coordinar las acciones pertinentes si fuera el caso.

En esta aplicación se usará el software “THE REPORTER IP”, el cual cumple con las siguientes características:

- Se puede dar prioridad a cierto tipo de alarmas y hacer que aparezcan de otro color en el monitor para que sean atendidas inmediatamente y para que el monitor del sistema se alarme al tener un contraste en los colores.
- Da las facilidades al usuario encargado del sistema para editar, añadir o remover los registros de las alarmas de la base de datos.
- Genera historiales de los eventos ocurridos.
- En el caso de que se produzca un evento o una alarma se generan ayudas visuales y auditivas para facilitar la alerta al monitor del sistema.
- Todos los eventos y alarmas generan la fecha y la hora en la que ocurrieron.

Además de cumplir con las características antes mencionadas, se necesitan ciertas especificaciones mínimas en el computador para que el software funcione correctamente, estas son:

- Sistema operativo Windows 9X/NT
- Computador multimedia Pentium 166MHz
- 32 MB RAM
- 800x600 pixels, Tarjeta de video 16 bit de color
- Monitor SVGA
- Mouse
- Tarjeta de sonido para el computador compatible con Windows.
- Teclado

En este caso los pasos que se seguirán para la instalación de este software son los siguientes:

- Insertar el CD de instalación.
- Ingresar al CD de instalación y se da doble clic en el ícono de instalación. (Figura 3.74)

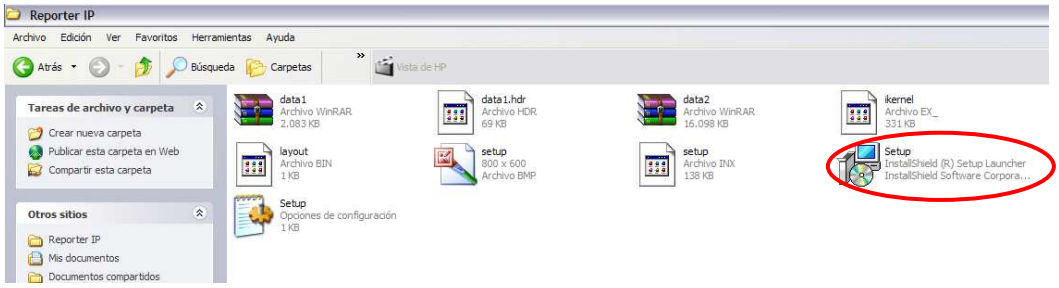


Figura 3.74 *Ventana del ícono de instalación*

- Aparece la pantalla mostrada en la Figura 3.75 que se presenta a continuación

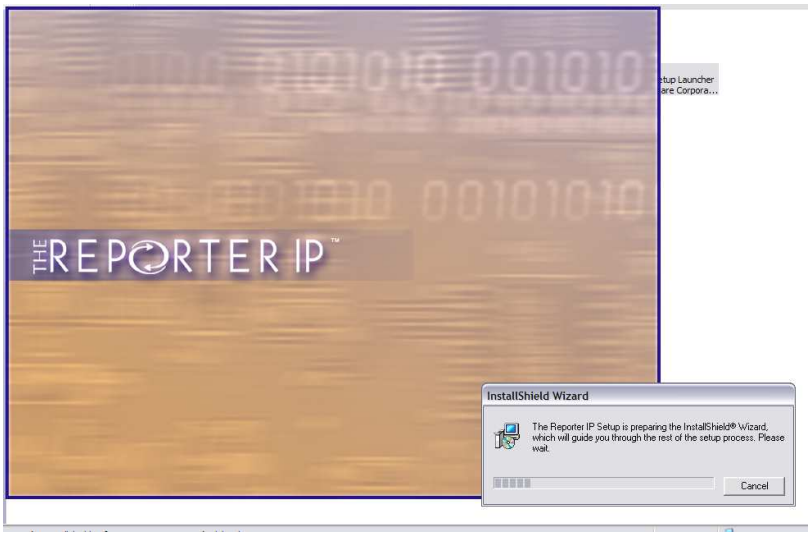


Figura 3.75 *Ventana de instalación*

- Luego de esto se sigue las instrucciones que aparecen en las siguientes pantallas que a continuación se presentan:

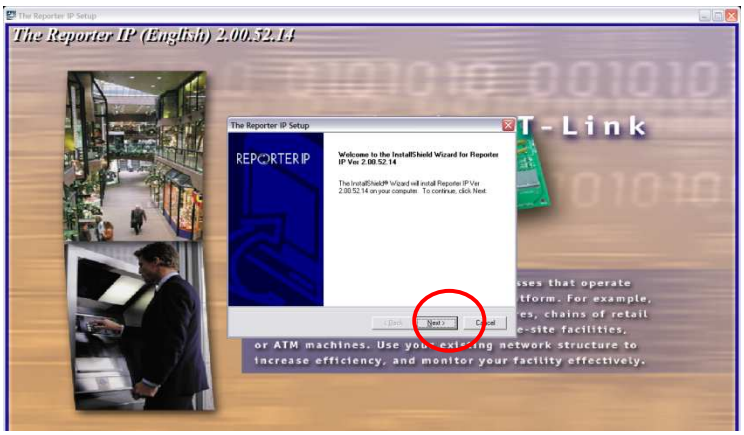


Figura 3.76 *Ventana de instalación*

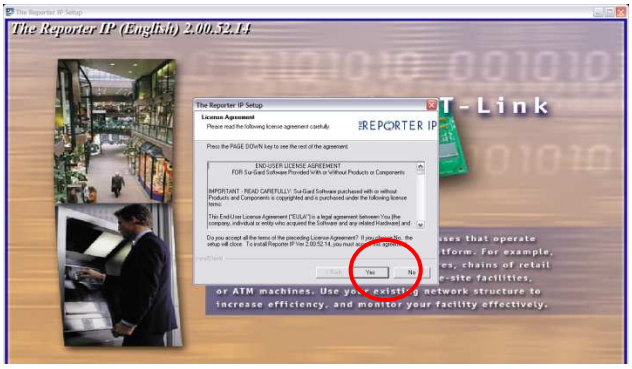


Figura 3.77 *Ventana de instalación*

- Se llena los datos requeridos por el programa y se sigue dando clic en los pasos indicados.

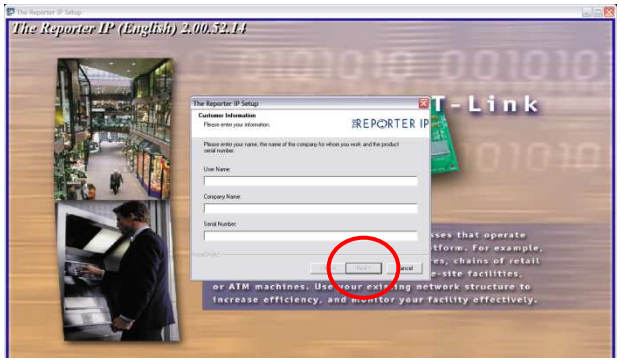


Figura 3.78 *Ventana de instalación*

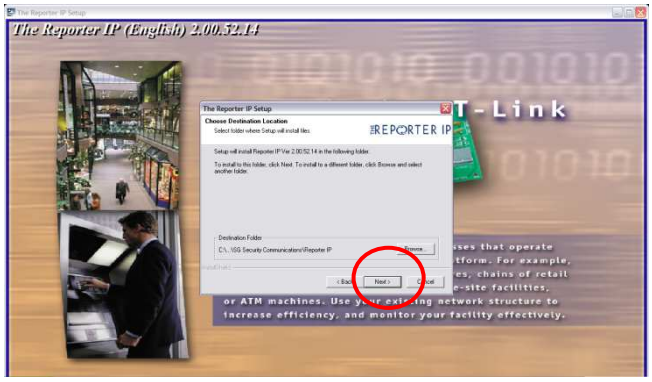


Figura 3.79 *Ventana de instalación*

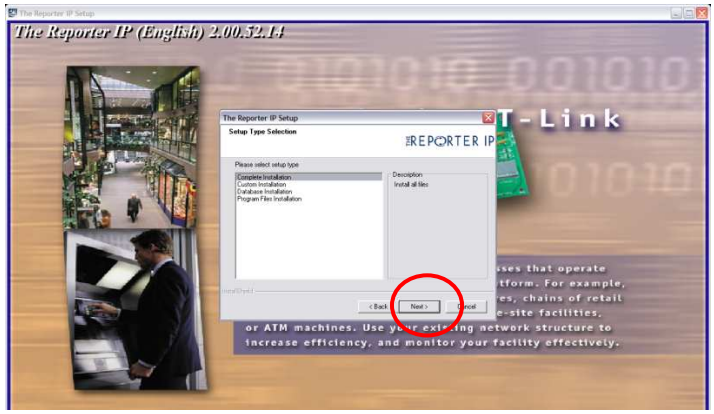


Figura 3.80 *Ventana de instalación*

- Se continúa con la instalación del programa hasta que se cargue y aparezca la última ventana y muestre el mensaje de *"Finish"*.

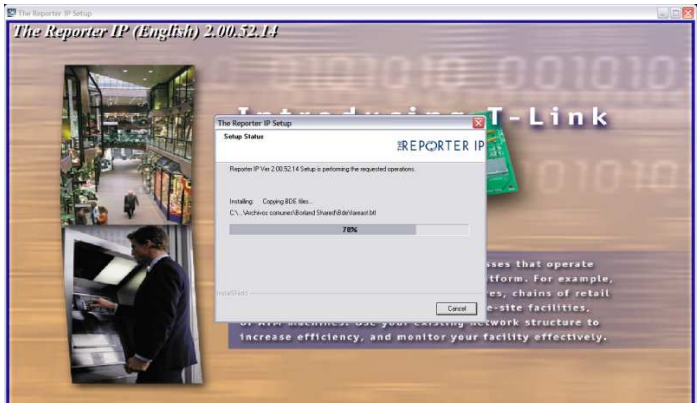


Figura 3.81 *Ventana de instalación*

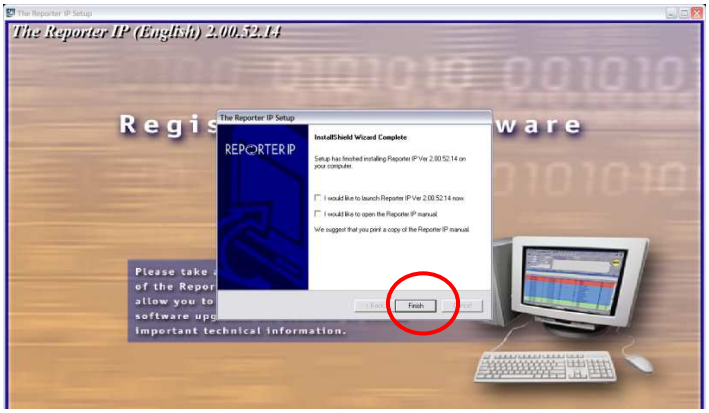


Figura 3.82 *Ventana de instalación*

Realizando esta última acción se tiene listo el software de monitoreo para la aplicación requerida.

3.7.1.1 Ejecución y Configuración del Software

El primer paso necesario para trabajar sobre el software de monitoreo es ejecutarlo, para esto, se procede a dar doble clic en el ícono mostrado en la Figura 3.83, el cual es, ejecución del programa a través del icono del Reporter sobre el escritorio de Windows.

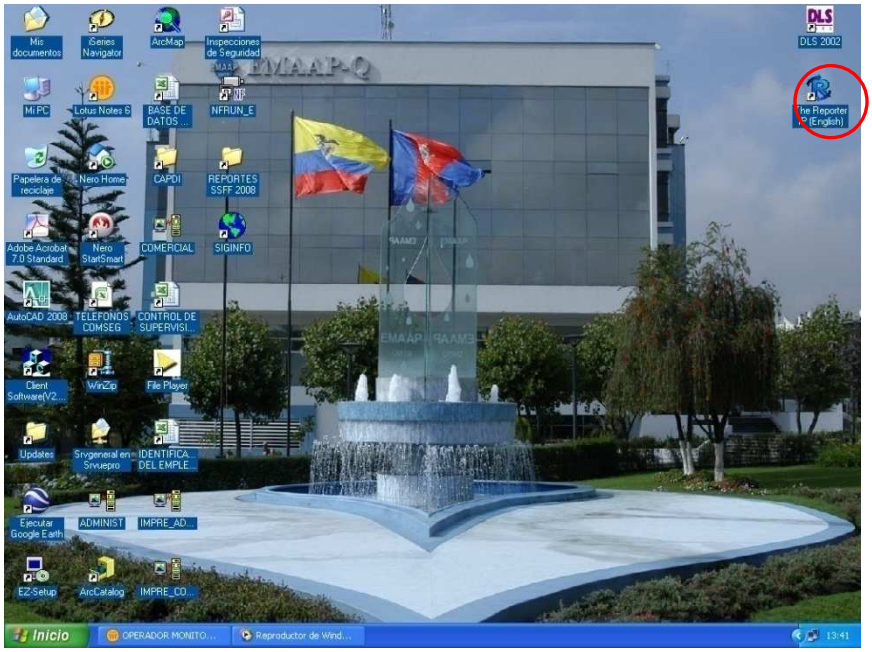


Figura 3.83 *Ejecución del software Reporter*

Cuando se ingresa por primera vez a este programa pide una palabra clave para el ingreso en “inicio de sesión” (Login) y una palabra clave para la “contraseña” (Password); en este caso por ser la primera vez, las palabras claves que se necesitan poner en la ventana que se muestra en la Figura 3.84 a continuación serán:

Login: supervisor, **Password:** password

Figura 3.84 *Ingreso de usuario y clave.*

Un supervisor solo puede añadir, editar o borrar usuarios y administradores, como es la primera vez que se ingresa en esta programa, se le pedirá al

supervisor en ese momento que ingrese una nueva contraseña para el supervisor y que la confirme como se muestra en la Figura 3.85.

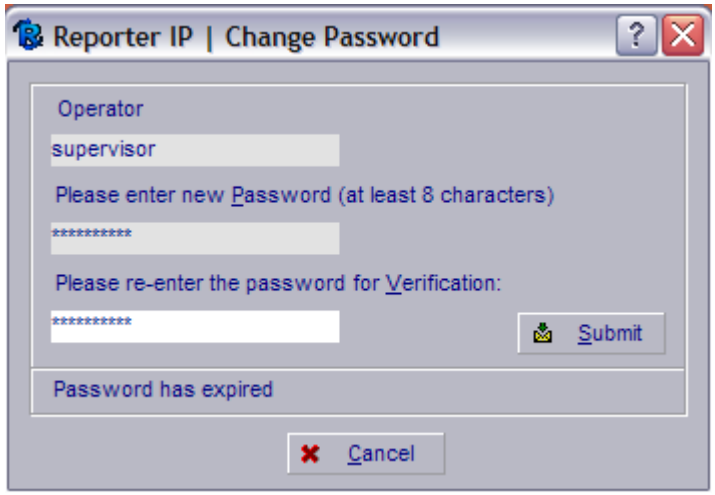


Figura 3.85 *Ingreso de nueva contraseña.*

Cuando se completa esta información se procede a dar clic en el recuadro que está en la figura anterior que dice “Submit”. Aparece una siguiente ventana (Figura 3.86) donde el operador tendrá la posibilidad de añadir administradores y usuarios pudiendo cambiar el nombre de usuario y contraseña (pero solo del supervisor) como se muestra en la Figura 3.86. Se debe tener cuidado en el momento que se crean los nuevos usuarios para darles el estatus (administrador o usuario) que les corresponde para que solo la persona autorizada pueda realizar todas las configuraciones necesarias del sistema.

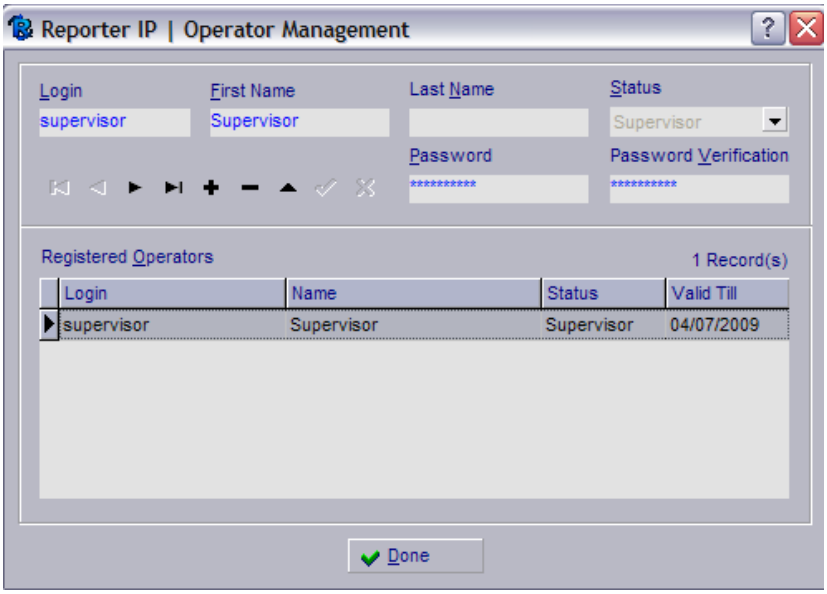


Figura 3.86 *Creación de nuevos operadores.*

Para crear los nuevos usuarios o administradores se hace clic sobre el signo "más" (**+**) que se encuentra en la parte superior, en el momento que se realiza esta acción aparece en la pantalla la posibilidad de ingresar el nombre y el estatus ya sea usuario o administrador, y cuando se termina de llenar los datos necesarios se da clic en el ícono del visto (✔) y luego un clic en el recuadro inferior que dice "Done". Figura 3.87

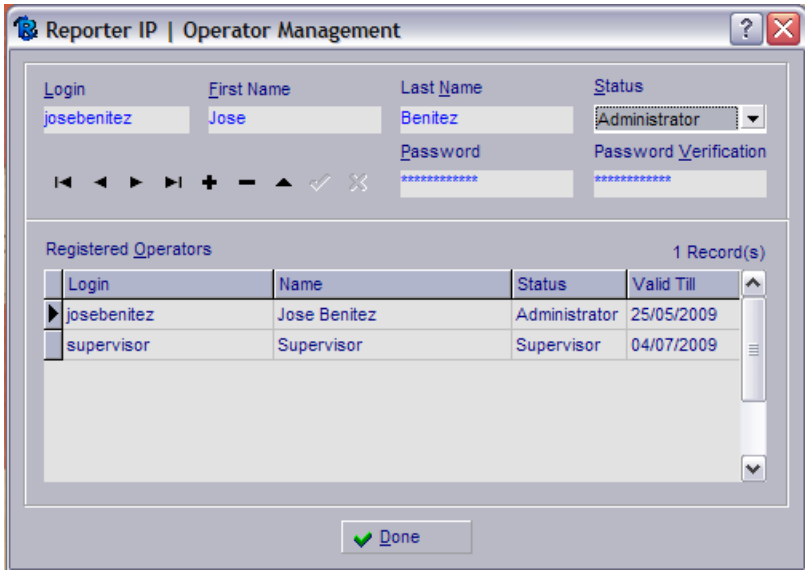


Figura 3.87 *Ingreso de nuevo administrador.*

Aparecerá nuevamente la ventana para iniciar una nueva sesión ya sea que se haya creado un usuario o un administrador nuevo como se indica en la

Figura 3.88 y Figura 3.89 que se muestra a continuación, y enseguida de ingresar los nuevos “Login” y “Password” aparecerá una ventana que advierte que la contraseña ha expirado y se necesita ingresar otra contraseña, esto se repite por dos ocasiones.

Figura 3.88 *Ingreso de contraseña.*

Figura 3.89 *Cambio de contraseña.*

Luego de esto aparece la pantalla de los eventos ocurridos, la cual es la más importante del programa ya que muestra todos los eventos en forma cronológica y en colores para que el tipo de alarma sea más fácil de identificar además muestra de forma resumida los datos complementarios del evento, es decir, la hora, la fecha, el lugar, el sensor que disparó la alarma y el tipo de alarma que se generó. También en la Figura 3.90 se observa que se puede acceder a la barra de herramientas que se encuentra en la parte superior de la ventana; obsérvese que la mayoría de íconos están activados para poder ingresar a estas opciones, esto se debe a que se ingresó al programa como tipo de operador “Administrador”.

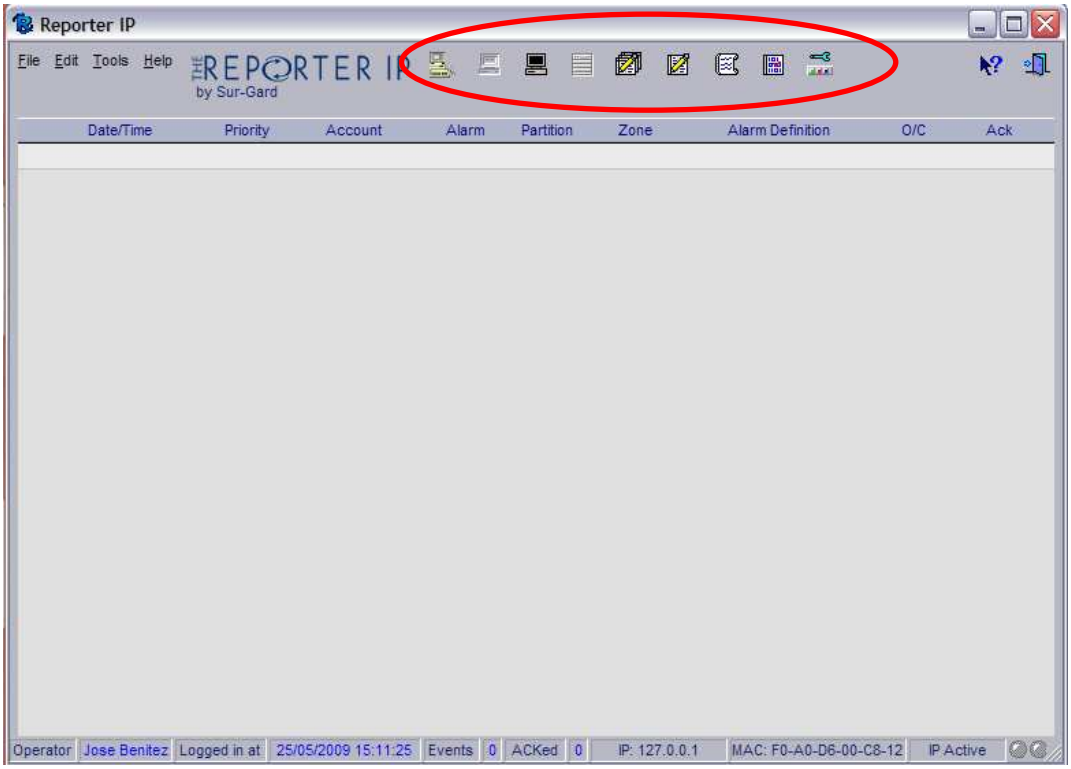


Figura 3.90 *Ventana de Eventos de Alarmas*

Por otro lado se tiene la ventana similar del reporte de eventos pero con algunos de los íconos de la barra de herramientas desactivados, esto se debe a que se ingresó como un tipo de operador "Usuario". Figura 3.91

Figura 3.91 *Ventana de Eventos de Alarma*

Como se menciona anteriormente en la parte superior se tienen diferentes íconos que ayudan en la configuración y administración del sistema, estos íconos son los siguientes:

- **Monitor IP**

Este ícono muestra una pantalla donde se registra el estado de la conexión entre la Matriz y cada una de las agencias. En este caso la matriz de recuadros representaría cada una de las agencias y en la parte inferior de la misma pantalla se muestra por colores el estado de cada conexión. En este caso en la Figura 3.92 se muestra una de las agencias que está conectada y está en activo como lo indica los estados en colores de la parte inferior de la ventana.

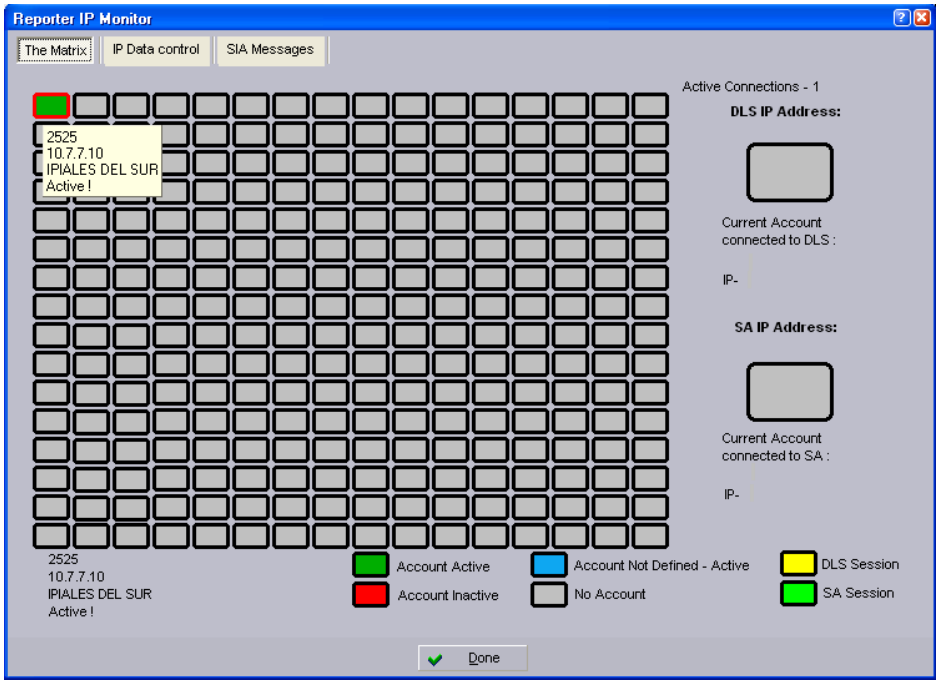


Figura 3.92 *Pantalla estado de conexión.*

- **Inicio de Sesión**

Con este ícono se puede ingresar al programa como otro usuario u otro administrador para los fines que se requiera.

- **Cerrar Sesión**

Al dar clic en este ícono aparece un mensaje de confirmación de cierre de sesión. Al cerrar la sesión los eventos de las alarmas seguirán llegando.

- **Pantalla Principal**

Con este ícono se regresa a la pantalla principal del programa donde se muestran los eventos de alarma ocurridos.

- **Edición de Base de Datos**

Al dar clic en este ícono aparece una ventana la cual muestra como está definida cada una de las alarmas, es decir, el nombre que se les ha dado para que se muestre en la ventana de eventos ocurridos.

- **Edición de Cuentas**

En esta parte aparece una ventana donde se puede crear y administrar las cuentas; en este caso son las agencias que se van a monitorear y sirve para darles ciertos atributos para que ayuden en el momento del monitoreo como son: direcciones, números de teléfono, etc. De esta manera se hace más eficiente el control del operador en cuanto al monitoreo de alarmas de las diferentes agencias.

- **Historial**

Dando clic en este ícono se muestra en una ventana todos los detalles de los acontecimientos ocurridos, estos reportes pueden ser impresos o pasarlos a una hoja de Microsoft Excel.

- **Pantalla de Depuración**

En esta pantalla se mostrará como están llegando los datos de las diferentes agencias. Esto sólo se puede observar cuando se ha ingresado a la sesión como administrador y esta información se muestra de dos formas ASCII y HEX.

- **Configuraciones**

Con esta opción aparece una pantalla donde se puede configurar lo referente a la comunicación IP, ya sea envío o recepción de datos.

Figura 3.93 *Pantalla de configuración de Comunicación.*

Para empezar a crear las cuentas necesarias se tiene que iniciar el programa como Administrador, luego dirigirse a la parte superior donde están los íconos y se escoge “Edición de Cuentas”, en esta pantalla aparece la siguiente ventana Figura 3.94.

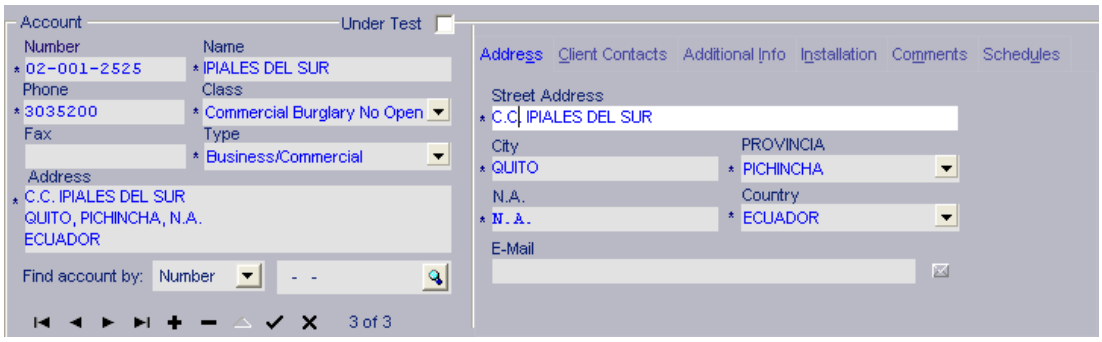


Figura 3.94 *Pantalla de configuración de Comunicación.*

En esta ventana se da clic en “insert record” en el signo de suma que se muestra, se llena todos los datos necesarios que se solicitan para crear la cuenta, los primeros datos a llenar son en “Acount” o “Cuenta” y luego

“Address” o “Direcciones”. Después al lado derecho de esto se tiene “Installation” o “Instalación” donde se coloca la dirección IP del panel de control. Figura 3.95.

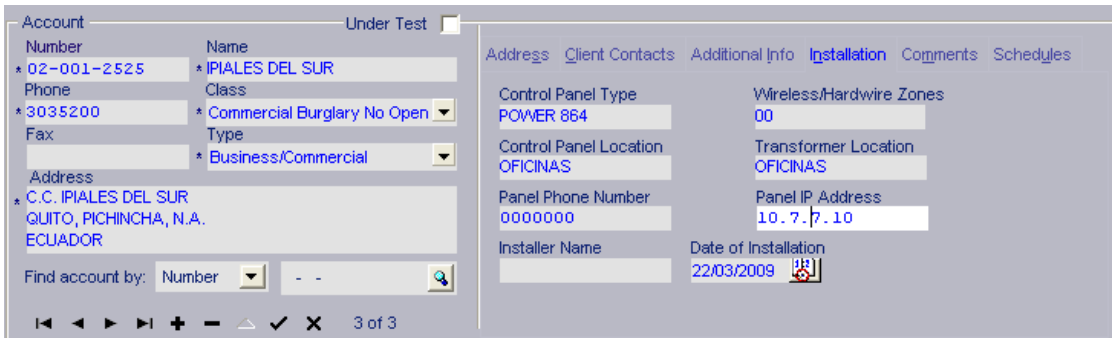


Figura 3.95 *Ingreso de IP.*

3.7.2 SOFTWARE DE CONFIGURACIÓN REMOTA DE ALARMAS

Con este programa se puede realizar las diferentes configuraciones en lo que se refiere al sistema de alarmas monitoreadas de cada uno de los equipos que se encuentran instalados en la agencia, ya que el programa anterior solo permite administrar los eventos ocurridos, es decir, muestra las alarmas activadas o los diferentes sucesos que se programan para saber que la comunicación entre Agencias y Matriz están funcionando.

Las configuraciones son las que se va a programar de acuerdo a las necesidades de cada agencia; como por ejemplo los horarios en los que los sistemas de alarma se van a encender o armar y apagar o desarmar; además se puede crear los diferentes tipos de usuarios que vayan a las agencias para darles sus propios códigos de ingreso, también para poder programar que se envíen pruebas de vida de cada agencia a la matriz para saber que el sistema está funcionando correctamente.

El software DLS permite programar y controlar sistemas de seguridad compatibles con la marca DSC desde cualquier computador que cumpla los requerimientos mínimos solicitados. El DLS puede enviar datos y datos de programación, así como alimentarse de la información pre-programada de los paneles utilizando un modem o el enlace PC LINK.

Los requerimientos mínimos del computador a usar para esta aplicación son:

- Computador con procesador Pentium de 200 MHz
- 64 Mb de RAM
- Los sistemas operativos con los que puede trabajar son Windows 95, 98, NT, Me, 2000 o XP.
- Puerto Ethernet
- CD room para instalación de software
- Puerto PS2 para mouse
- Disco duro 250 Mb destinados para los archivos DLS

En este caso los pasos que se siguen para la instalación de este software son los siguientes:

- Se inserta el CD de instalación.
- Luego se abre el contenido del CD y se da doble clic en el ícono de instalación. Figura 3.96

Figura 3.96 *Ícono de instalación.*

- Una vez realizada la acción anterior aparece la pantalla siguiente para saber donde se va a guardar el programa que se esta instalando. Figura 3.97.

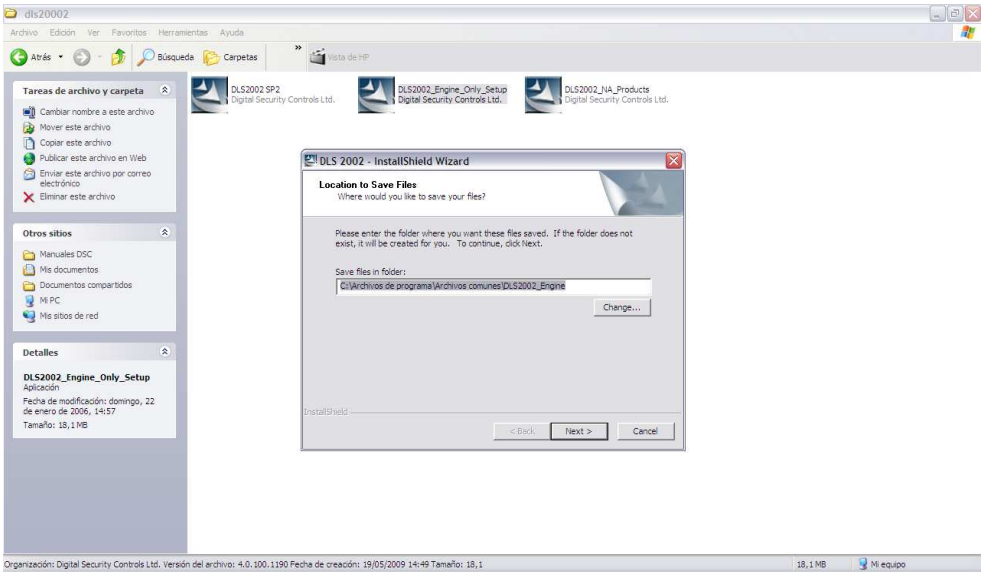


Figura 3.97 *Pantalla de instalación.*

- En el siguiente paso aparecerán las siguientes pantallas donde solo se debe seguir los pasos, en este caso se da clic en los recuadros que dicen “Next”.

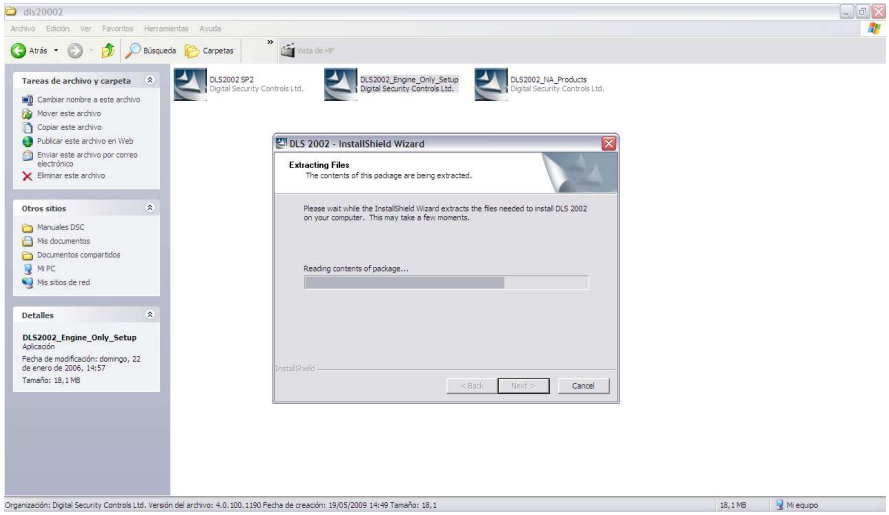


Figura 3.98 *Pantalla de instalación.*

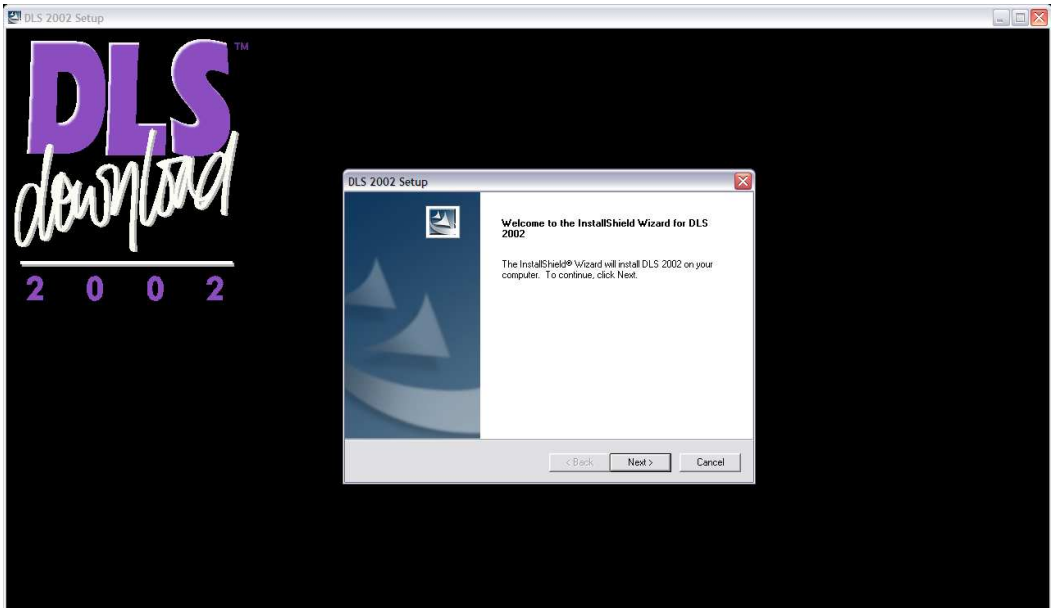


Figura 3.99 *Pantalla de instalación.*

- Luego aparecerá la pantalla donde se debe aceptar las condiciones que pone el programa para su uso.

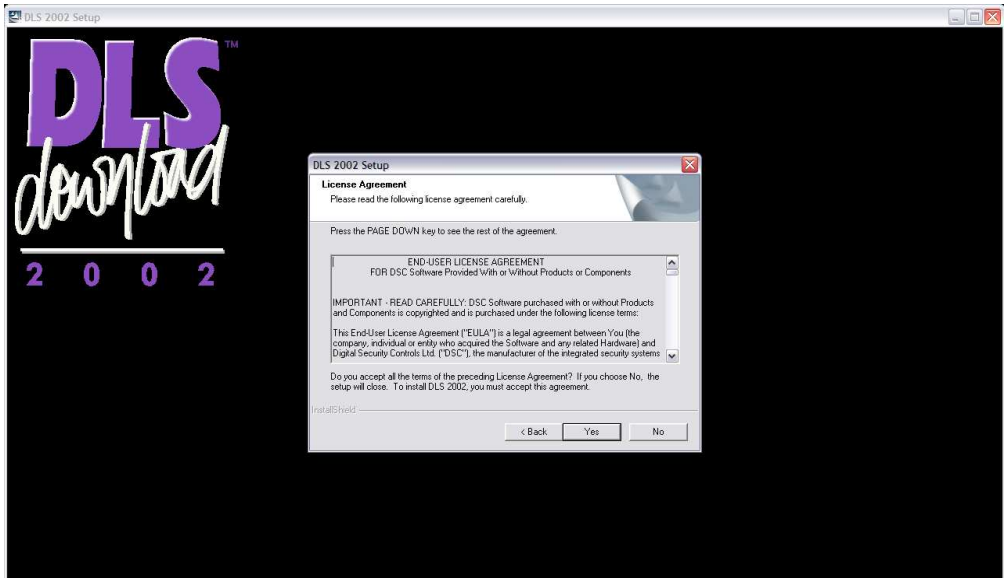


Figura 3.100 *Pantalla de instalación.*

- A continuación aparece una pantalla donde se debe llenar los datos solicitados. Y después de esto se sigue nuevamente con los pasos dando clic en los recuadros que afirmen las acciones.

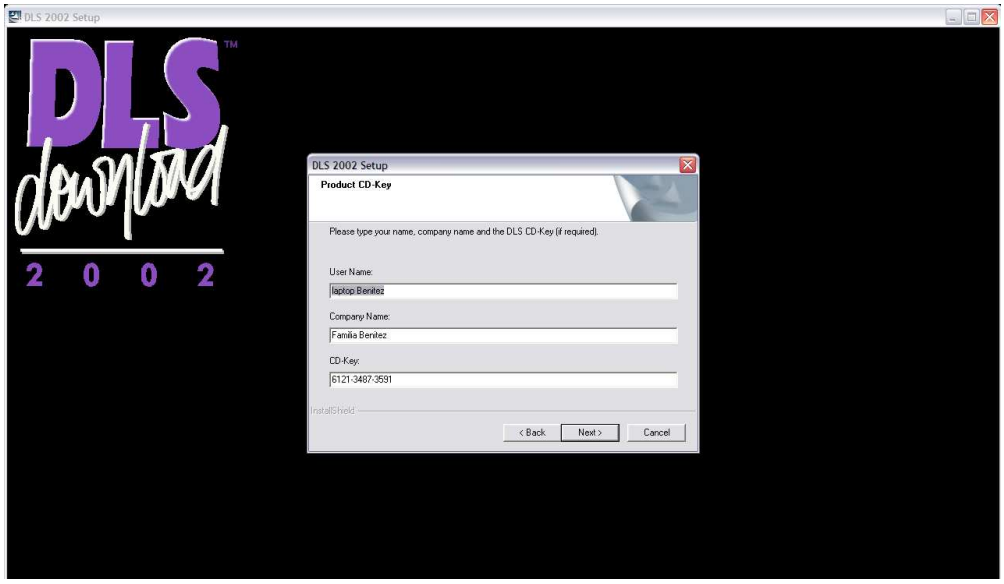


Figura 3.101 *Pantalla de instalación.*

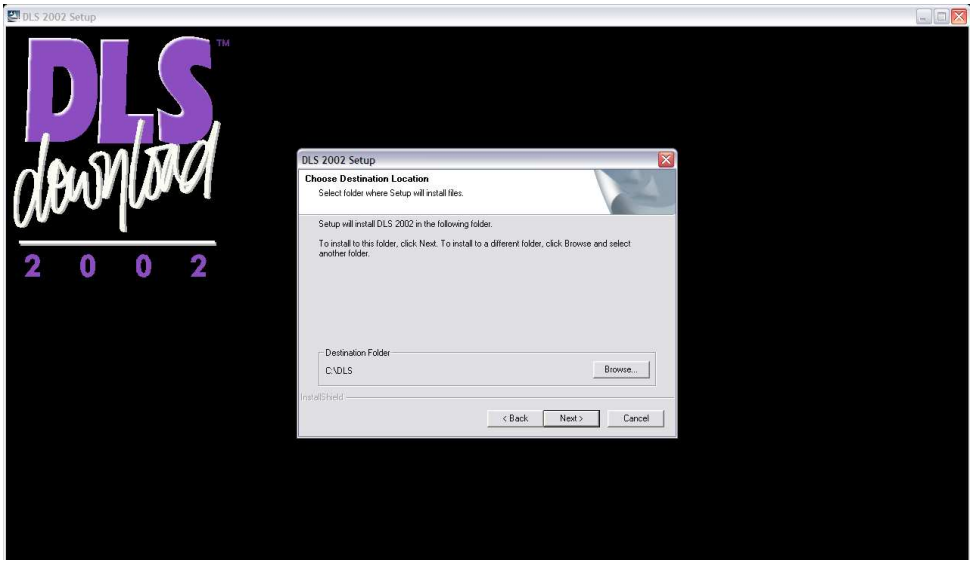


Figura 3.102 *Pantalla de instalación.*

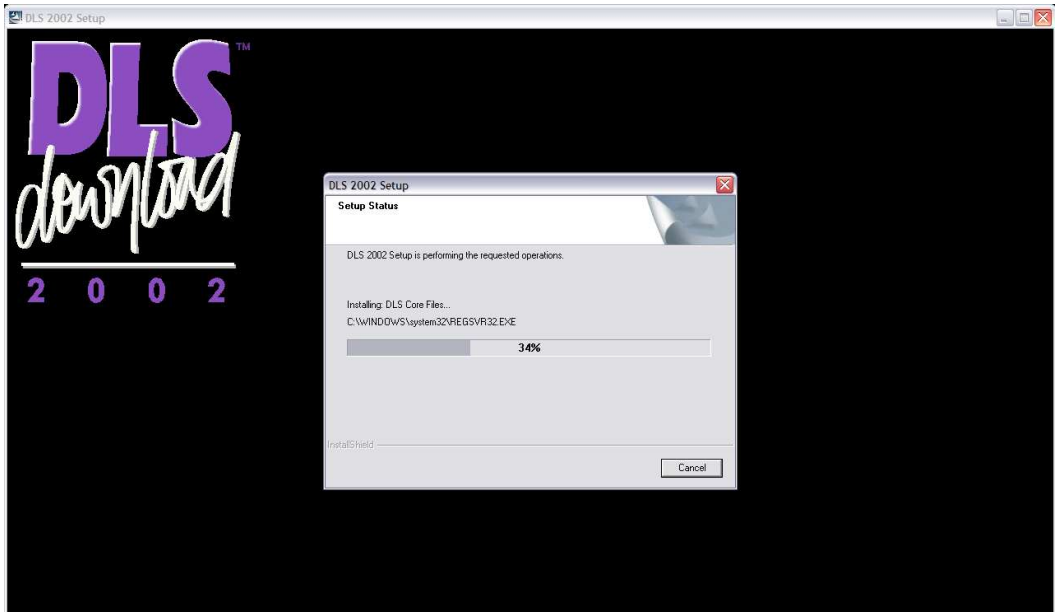


Figura 3.103 *Pantalla de instalación.*

- Después de esperar cierto tiempo en que se instale el programa aparece otra ventana en la cual pregunta si se quiere que aparezca un ícono de inicio del programa en el escritorio.

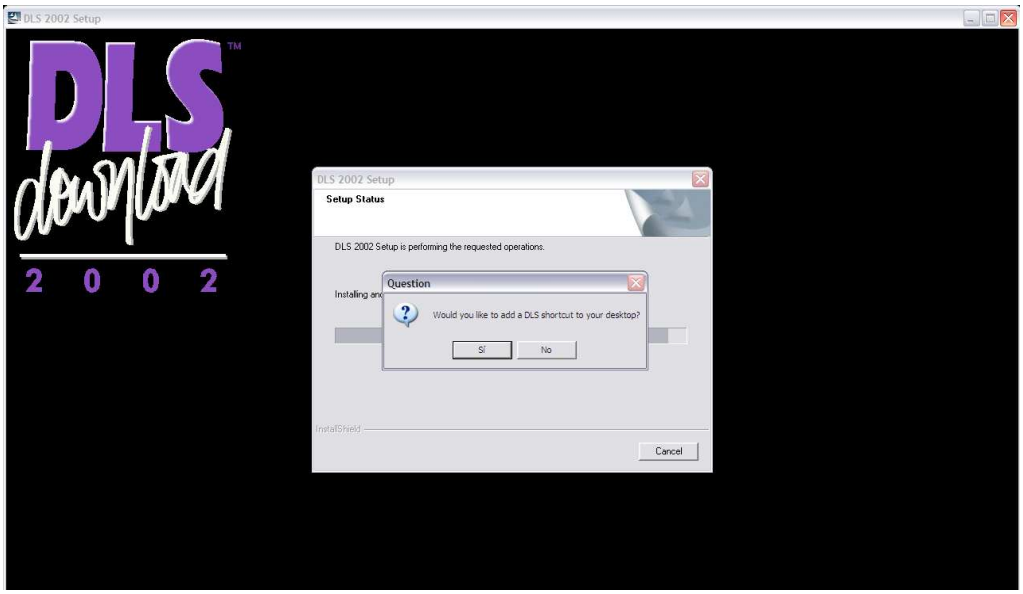


Figura 3.104 *Pantalla de instalación.*

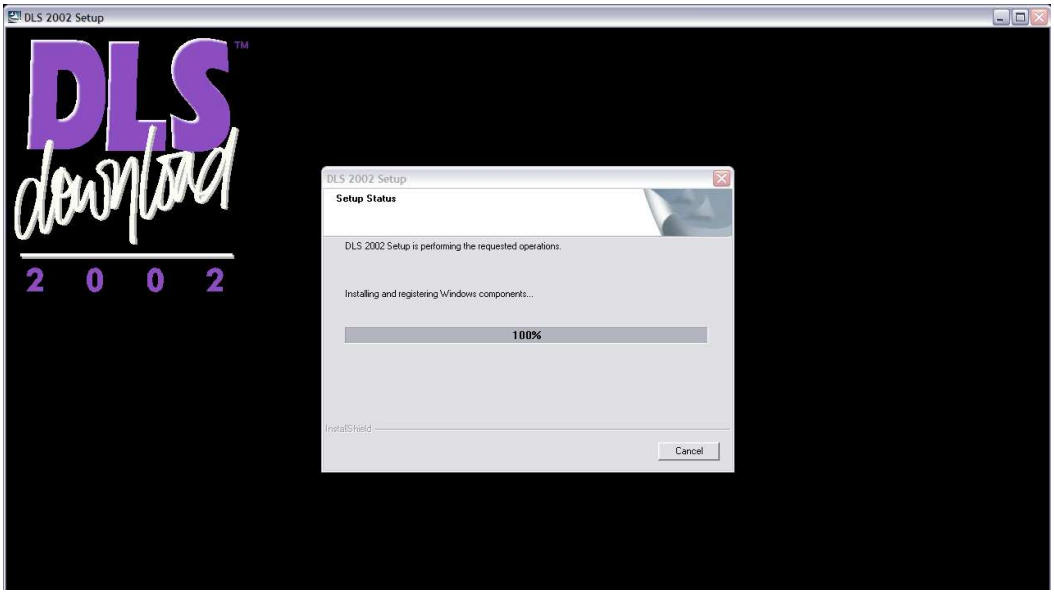


Figura 3.105 *Pantalla de instalación.*

- Por último se finaliza la instalación del programa dando clic en el recuadro que dice “finish”

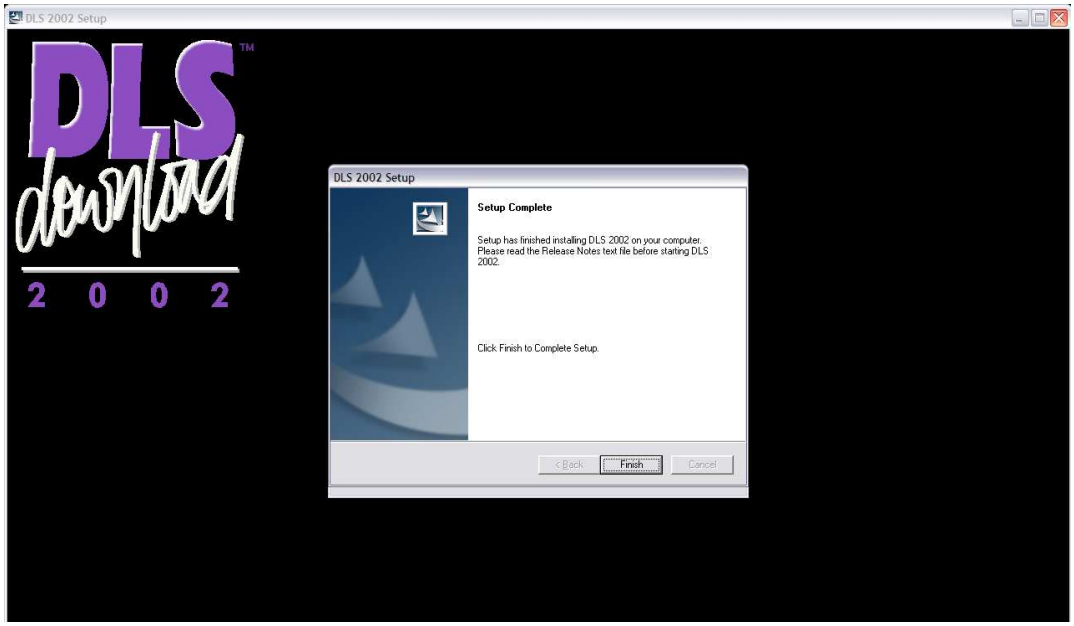


Figura 3.106 *Pantalla de instalación.*

3.7.2.1 Ejecución y Configuración del Software

El software de configuración del sistema remoto es el DLS 2002. Lo primero que se debe realizar para trabajar con el mismo es su ejecución, procedimiento el cual se detallará a continuación.

Sobre el icono DLS en el escritorio de Windows (Figura 3.107), se debe dar dos clics, tras lo cual, se extiende una pantalla emergente del software, la cual, cumple la función de login del sistema (Figura 3.108).

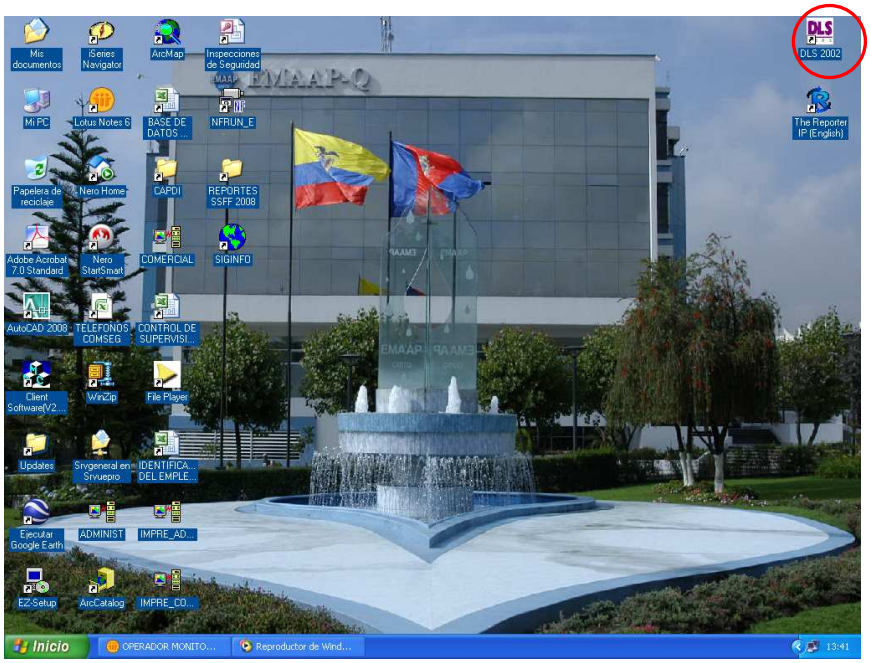


Figura 3.107 *Ejecución del software DLS*

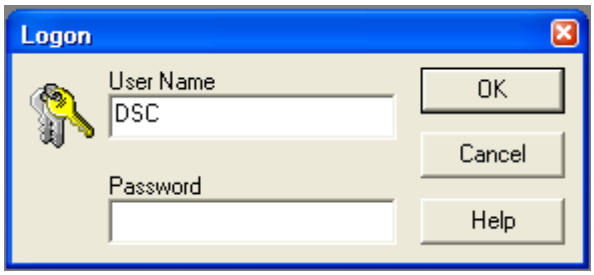


Figura 3.108 *Cuadro de Login al software DLS*

Como se observa en la Figura 3.108, el software DLS solicita un password de inicio, el cual, por default en su instalación, está conformado por cuatro números, en este caso:

Login: DSC, **Password:** 1234

Tras esto se procede a dar un clic en OK, con lo cual, se ejecuta el software y muestra la pantalla principal de manejo. Dicha pantalla se muestra en la Figura 3.109.

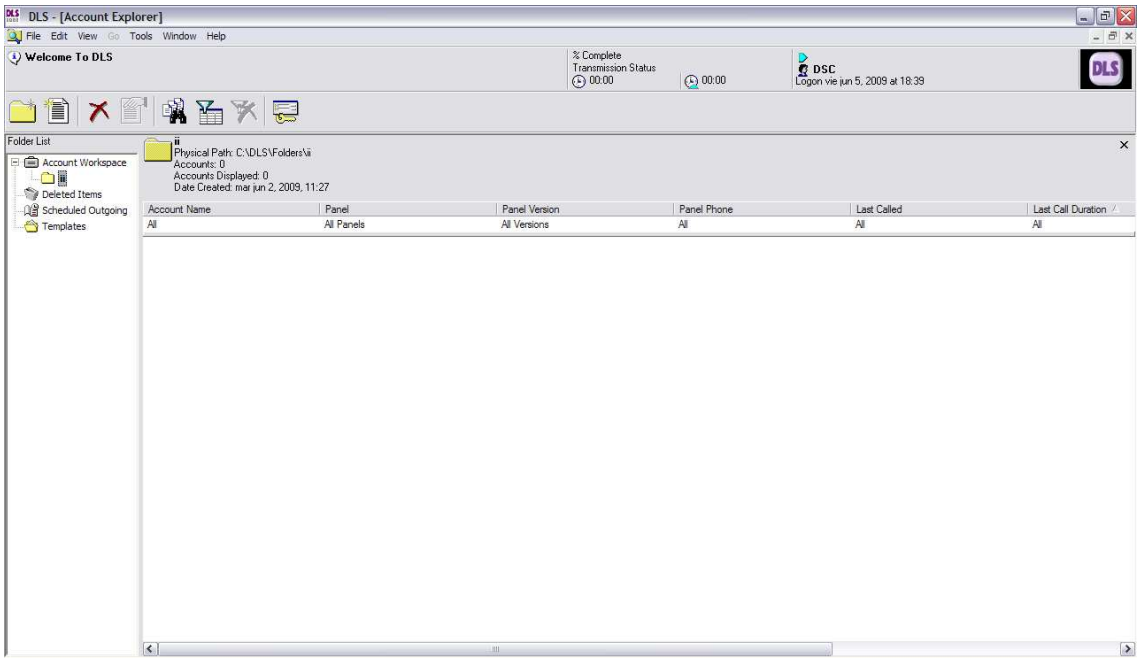


Figura 3.109 *Pantalla principal del software de configuración*

Para empezar con la configuración se procede en la pantalla principal, en el lado izquierdo de la pantalla se muestra una columna donde se encuentran varios íconos y carpetas, donde dice “Account Workspace” se da un clic derecho y se escoge “New Folder” y se pone el nombre, en este caso se escogió EMAAP y se da clic en el recuadro donde dice “Create”. Figuras 3.110 y 3.111.

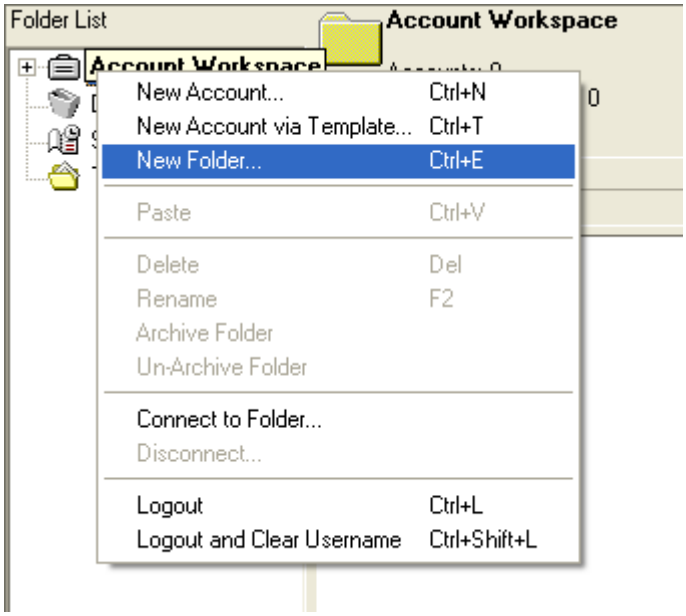


Figura 3.110 *Creación de una nueva cuenta.*

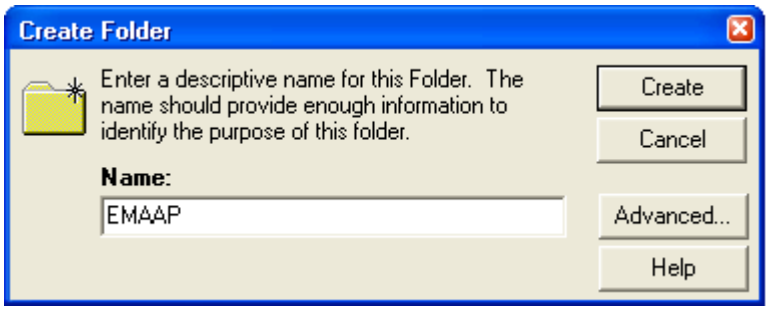


Figura 3.111 *Creación de una nueva cuenta.*

Siguiendo con el procedimiento se da clic derecho en el centro de la pantalla que se muestra en la Figura 3.109 y se escoge la opción “New Account” y aparece la pantalla siguiente. Figura 3.112.

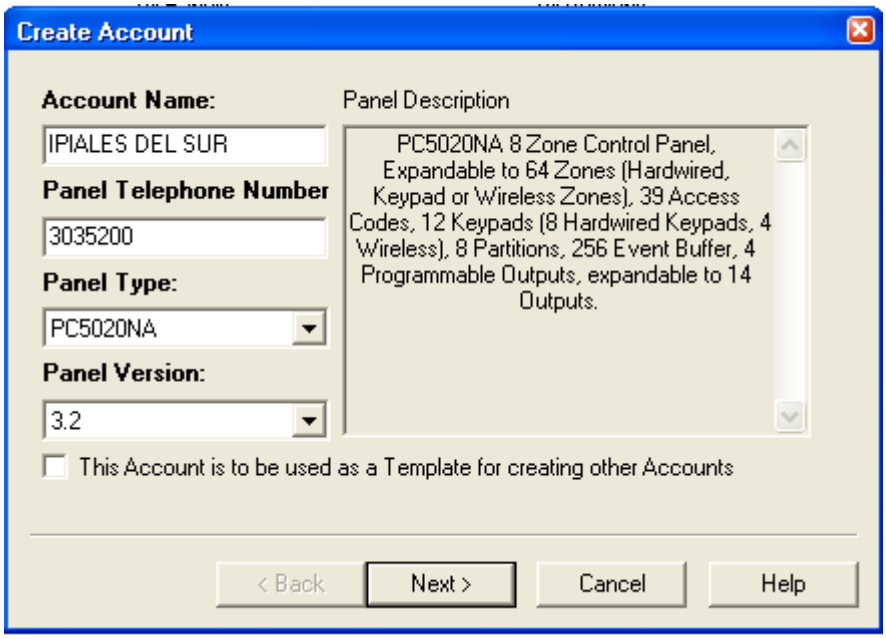


Figura 3.112 *Creación de una nueva cuenta.*

Luego se procede a llenar los datos solicitados, en esta parte se debe tomar en cuenta que los datos van a ser transmitidos vía IP y no por vía telefónica. Se sigue con el procedimiento dando clic en “Next” para ir completando los datos requeridos.

En la siguiente pantalla que se despliega se solicita el ingreso de módulos extras por ejemplo expansores, transmisores de radiofrecuencia, etc., y se sigue con el procedimiento de dar clic en el recuadro de “Next”. Figura 3.113.

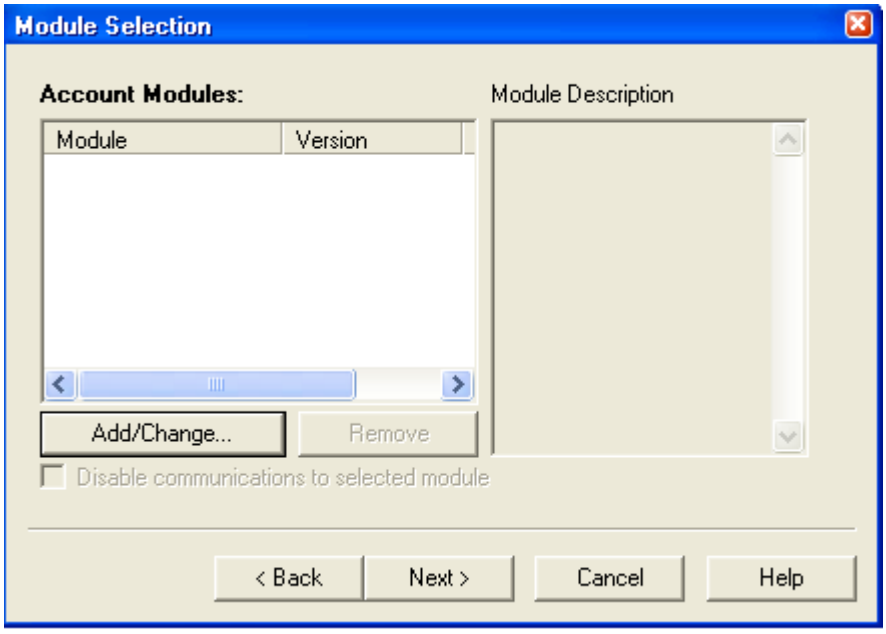


Figura 3.113 *Creación de una nueva cuenta.*

En la pantalla que se despliega posteriormente se solicita el ingreso de la información pertinente de la compañía que va a ser uso de este software en este caso la EMAAP-Q. Luego de seguir con el proceso de dar clic en el recuadro "Next", en la última pantalla desplegada aparece la opción para elegir el "Espacio de Trabajo" en donde se elige EMAAP y se da clic en el recuadro que dice "Finish" para finalizar el proceso de creación de cuenta. Figura 3.114.

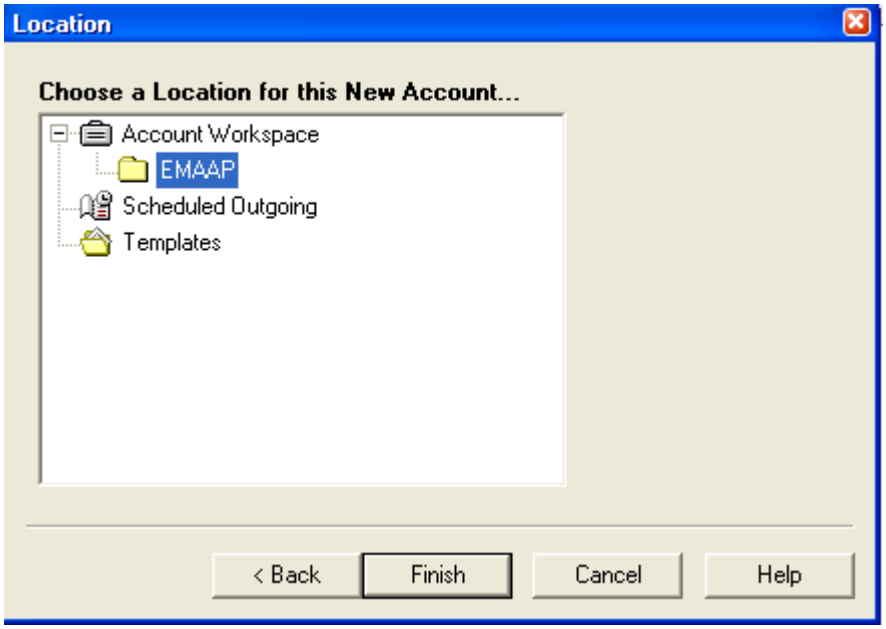


Figura 3.114 *Datos de comunicación.*

Continuando con la configuración de la cuenta se debe definir ciertos datos para la comunicación, en la pantalla principal se debe dirigir a la cuenta creada que aparece, se da clic derecho y se escoge “Properties”. Dentro de esta opción se escoge “TCP/IP Settings” en la cual se ingresa la dirección IP del panel de control de alarma y se finaliza dando clic en el recuadro que dice “OK”. Figura 3.115.

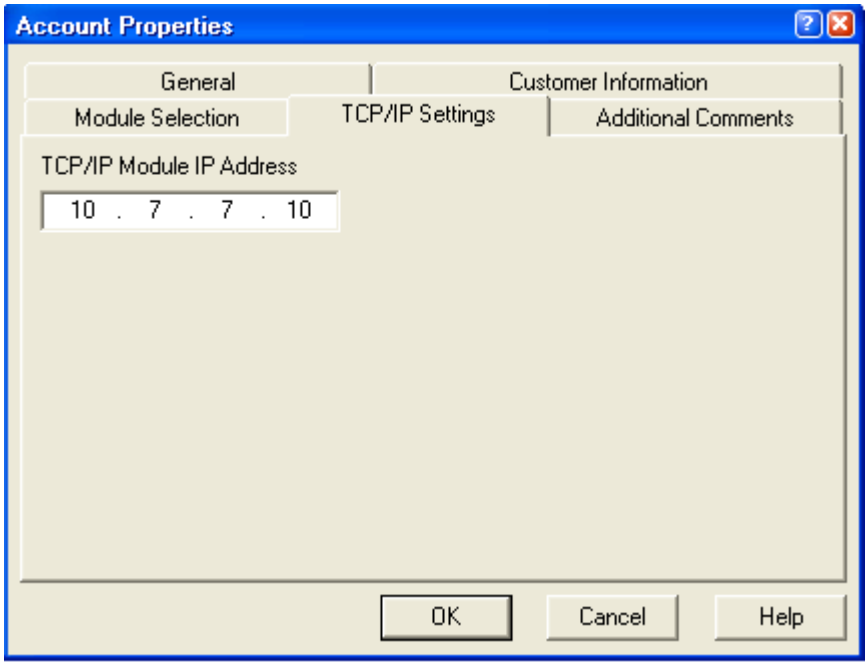


Figura 3.115 *Datos de comunicación.*

CAPITULO 4. PRUEBAS Y RESULTADOS

4.1 PRUEBAS A TRAVÉS DEL SOFTWARE DE CONFIGURACION

Las siguientes pruebas se realizaron en la central de monitoreo que se encuentra ubicada en el edificio matriz de la EMAAP-Q, las pruebas se realizan a través de la comunicación existente entre la Agencia Ipiales del Sur y la matriz de la EMAAP-Q. El panel de control del sistema de alarmas que se encuentra en la agencia de recaudación siempre está enviando y recibiendo datos de esta manera siempre se esta verificando el funcionamiento de la red entre las dos dependencias antes mencionadas.

4.1.1 INGRESO AL SISTEMA

Para poder ingresar al sistema Ipiales del Sur, se debe dar doble clic en la barra azul de la pantalla principal del software, sobre la cual se describe: IPIALES DEL SUR. (Figura 4.1)

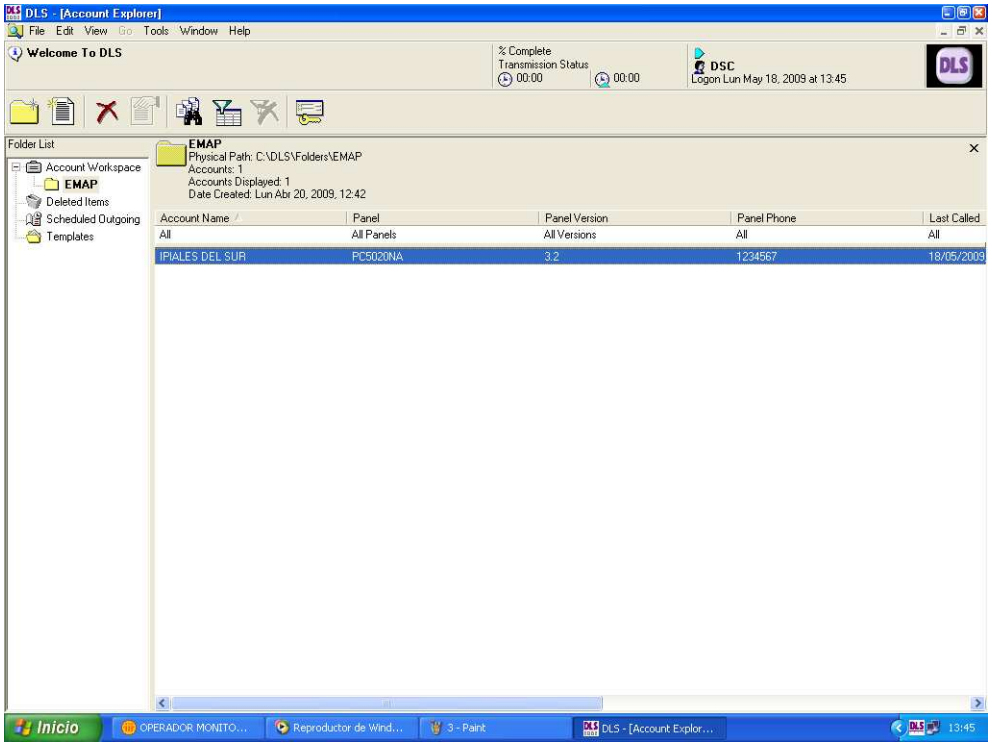


Figura 4.1 *Pantalla principal del software de configuración*

A continuación, tal como se muestra en la Figura 4.2, se despliega una pantalla secundaria que describe y permite modificar las características del panel PC5020 perteneciente a la agencia de recaudación. Sobre esta se puede proceder a realizar cualquier modificación deseada en el panel.

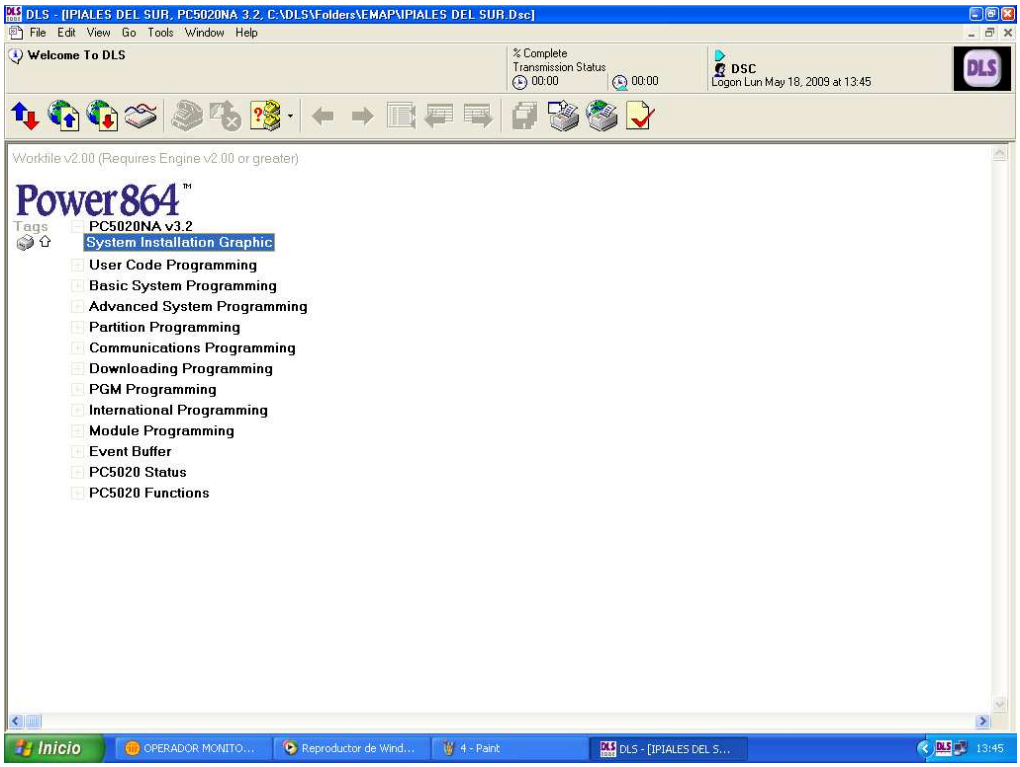


Figura 4.2 *Pantalla principal del software de configuración*

4.1.2 PRUEBA DE CONFIGURACION REMOTA DE TIEMPO DE VIDA

Esta prueba consistirá en la configuración remota del tiempo periódico con el cual el panel de control implementado en la agencia de recaudación Ipiales del Sur transmitirá sus Automatic Test o Pruebas de vida.

Dentro de la pantalla de configuración, mostrada en la Figura 4.2, se encuentra la opción **Communications Programming** (Programación de comunicaciones). Sobre esta se debe dar doble clic y esperar se despliegue en la misma pantalla las opciones de configuración en las comunicaciones (Figura 4.3).

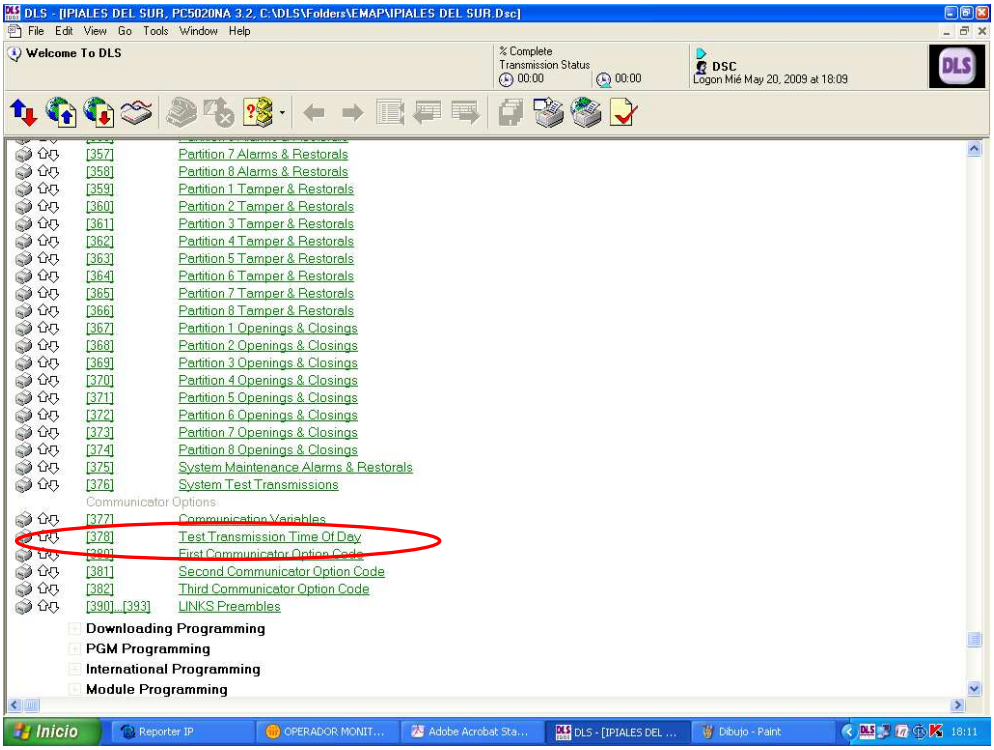


Figura 4.3 *Opciones de configuración desplegadas*

De este listado se escoge la **opción 377: Communication Variables,** se da dos clics en la misma y se espera que se despliegue el siguiente sub menú de la configuración, tal como lo muestra la Figura 4.4

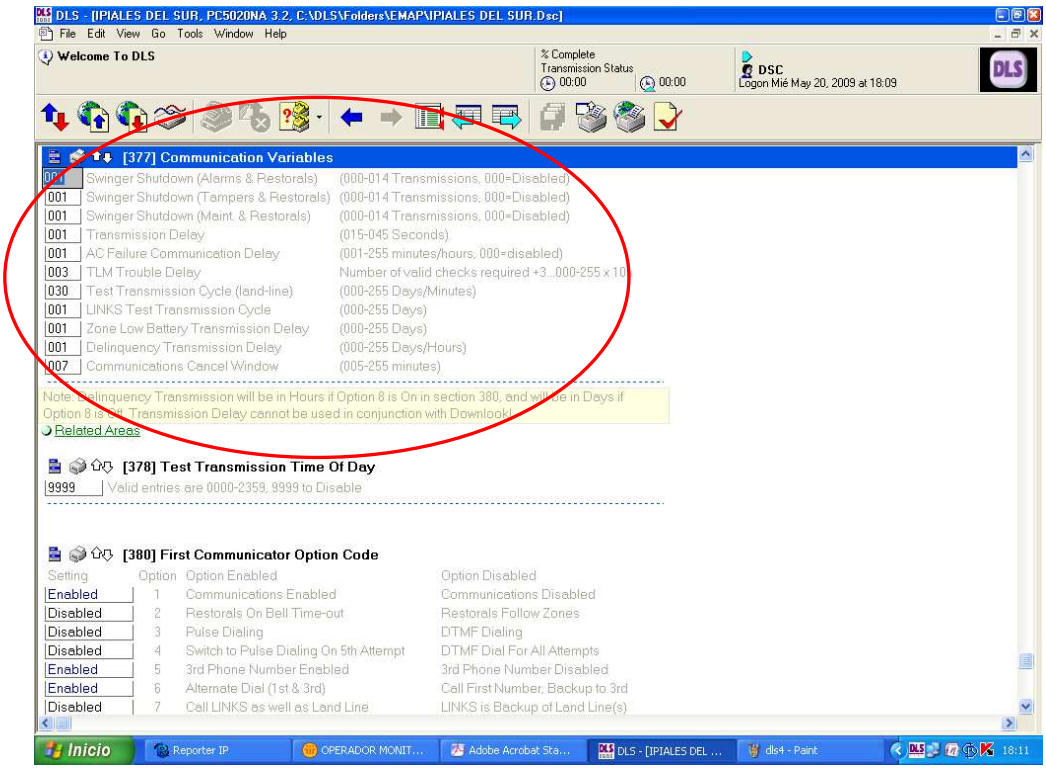


Figura 4.4 *Menú de Communication Variables*

Para cambiar el tiempo de transmisión de la prueba de vida se deberá elegir la opción **Test Transmisión Cycle** (Ciclo de transmisión de prueba) mostrada en la Figura 4.5, para lo cual, a la izquierda de su nombre, se ingresará el tiempo periódico deseado para transmitir el Automatic Test.

En esta prueba, se cambiara la cifra de 30 minutos a 120 minutos, y a su vez, se descargará el mencionado cambio al panel de control utilizando la vía ADSL.

001	Transmission Delay	(015-045 Seconds)
001	AC Failure Communication Delay	(001-255 minutes/hours, 000=disabled)
003	TLM Trouble Delay	Number of valid checks required +3...000-255 x 10s
030	Test Transmission Cycle (land-line)	(000-255 Days/Minutes)
001	LINKS Test Transmission Cycle	(000-255 Days)
001	Zone Low Battery Transmission Delay	(000-255 Days)

Figura 4.5 *Opción Test Transmisión Cycle*

Lo primero en realizarse es posar el cursor sobre la cifra 30, borrarla y colocar en vez de esta 120, tal como lo muestra la Figura 4.6

001	Transmission Delay	(015-045 Seconds)
001	AC Failure Communication Delay	(001-255 minutes/hours, 000=disabled)
003	TLM Trouble Delay	Number of valid checks required +3...000-255 x 10s
120	Test Transmission Cycle (land-line)	(000-255 Days/Minutes)
001	LINKS Test Transmission Cycle	(000-255 Days)
001	Zone Low Battery Transmission Delay	(000-255 Days)

Figura 4.6 *Cambio de tiempo sobre la opción Test Transmisión Cycle*

Tras haber ingresado el nuevo valor de tiempo en minutos que le tomará al panel de control transmitir cíclicamente su prueba de vida, se debe bajar el mencionado dato al panel de control, para lo cual, en la parte izquierda de título del menú (Communication Variables) se debe dar un clic en el primer icono en espera que se despliegue un menú emergente con las opciones: Upload Section, Download Section, Print Section y Tag This Section. La opción a elegir, tal como se muestra en la figura 4.7 será la opción Download Section, o en español: descargar sección.

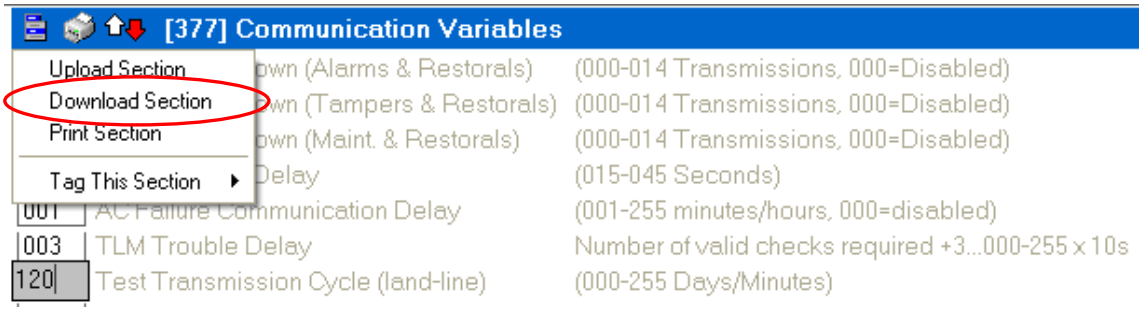


Figura 4.7 *Cambio de tiempo sobre la opción Test Transmision Cycle*

Inmediatamente el software de control establece comunicación con el panel de control, descarga la información y se mantiene enlazado a la agencia de recaudación en espera de descargar un nuevo dato o a su vez, que se le ordene desconectarse y volver a estado normal de software

Debido a que las pruebas se realizaran independientemente una de otra, se procederá a desconectar el software del panel de control, procedimiento el cual se detalla a continuación.

La Figura 4.8 muestra la parte superior izquierda de la pantalla del software DLS. Sobre esta, se denota un icono similar a un teléfono. Al dar clic sobre este, se desconecta el software del panel de control PC5020, con lo cual, si se considera necesario, se procede a cerrar el software DLS.

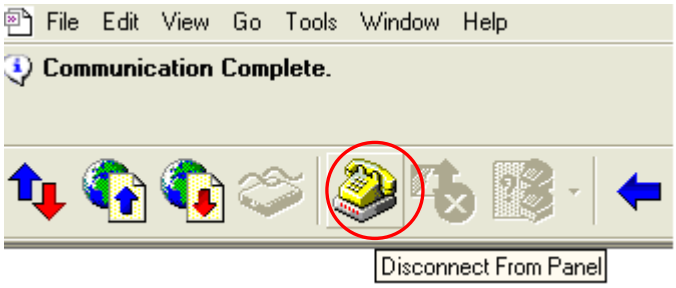


Figura 4.8 *Desconexión del panel de control al software DLS*

4.1.3 PRUEBA DE ARMADO REMOTO DEL SISTEMA

Esta prueba consiste en armar el sistema de alarmas sin necesidad de encontrarse en la agencia Ipiales del Sur, en otras palabras, armar el sistema

desde la central de monitoreo sin intermediación de un tercero en la instalación a monitorearse.

Para dar inicio a la misma, se debe ir a la pantalla principal de configuración (mostrada en la Figura 4.2), elegir la opción: “PC5020 Functions”, y sobre la pantalla emergente mostrada, trabajar sobre el listado: “Arming & Disarming”.

En la opción **Partition 1**, se debe dar un clic a la opción “Yes”, para posteriormente elegir el comando “Arm Partition”, tal como lo muestra la Figura 4.9.

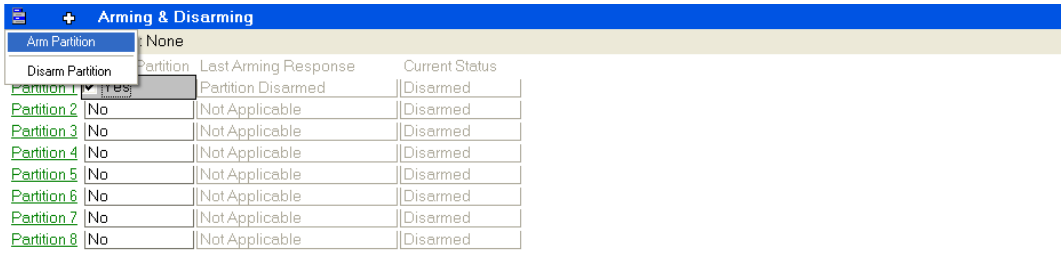


Figura 4.9 *Desconexión del panel de control al software DLS*

A continuación se da inicio a la transferencia de mandos para la ejecución del evento, misma que es alertada en la agencia Ipiales del Sur con los pitidos de tiempo de demora sobre el teclado de programación.

4.1.4 PRUEBA DE DESARMADO REMOTO DEL SISTEMA

Tras haber armado el sistema remotamente, se debe proceder a realizar la prueba de desarmado, misma que contempla los mismos pasos detallados en el punto anterior con la única diferencia de elegir el comando “Disarm Partition” a ser ejecutado, tal como se muestra en la Figura 4.10

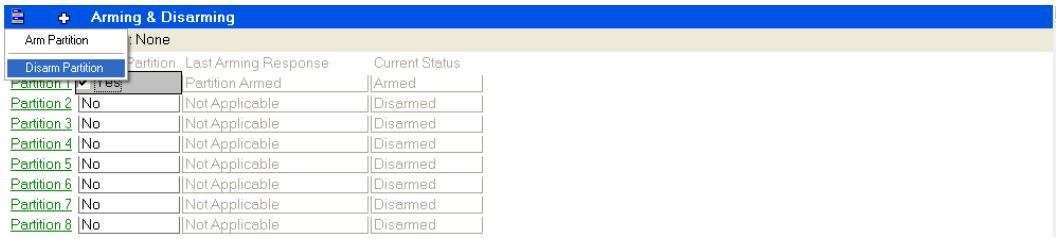


Figura 4.10 *Desconexión del panel de control al software DLS*

Cabe señalarse que los eventos de Armado y Desarmado son mostrados en el software de monitoreo Reporter, en este caso, uno seguido del otro debido al desarrollo de las pruebas continuamente.

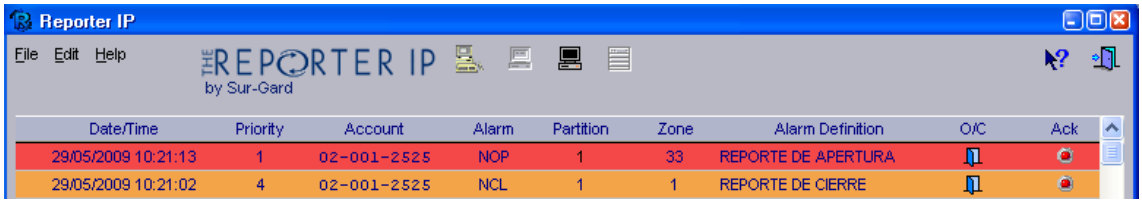


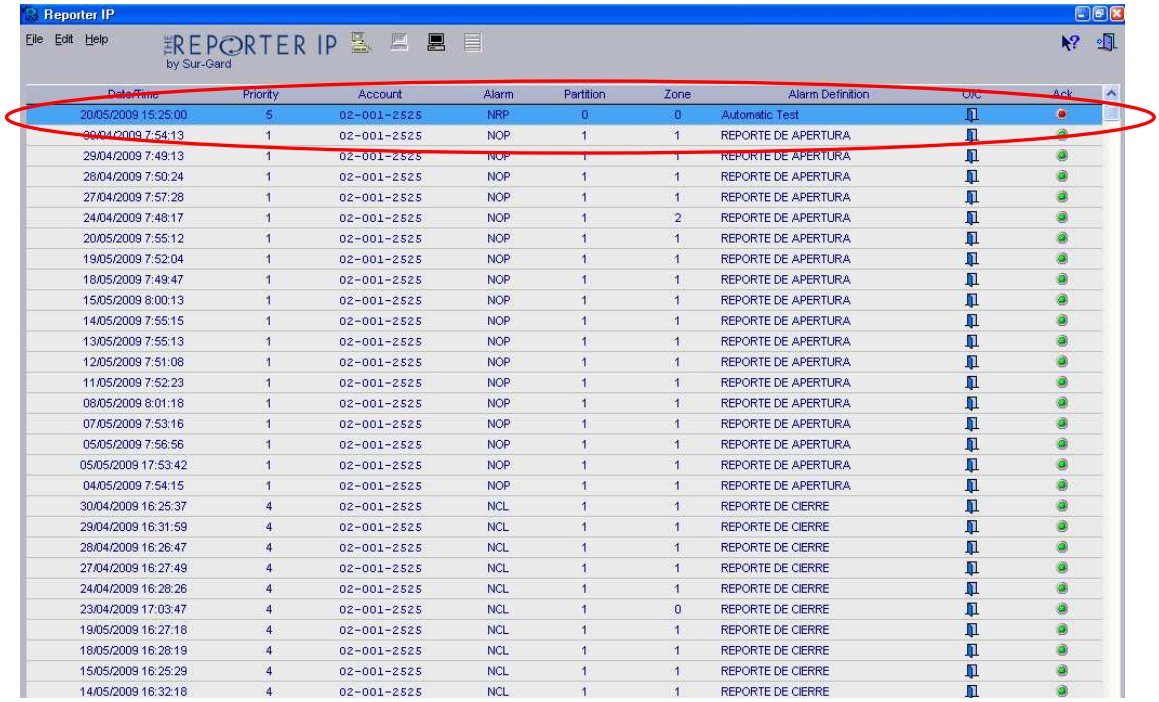
Figura 4.11 *Eventos de armado y desarmado del sistema*

Para realizar las acciones antes mencionadas se debe tener un conocimiento básico en el uso del computador luego se puede decir que la programación o las pruebas antes mencionadas no son muy complicadas de realizar si se tiene el conocimiento del uso del software requerido, aunque si se necesita un conocimiento en cuanto se refiere a la disposición de los equipos instalados y como funciona el sistema.

4.2 SOFTWARE DE MONITOREO

4.2.1 PRUEBA DE VIDA DEL SISTEMA

Al panel de control en Ipiales del Sur se lo programó para emitir una prueba de vida cada treinta minutos, siendo así, y como ejemplo del funcionamiento correcto del mismo, se tomó como referencia la prueba del día 20 de mayo de 2009, a las 15:25 pm, tal como lo muestra la Figura 4.12



Date/Time	Priority	Account	Alarm	Partition	Zone	Alarm Definition	O/C	Ack
20/05/2009 15:25:00	5	02-001-2525	NRP	0	0	Automatic Test		
30/04/2009 7:54:13	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
29/04/2009 7:49:13	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
28/04/2009 7:50:24	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
27/04/2009 7:57:28	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
24/04/2009 7:48:17	1	02-001-2525	NOP	1	2	REPORTE DE APERTURA		
20/05/2009 7:55:12	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
19/05/2009 7:52:04	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
18/05/2009 7:49:47	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
15/05/2009 8:00:13	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
14/05/2009 7:55:15	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
13/05/2009 7:55:13	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
12/05/2009 7:51:08	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
11/05/2009 7:52:23	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
08/05/2009 8:01:18	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
07/05/2009 7:53:16	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
05/05/2009 7:56:56	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
05/05/2009 17:53:42	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
04/05/2009 7:54:15	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
30/04/2009 16:25:37	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
29/04/2009 16:31:59	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
28/04/2009 16:26:47	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
27/04/2009 16:27:49	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
24/04/2009 16:28:26	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
23/04/2009 17:03:47	4	02-001-2525	NCL	1	0	REPORTE DE CIERRE		
19/05/2009 16:27:18	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
18/05/2009 16:28:19	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
15/05/2009 16:25:29	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
14/05/2009 16:32:18	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		

Figura 4.12 *Evento prueba de vida*

El siguiente paso tras recibir la prueba de vida es reconocer el evento, dando doble clic sobre el mismo en espera de la pantalla de reconocimiento, la cual, se muestra en la Figura 4.13

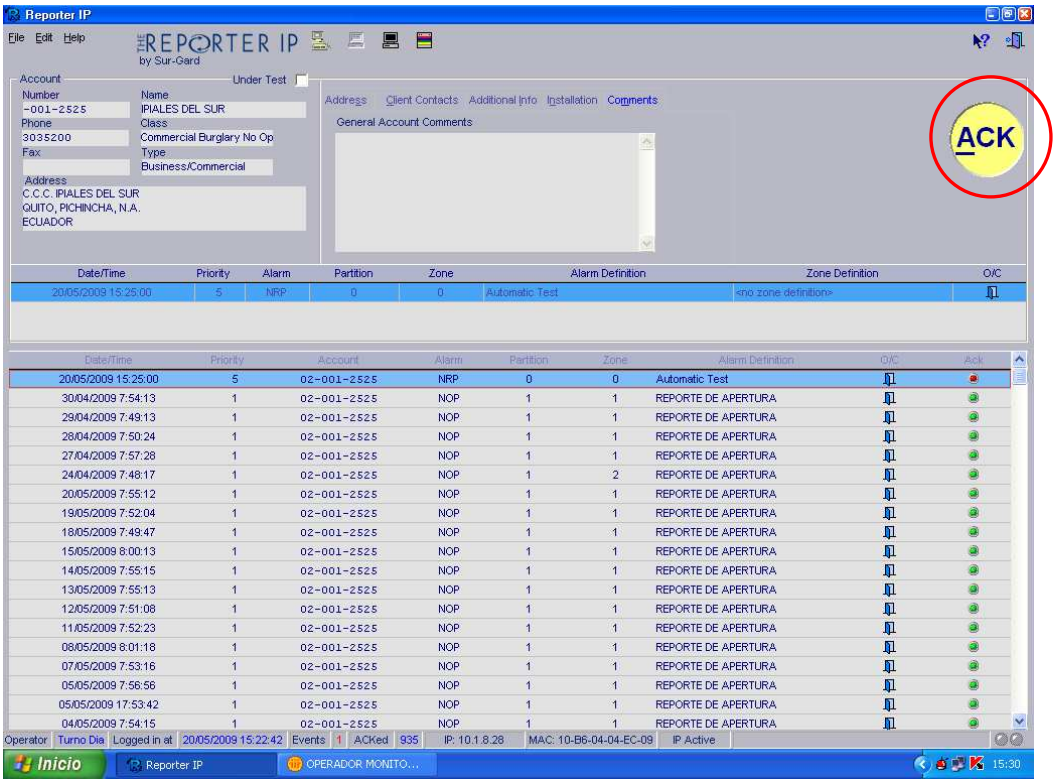


Figura 4.13 *Pantalla para reconocimiento de evento*

A continuación se procede a dar doble clic sobre el icono ACK (acknowledge o reconocimiento), ubicado en la parte superior derecha de color amarillo, presentándose seguido a esto una segunda pantalla emergente que solicita se confirme el reconocimiento.

El mencionado reconocimiento es solicitado en la única barra de color rojo presentada en la pantalla emergente (Figura 4.14).

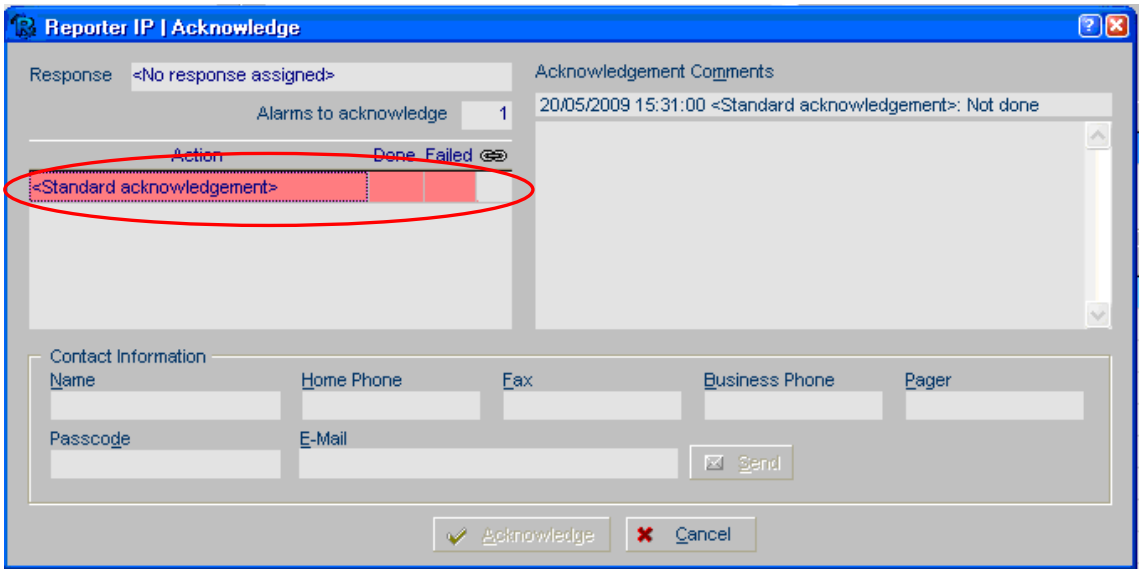


Figura 4.14 *Pantalla emergente para reconocimiento de evento*

Posterior a esto, se debe dar un clic en la sección Done (realizado) o Failed (fallido) para determinar el tipo de reconocimiento realizado por el monitor, en este caso: Done, debido a que es una prueba estándar del sistema. Dicho procedimiento se muestra en la Figura 4.15.

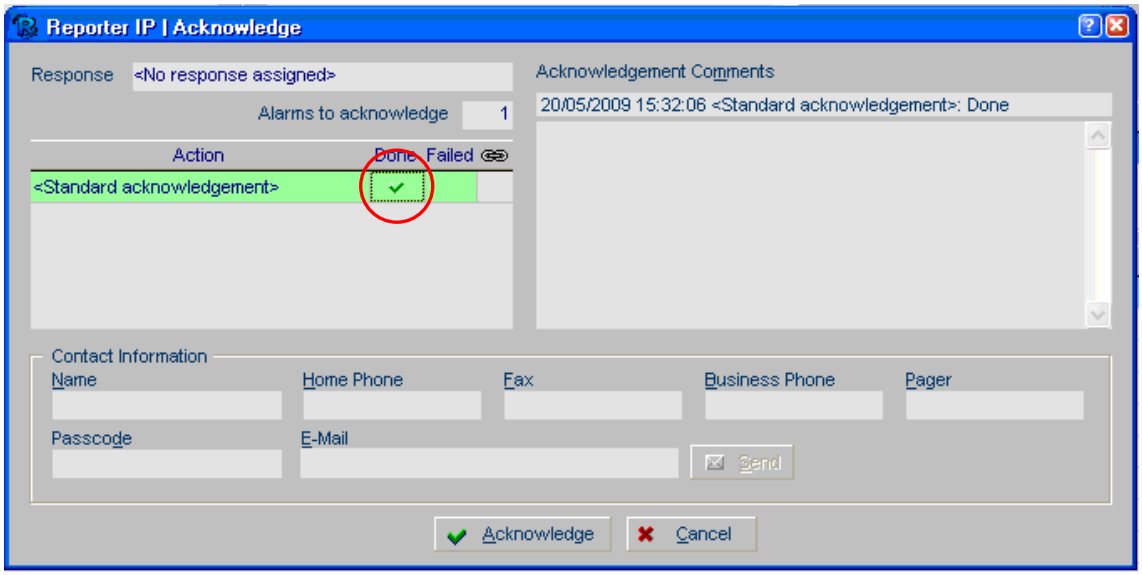


Figura 4.15 *Reconocimiento normal realizado*

En la parte posterior derecha de la pantalla emergente se puede colocar un comentario si uno lo considera necesario, en este caso se coloca el nombre de la persona que estaba realizando dicho monitoreo. Para finalizar, se da un clic en el icono inferior izquierdo: Acknowledge. (Figura 4.16)

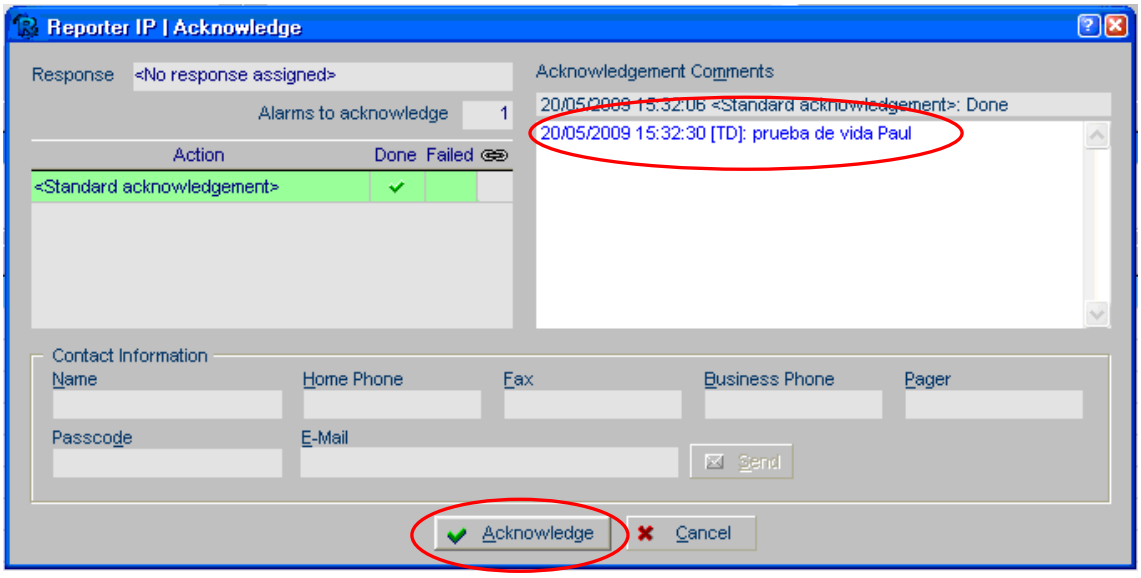


Figura 4.16 *Comentario sobre el reconocimiento realizado*

De esta forma se completa el reconocimiento de la prueba de vida del panel de control, continuando con la pantalla normal del software Reporter, la cual ya mostrará la prueba de vida que se acabó de confirmar. (Figura 4.17)

20/05/2009 15:55:00	5	02-001-2525	NRP	0	0	Automatic Test
20/05/2009 15:29:08	5	02-001-2525	NRS	0	0	Remote Program Success
20/05/2009 15:25:00	5	02-001-2525	NRP	0	0	Automatic Test
20/05/2009 14:28:08	5	02-001-2525	NRS	0	0	Remote Program Success

Figura 4.17 *Reconocimiento de evento sobre pantalla de monitoreo*

4.2.2 PRUEBA DE BOTÓN DE PÁNICO

A continuación se detalla una prueba de botón de pánico, mismo que fue desarrollado el día 20 de mayo de 2009 a las 16:26 PM. La Figura 4.18 muestra la pantalla de monitoreo con la notificación de Panic Alarm (Alarma de Pánico)

Cabe detallarse que el evento suscitado fue solamente una prueba, es decir, se solicito al personal de la Agencia de Recaudación que active uno de los botones de pánico ubicados en las cajas de recaudación.

Reporter IP

File Edit Help

THE REPORTER IP by Sur-Gard

Date/Time	Priority	Account	Alarm	Partition	Zone	Alarm Definition	O/C	Ack
20/05/2009 16:26:16	5	02-001-2525	NPA	1	5	Panic Alarm		
30/04/2009 7:54:13	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
29/04/2009 7:49:13	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
28/04/2009 7:50:24	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
27/04/2009 7:57:28	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
24/04/2009 7:48:17	1	02-001-2525	NOP	1	2	REPORTE DE APERTURA		
20/05/2009 7:55:12	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
19/05/2009 7:52:04	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
18/05/2009 7:49:47	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
15/05/2009 8:00:13	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
14/05/2009 7:55:15	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
13/05/2009 7:55:13	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
12/05/2009 7:51:08	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
11/05/2009 7:52:23	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
08/05/2009 8:01:18	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
07/05/2009 7:53:16	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
05/05/2009 7:56:56	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
05/05/2009 17:53:42	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
04/05/2009 7:54:15	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA		
30/04/2009 16:25:37	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
29/04/2009 16:31:59	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
28/04/2009 16:26:47	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
27/04/2009 16:27:49	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
24/04/2009 16:28:26	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
23/04/2009 17:03:47	4	02-001-2525	NCL	1	0	REPORTE DE CIERRE		
19/05/2009 16:27:18	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
18/05/2009 16:28:19	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
15/05/2009 16:25:29	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
14/05/2009 16:32:18	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
13/05/2009 16:23:25	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
12/05/2009 16:25:59	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
11/05/2009 16:25:37	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
08/05/2009 16:43:58	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		
07/05/2009 16:34:21	4	02-001-2525	NCL	1	1	REPORTE DE CIERRE		

Operator | Turno Dia | Logged in at | 20/05/2009 15:22:42 | Events | 1 | ACKed | 938 | IP: 10.1.8.28 | MAC: 10-B6-04-04-EC-09 | IP Active

Figura 4.18 *Pantalla de monitoreo con notificación de Alarma de Pánico*

El siguiente paso es reconocer el evento (Figura 4.19), el cual, y en este caso, a más de mostrar la “Alarma de Pánico” muestra la “Alarma de Pánico

Restaurada", es decir, los eventos de activación y desactivación de los botones de pánico por parte del personal de la agencia de recaudación.

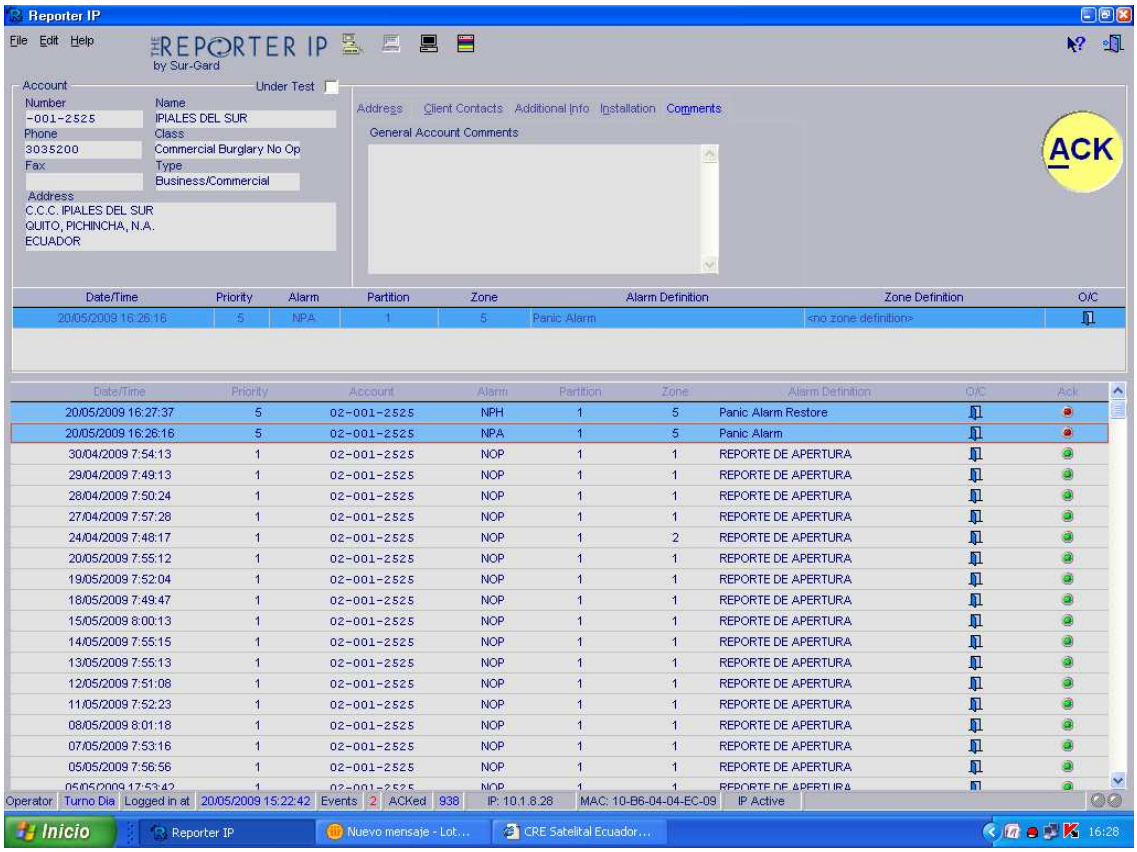


Figura 4.19 *Pantalla para reconocimiento de evento*

Como muestra de mejor manera la Figura 4.20, el evento de "Alarma de Pánico" ocurrió a las 16:26:16, y la desactivación del mismo, es decir, el levantamiento del botón de pánico presionado, a las 16:27:37.

Date/Time	Priority	Account	Alarm	Partition	Zone	Alarm Definition
20/05/2009 16:27:37	5	02-001-2525	NPH	1	5	Panic Alarm Restore
20/05/2009 16:26:16	5	02-001-2525	NPA	1	5	Panic Alarm
30/04/2009 7:54:13	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA
29/04/2009 7:49:13	1	02-001-2525	NOP	1	1	REPORTE DE APERTURA

Figura 4.20 *Eventos de la Alarma de Pánico*

A continuación, y de igual forma que lo realizado en la prueba de vida del sistema, se procede con el reconocimiento de los eventos, mismos que son mostrados a través de las Figuras 4.21 y 4.22

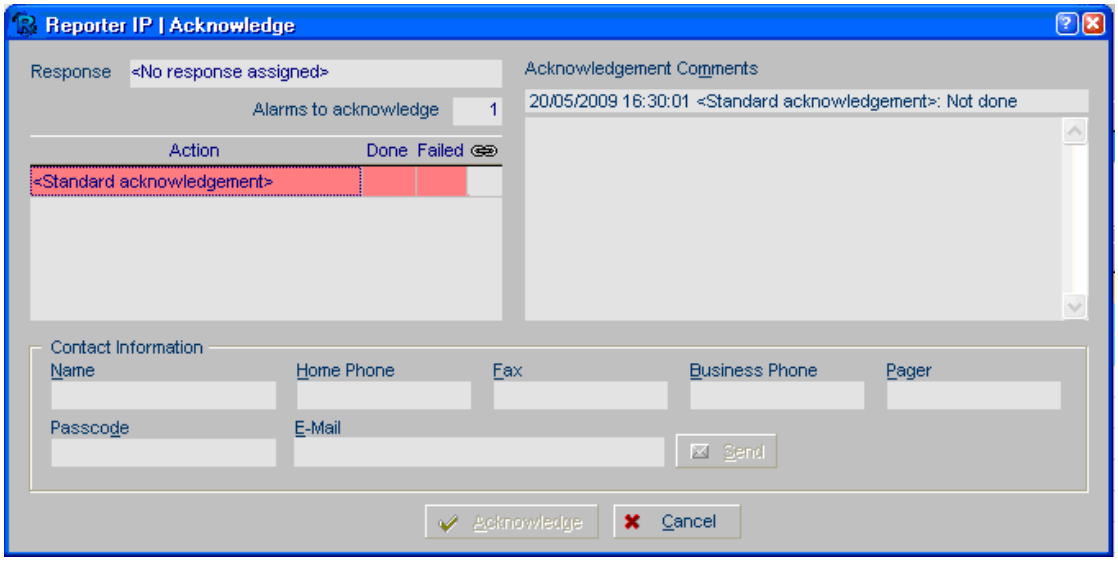


Figura 4.21 *Pantalla emergente para reconocimiento de evento*

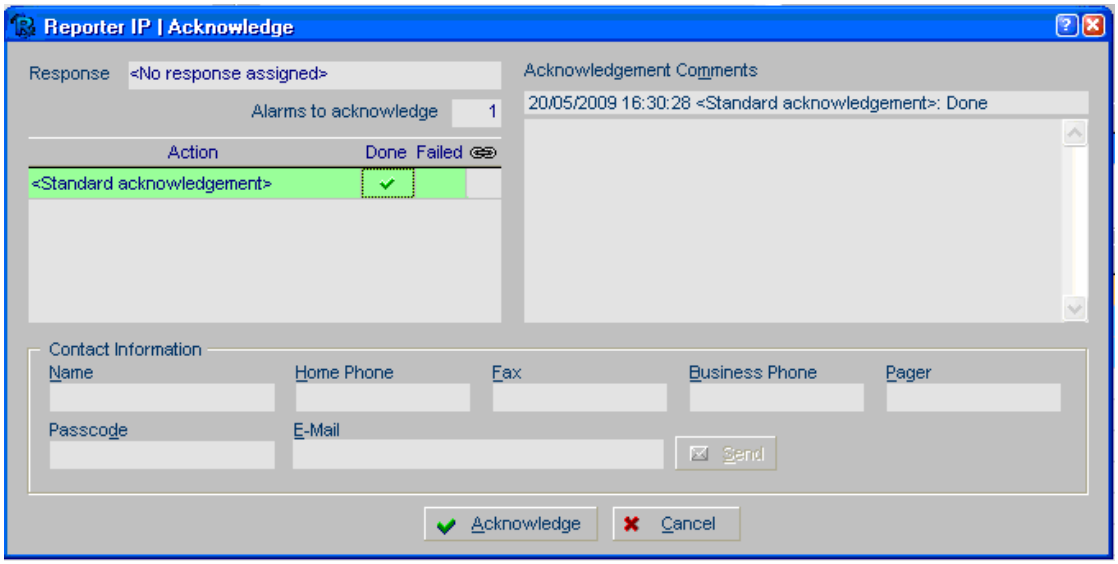


Figura 4.22 *Reconocimiento normal realizado*

4.2.3 PRUEBA DE BOTÓN DE PÁNICO INALÁMBRICO

El botón de pánico inalámbrico fue probado en el exterior de la dependencia, a una distancia aproximada de 10 metros (comprendida entre receptor inalámbrico y dispositivo transmisor).

Inmediatamente tras aplicar la señal, al software Reporter le llega la alarma de “Panic Alarm”y a continuación de la misma: “Panic Alarm Restore”. Aquí debe mencionarse que la restauración del evento, tal como lo muestra la

Figura 4.23 es inmediata, debido a que el tiempo entre las acciones: Panic Alarm y Panic Alarm Restore es el tiempo que al guardia de seguridad, en un evento real, le tomaría mantener pulsado el botón de accionamiento de la alarma.

Figura 4.23 *Eventos de pánico inalámbrico*

A continuación, se procedió a reconocer el evento como prueba con el respectivo comentario del mismo, tal como lo muestra la Figura 4.24.

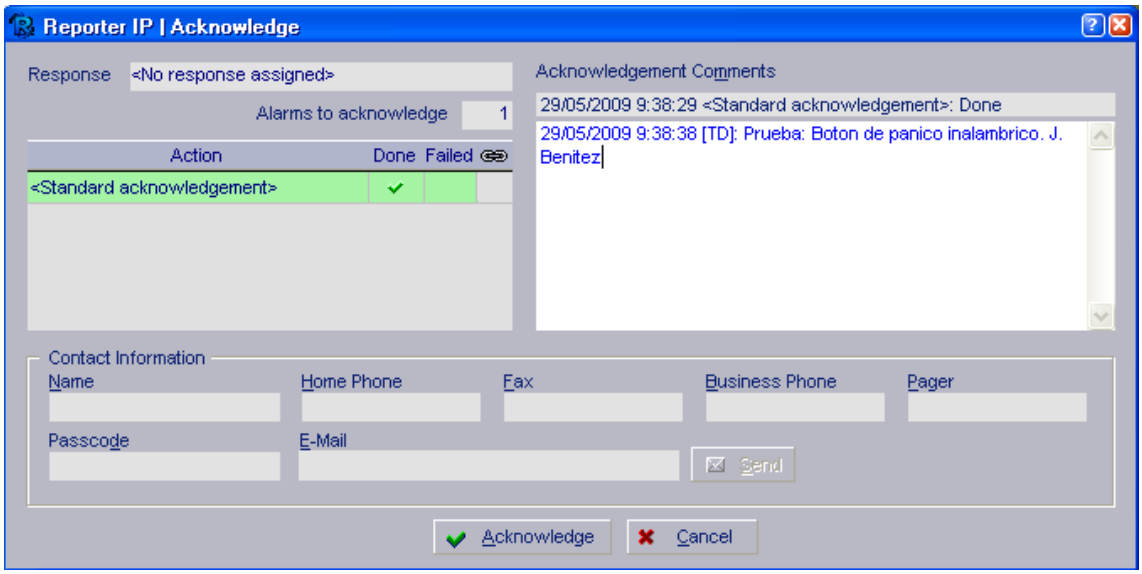


Figura 4.24 *Reconocimiento del evento "Botón de Pánico Inalámbrico"*

4.2.4 PRUEBA DE REPORTE DE CIERRE

El reporte de cierre consiste en una notificación del evento de armado del sistema por parte del personal de la agencia de recaudación.

La prueba fue realizada el día 20 de mayo de 2009, a las 16:28 PM, tal como lo muestra la Figura 4.25.

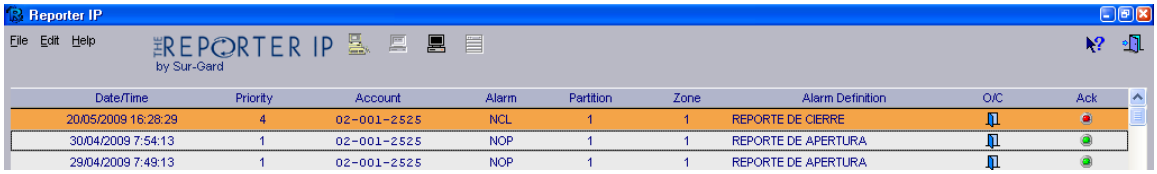


Figura 4.25 *Pantalla de monitoreo con notificación de Reporte de cierre*

Al igual que los Automatic Test y las pruebas de botones de pánico, se debe reconocer el evento, este procedimiento es el mismo que el efectuado en los otros acontecimientos, por lo cual, no se detallará el mismo pero si se mostrarán las figuras de las actividades realizadas. (Figura 4.26 y 4.27)

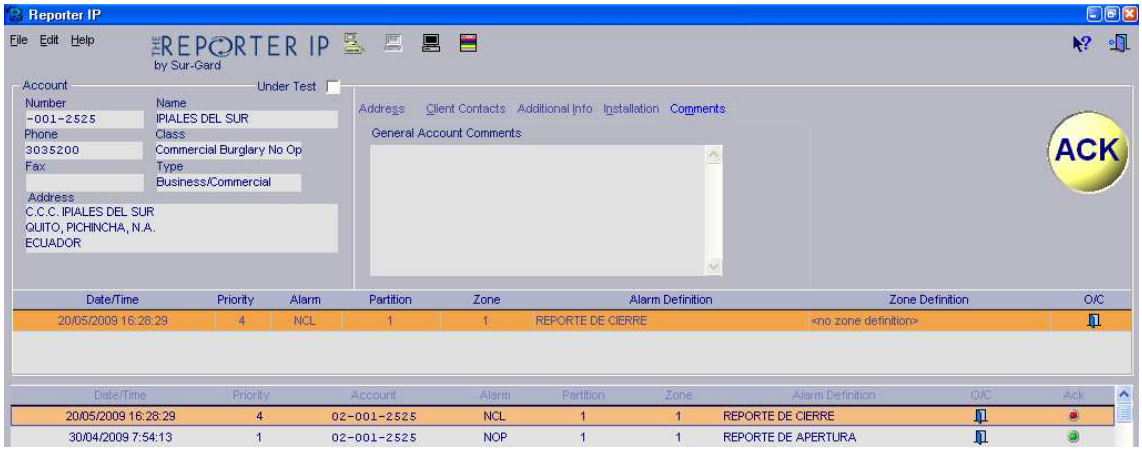


Figura 4.26 *Pantalla de reconocimiento de Reporte de Cierre*

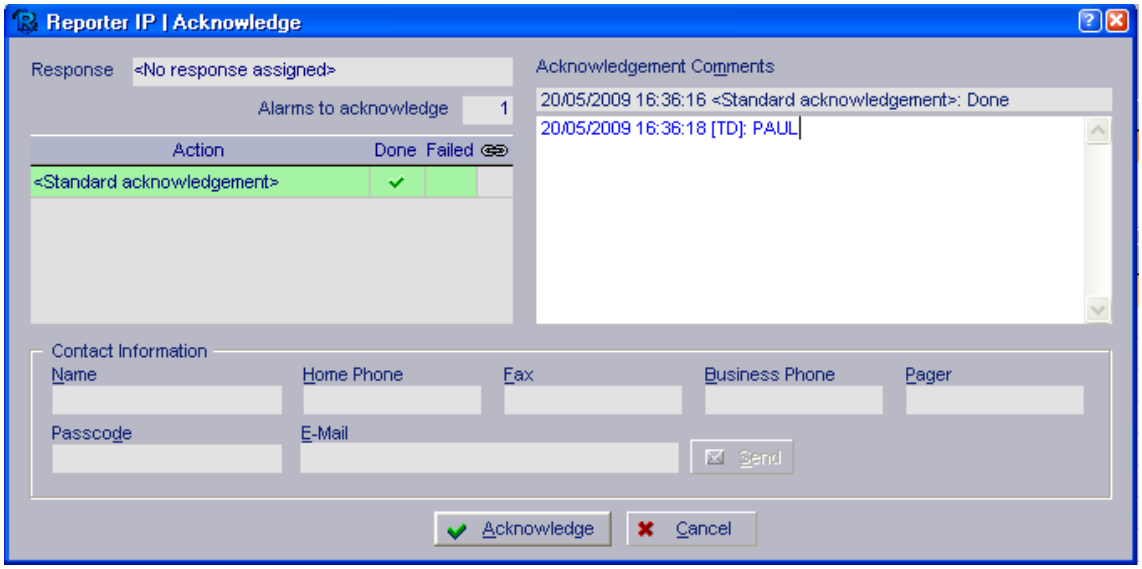


Figura 4.27 *Pantalla emergente de reconocimiento*

4.2.5 PRUEBA DE REPORTE DE APERTURA

El Reporte de Apertura informa que el personal que desarrolla sus labores cotidianas ha ingresado a la agencia de recaudación, y como procedimiento, ha desactivado el sistema de alarma de la dependencia.

La prueba de Reporte de Apertura que se detallará a continuación se ejecutó el día 22 de mayo de 2009, a las 7:52:18 AM, tal como lo muestra la Figura 4.28

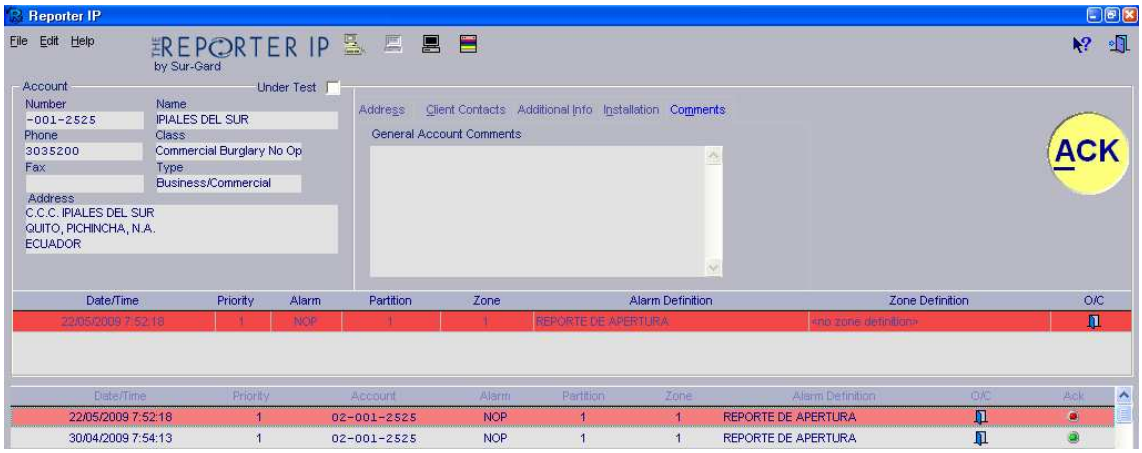


Figura 4.28 *Pantalla de monitoreo con notificación de Reporte de apertura*

El reconocimiento de la misma se detalla en la Figura 4.29.

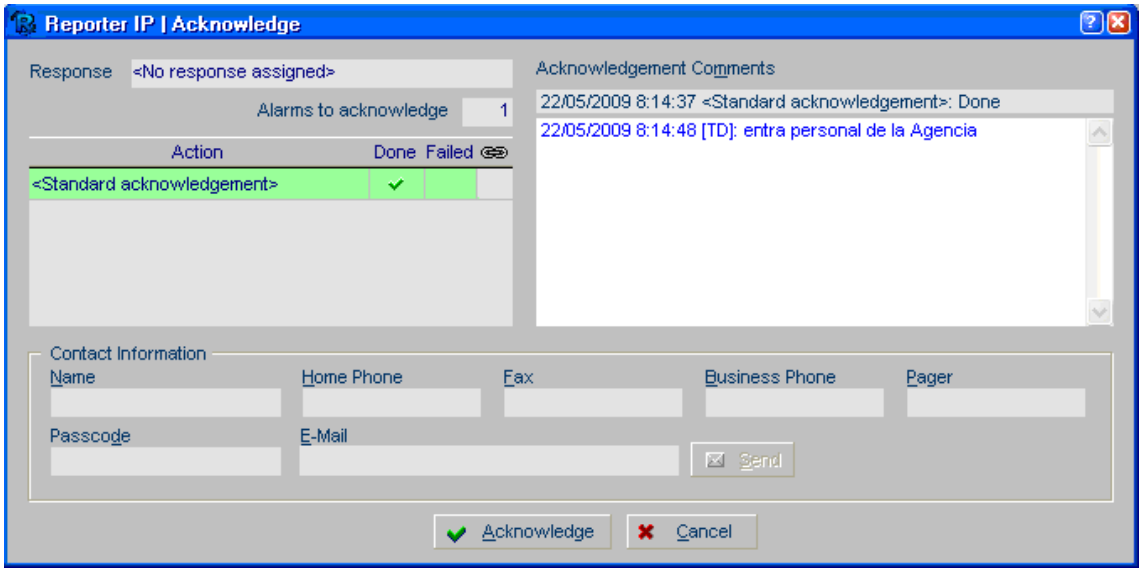


Figura 4.29 *Reconocimiento del evento Reporte de Apertura*

4.2.6 PRUEBA DE FALLO DE ENERGÍA

El sistema de monitoreo de alarmas instalado en la agencia de recaudación posee un sistema de alimentación de emergencia conformado por una batería de 7 amp/h. En esta prueba se desconectará la alimentación eléctrica y se probará la correcta transmisión de la novedad a la central de monitoreo y el tiempo de duración de funcionamiento de todos los dispositivos con esta fuente de energía de back up.

Siendo las 15:55:53 PM del día 21 de mayo de 2009 se procedió a desconectar la alimentación AC directa del panel de control, mostrándose inmediatamente, tal cual lo muestra la Figura 4.30, el detalle del mencionado evento en la pantalla de monitoreo con la denominación: AC Trouble (Problema de alimentación AC).

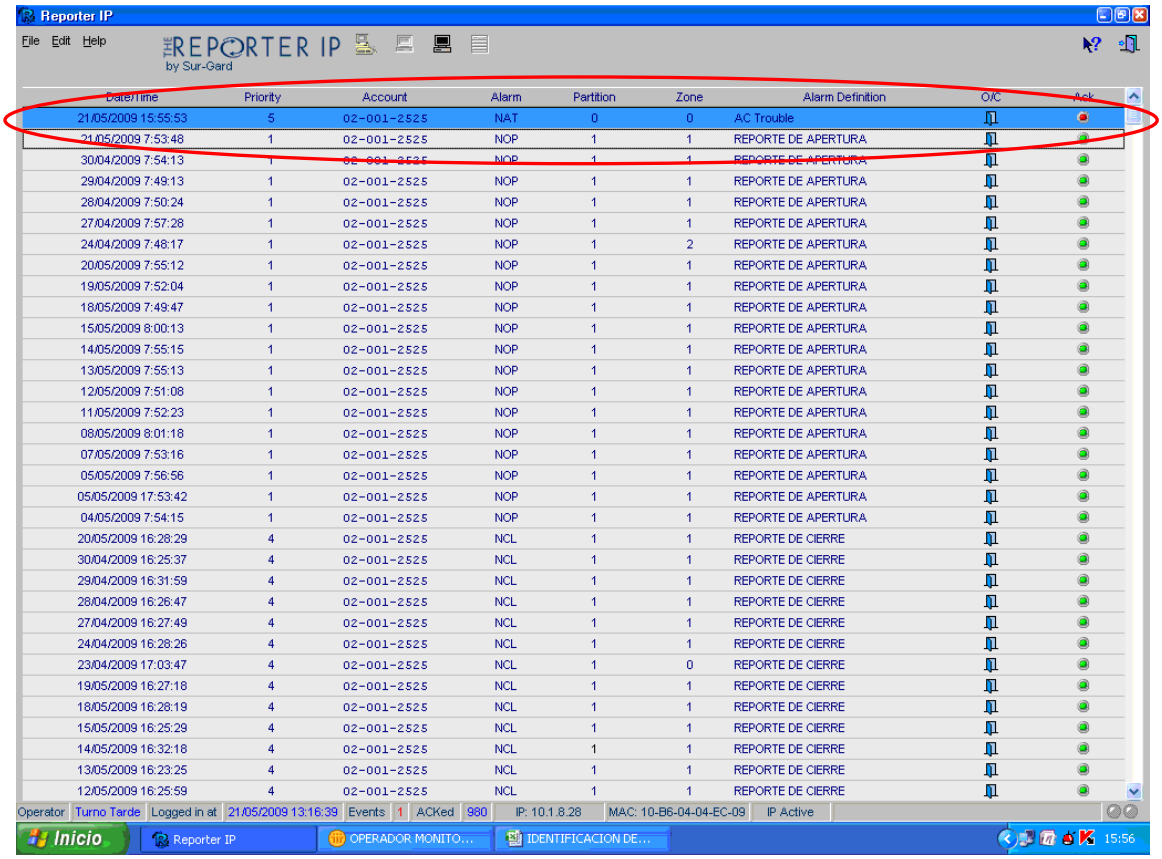


Figura 4.30 *Pantalla de monitoreo con novedad AC Trouble*

Tal cual se ha detallado anteriormente, el siguiente paso en el procedimiento debe ser reconocer el evento; para este caso, mostrado en las Figuras 4.31 y 4.32.

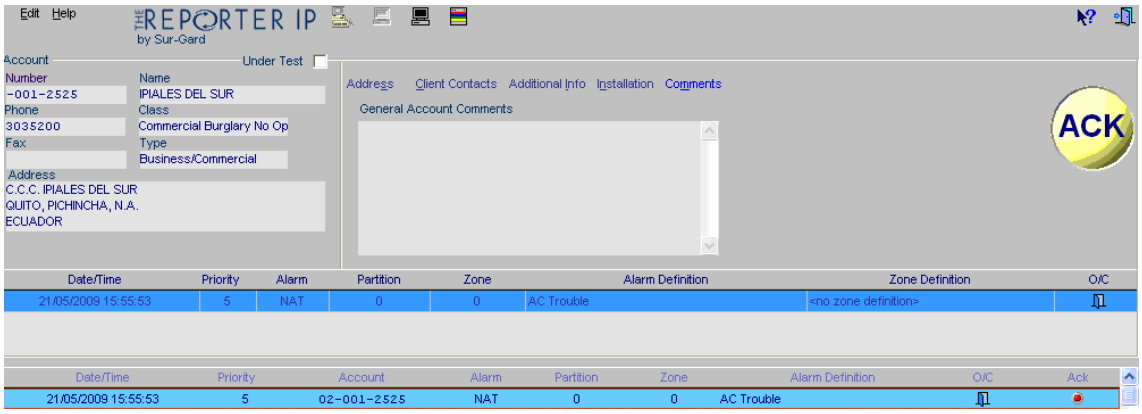


Figura 4.31 *Pantalla de reconocimiento alarma AC Trouble*

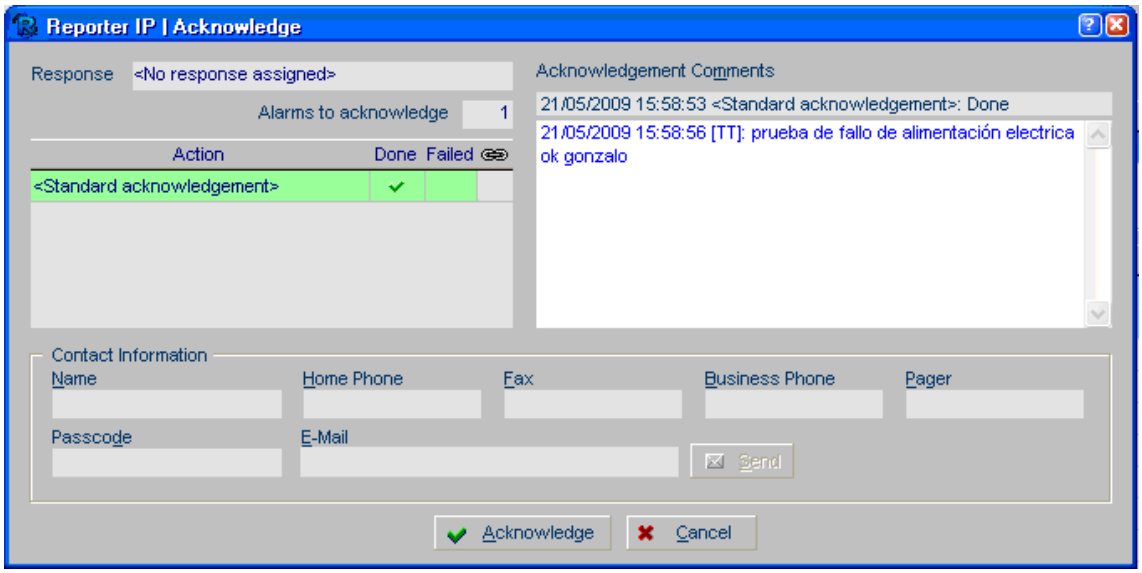


Figura 4.32 *Reconocimiento alarma AC Trouble con comentario por parte del monitor*

En espera de obtener la información la cual alerte el tiempo de duración de la batería, se procedió a esperar y recibir las últimas notificaciones de funcionamiento normal del equipo.

El día 22 de Mayo de 2009, es decir, un día después a la desconexión, se recibió dos eventos sobre la pantalla de monitoreo con relación a la finalización de la batería de emergencia. El primer evento: System Battery

Trouble, alertando la falla del sistema, se presento a las 19:44:52, tal como lo muestra la Figura 4.33.

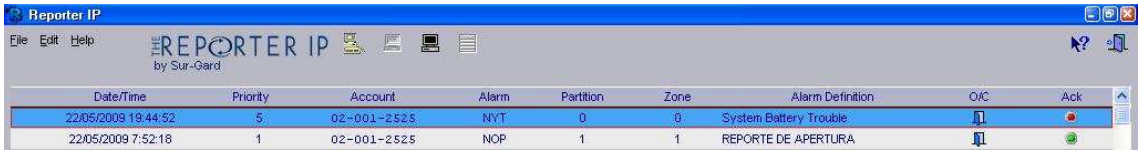


Figura 4.33 *Pantalla de monitoreo con evento System Battery Trouble*

El segundo evento consistió en el último Automatic Test o prueba de vida del sistema, mismo que fue recibido a las 20:01:25 PM, tal como lo muestra la Figura 4.34.

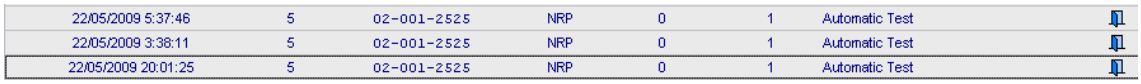


Figura 4.34 *Pantalla de monitoreo con evento Ultimo Automatic Test*

Adicionalmente, cabe señalarse que el sistema fue reconectado a la alimentación AC el día lunes 25 de Mayo de 2009 a las 7:59, iniciando nuevamente sus funciones de monitoreo y reporte.

4.2.7 REVISIÓN DE HISTORIAL

El primer paso a seguirse es cambiar el usuario que está trabajando en la central de monitoreo, esto debido a que solamente el Administrador del sistema es la única persona capacitada y con suficientes privilegios para realizar dicha actividad.

Siendo así, se procede a ejecutar un Log out (salida del sistema), confirmar dicha acción e iniciar a su vez un Log in (entrada al sistema) con los datos del administrador del sistema. En este caso:

Login: administrador, **Password:** administrador

Tal como se detalló anteriormente, se despliega una nueva lista de comandos, sobre la cual, se elige la opción comando **History**, acción que se detalla de mejor manera en la Figura 4.35, esperando de esta manera que se ejecute el mismo y se despliegue una pantalla emergente con los datos a ser llenados por el Administrador.

Figura 4.35 *Iconos de History*

Estos datos determinarán de que panel se desea realizar la búsqueda, de que fecha a que fecha y que tipo de evento es el que se desea buscar en el mencionado historial (Figura 4.36).

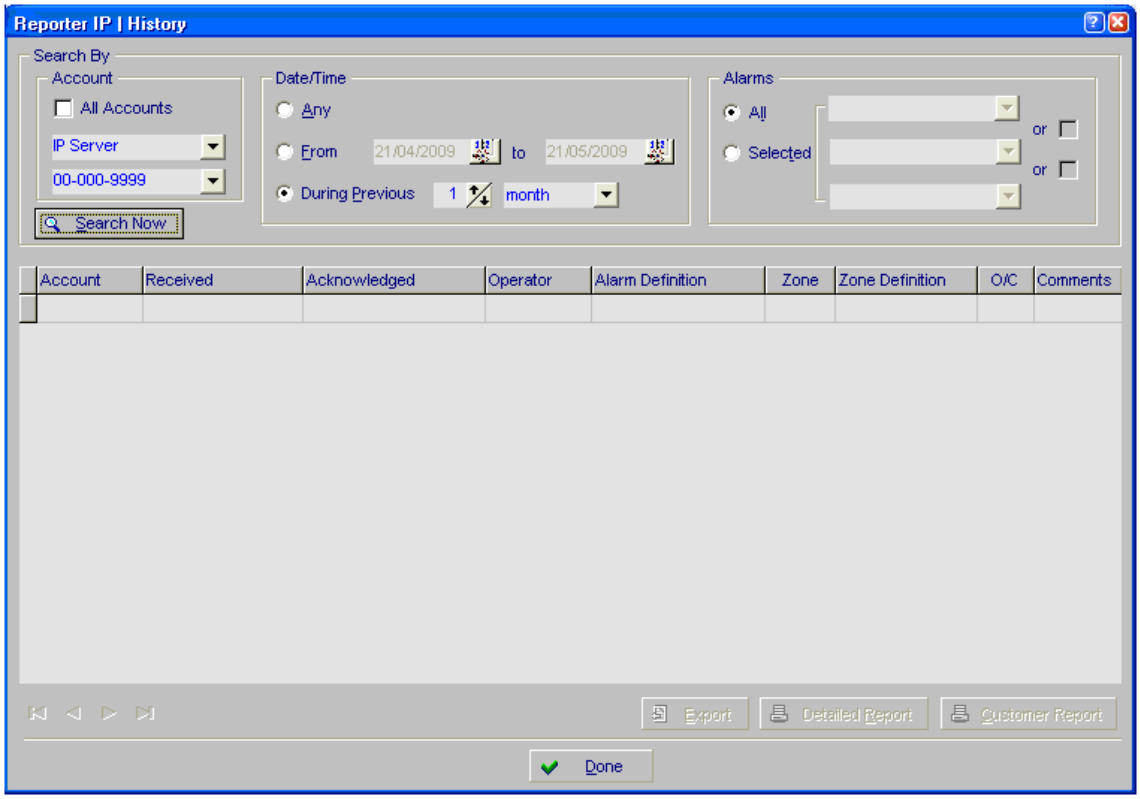


Figura 4.36 *Cuadro de dialogo para obtención del historial*

Como prueba en la obtención de un historial deseado, se procedió a llenar el cuadro de diálogo con la cuenta: IPIALES DEL SUR, con las fechas referenciales:

Desde: 21/05/2009 hasta: 21/05/2009

Y con la clasificación de tipo de eventos: All (todos).

El cuadro de diálogo con toda esta información de búsqueda y los resultados encontrados se denota en la Figura 4.37.

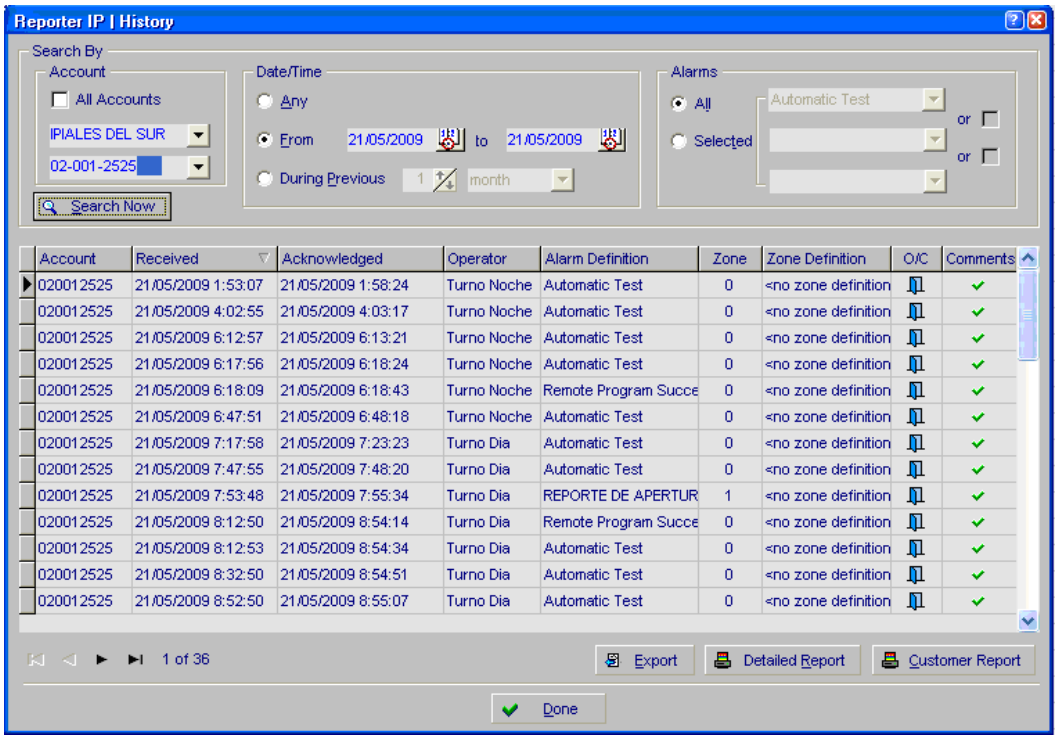


Figura 4.37 *Cuadro de dialogo con historial deseado*

4.2.7.1 Exportación de historial a archivo XLS

Este procedimiento consiste en exportar el historial obtenido siguiendo el procedimiento detallado en el punto anterior a un archivo tipo XLS (ejecutable de Microsoft Office Excel). El único paso adicional, será ejecutar el comando “Export”, localizado en la parte inferior de la Figura 4.31 “Cuadro de dialogo con historial deseado”, esperando que a su vez se presente una ventana emergencia la cual solicita el destino y el nombre del archivo en formato XLS a guardarse, tal como lo muestra la Figura 4.38

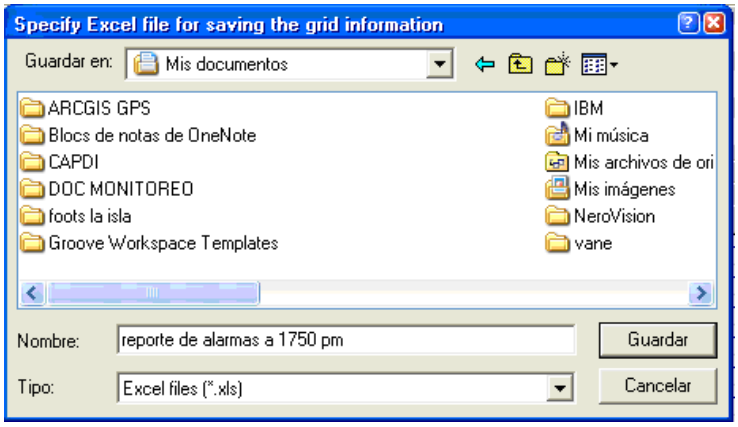


Figura 4.38 *Ventana emergente para exportar historial a formato xls*

El historial ya exportado a Excel se mostrará con la estructura mostrada en las Figura 4.39 y 4.40, siendo la última de éstas la continuación de la primera.

	A	B	C	D	E	F	G	H
1	Reporter IP | History Report							
2	21/05/2009 17:51:12							
3								
4	Account	Account Name	Received	Acknowledged	Operator	Alarm Definition	Zone	Zone Definition
5	20012525	IPIALES DEL SUR	21/05/2009 1:53:07	21/05/2009 1:58:24	Turno Noche	Automatic Test	0	<no zone definition>
6	20012525	IPIALES DEL SUR	21/05/2009 4:02:55	21/05/2009 4:03:17	Turno Noche	Automatic Test	0	<no zone definition>
7	20012525	IPIALES DEL SUR	21/05/2009 6:12:57	21/05/2009 6:13:21	Turno Noche	Automatic Test	0	<no zone definition>
8	20012525	IPIALES DEL SUR	21/05/2009 6:17:56	21/05/2009 6:18:24	Turno Noche	Automatic Test	0	<no zone definition>
9	20012525	IPIALES DEL SUR	21/05/2009 6:18:09	21/05/2009 6:18:43	Turno Noche	Remote Program Success	0	<no zone definition>
10	20012525	IPIALES DEL SUR	21/05/2009 6:47:51	21/05/2009 6:48:18	Turno Noche	Automatic Test	0	<no zone definition>
11	20012525	IPIALES DEL SUR	21/05/2009 7:17:58	21/05/2009 7:23:23	Turno Dia	Automatic Test	0	<no zone definition>
12	20012525	IPIALES DEL SUR	21/05/2009 7:47:55	21/05/2009 7:48:20	Turno Dia	Automatic Test	0	<no zone definition>
13	20012525	IPIALES DEL SUR	21/05/2009 7:53:48	21/05/2009 7:55:34	Turno Dia	REPORTE DE APERTURA	1	<no zone definition>

Figura 4.39 *Ventana emergente para exportar historial a formato xls*

I	J	K
O/C	Comments	
Opened	21/05/2009 1:58:02 [TN]: PRUEBA DE VIDA ROBERTO	
Opened	21/05/2009 4:03:09 [TN]: PRUEBA DE VIDA ROBERTO	
Opened	21/05/2009 6:13:11 [TN]: PRUEBA DE VIDA ROBERTO	
Opened	21/05/2009 6:18:15 [TN]: PRUEBA DE VIDA ROBERTO	
Opened	21/05/2009 6:18:37 [TN]: PROGRAM SUCES	
Opened	21/05/2009 6:48:10 [TN]: PRUEBA DE VIDA ROBERTO	
Opened	21/05/2009 7:23:08 [TD]: prueba de vida wilson	
Opened	21/05/2009 7:48:05 [TD]: AUTOMATIC TEST WILSON	
Opened	21/05/2009 7:54:51 [TD]: DESACTIVA LA ALARMA PA EL INGRESO EN IPIALES DEL SUR OK WILSON	

Figura 4.40 *Ventana emergente para exportar historial a formato xls*

4.2.8 PRUEBA DE BOTONES DE PÁNICO DEL TECLADO

A continuación se detallarán las pruebas realizadas a los tres botones de pánico pertenecientes al teclado de control del sistema (Incendio, emergencia médica y robo en proceso) (Figura 4.41)

Figura 4.41 *Botones de pánico del teclado*

4.2.8.1 Prueba de Alarma de Incendio

El día 29 de Mayo de 2009, a las 9:49 AM, se procedió a probar el botón de pánico de evento “Incendio”, mismo que para ser activado, requirió de ser presionado por dos segundos hasta emitir el pitido de confirmación de transmisión del evento. La Figura 4.42 muestra el evento sobre la pantalla de monitoreo con el texto “Fire Alarm”, así como, la Figura 4.43 muestra el reconocimiento del mismo.

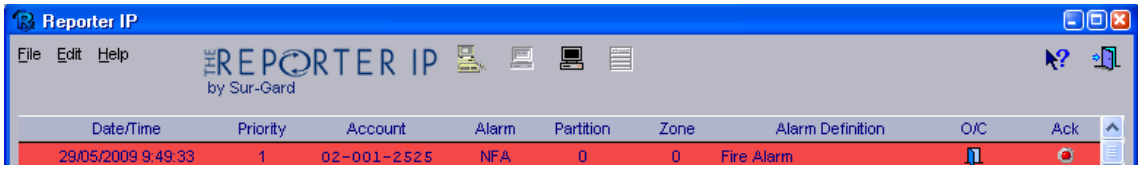


Figura 4.42*Evento de Alarma de Incendio*

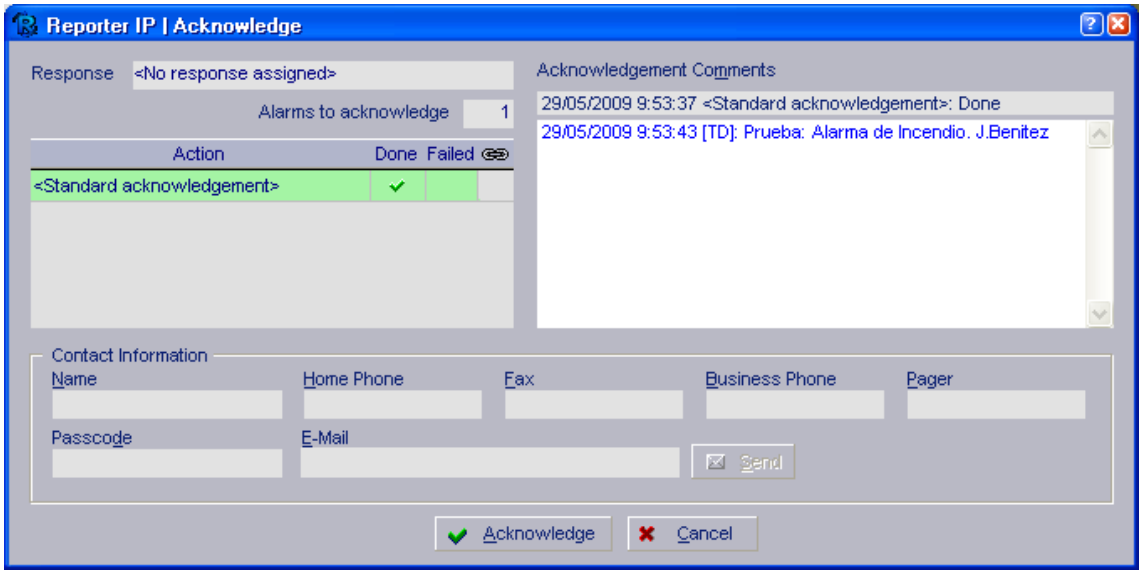


Figura 4.43 *Reconocimiento de la prueba de Incendio*

4.2.8.2 Prueba de Emergencia Médica

A continuación de la prueba de Alarma de Incendio, se procedió a realizar la prueba de emergencia médica, misma que dio inicio a las 9:56 AM, con la respectiva transmisión de la señal tras presionar el botón correspondiente por dos segundos y confirmar por el pitido de teclado la transferencia del evento a la central de monitoreo, con el texto de evento: “Medical Alarm”. (Figura 4.44)

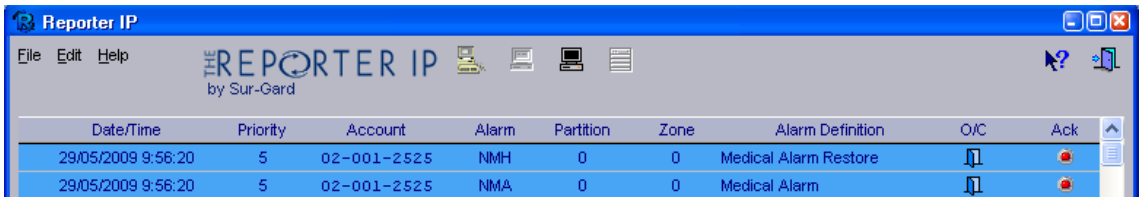


Figura 4.44 *Evento de Emergencia Médica*

El reconocimiento del mismo consto de su respectivo comentario, tal como se muestra en la Figura 4.45

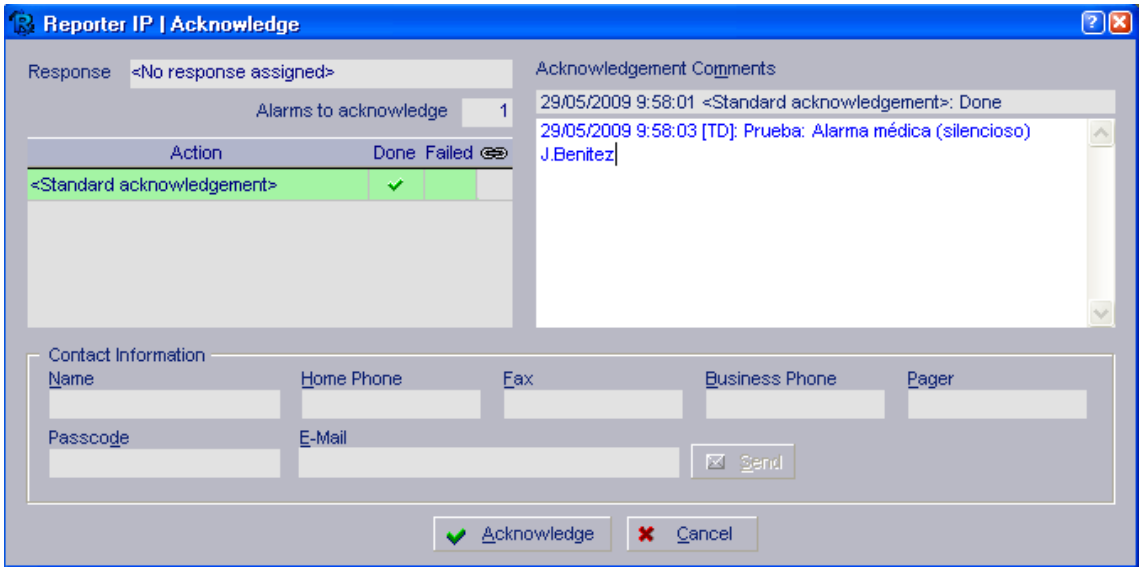


Figura 4.45 *Reconocimiento de la prueba Emergencia Médica*

4.2.8.3 Prueba de Robo en Proceso

Ya para finalizar las pruebas de los comandos de emergencia del teclado, a las 10:04 AM, se procedió a enviar la prueba de robo en proceso a través del botón de pánico del teclado, mismo que llegó a la central de monitoreo con el texto: “Panic Alarm”, tal como se muestra en la Figura 4.46.

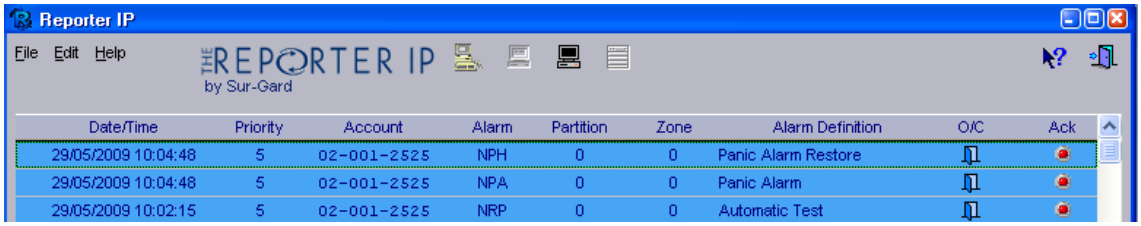


Figura 4.46 *Evento de Alarma de Pánico*

El reconocimiento del evento con su respectivo comentario se muestra en la Figura 4.47

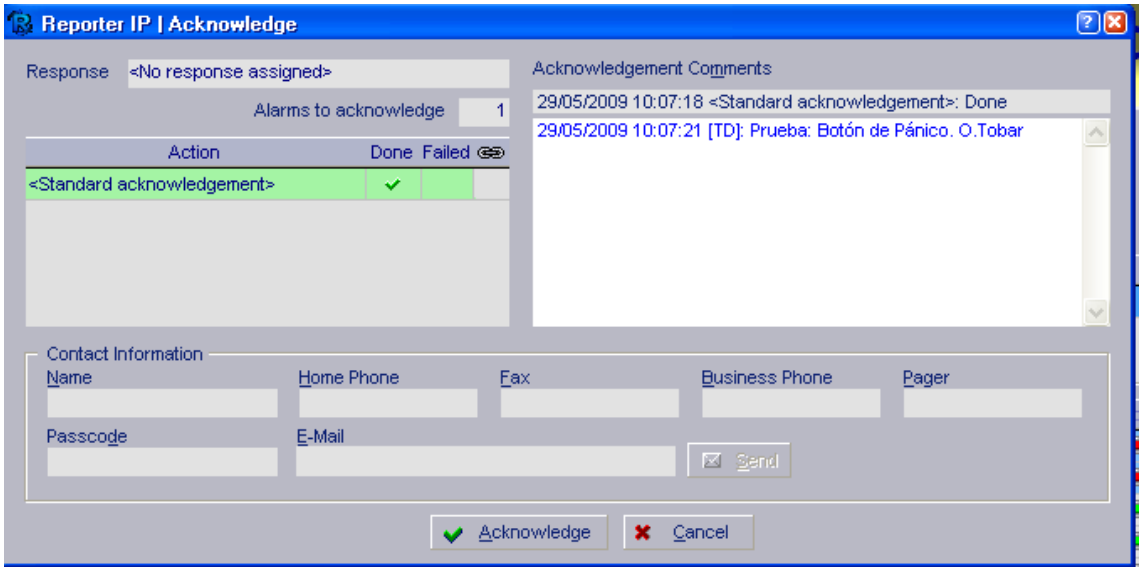


Figura 4.47 *Reconocimiento del Botón de Pánico*

CAPITULO 5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Se realizó el análisis, diseño e implementación del sistema de seguridad electrónica para una Agencia de Recaudación de la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito, con una comunicación vía TCP/IP a la Matriz de la misma.

- La EMAAP-Q no pudo completar la implementación de este proyecto en las 15 agencias de recaudación debido a cuestiones financieras, las cuales, afectaron directamente la puesta en marcha del sistema de seguridad electrónica propuesto.

- El Departamento de Seguridad Física y Radio Comunicaciones, como representante de la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito en el área de seguridad electrónica, revisó el proyecto presentado y lo aprobó en su totalidad.

- En la agencia de recaudación Ipiales del Sur, de la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito, se ha instalado con éxito un sistema de seguridad electrónica, el cual, contempla todos los dispositivos necesarios para cumplir su funcionalidad planteada a cabalidad.

- El sistema presentado realiza un papel muy importante en la seguridad de la agencia de recaudación, pero siempre deberá ir acompañado de otras medidas extras, como lo son: cerraduras de seguridad, puertas blindadas, cristales blindados, y por supuesto, costumbres y medidas personales de seguridad a adoptarse por todos quienes conforman la EMAAP-Q.

- La costumbre del buen uso de este sistema por parte del personal de las agencias de recaudación es sumamente importante, así como, recordarles a éstos de la activación del mismo, mantenerlo en buen estado, informar cualquier inconveniente al Departamento de Seguridad Física y Radiocomunicaciones de la EMAAP-Q y, mantener las contraseñas de habilitación o desactivación del sistema personales.

- Se debe tomar en cuenta que al instalar un sistema de seguridad electrónica en determinado lugar, no se puede asegurar que este se encuentre libre de sufrir un atentado delincuencial o algo similar, el sistema de seguridad cumple la función de ayudar a informar a las personas pertinentes (central de monitoreo) lo que está ocurriendo en el lugar, y que la posible emergencia debe ser atendida inmediatamente.

- La respuesta armada por parte de una compañía de seguridad privada a una emergencia suscitada en este tipo de sistemas, misma que se compromete a llegar al punto crítico en un lapso comprendido de 5 a 10 minutos, resulta una opción práctica a ser implementada, razón por la cual, la EMAAP-Q está realizando los análisis necesarios para la contratación de la misma cuando el proyecto se encuentre finalizado en su totalidad.

- Dentro de las pruebas realizadas se encontró que a más de entrenar al personal directo de la EMAAP-Q, como lo son los cajeros, se llegó a la conclusión de que es sumamente necesario capacitar a los guardias de seguridad y al personal que realiza el mantenimiento en la agencia donde se encuentre funcionando el sistema de seguridad, tanto en simulacros de asaltos como posibles enfrentamientos para evitar lesiones o perdidas humanas.

- Ahora en el mercado existen muchos equipos que se usan para aplicaciones de alarmas de seguridad, pero se debe tener en cuenta que los equipos electrónicos están en constante innovación; es por esto que al realizar la adquisición de estos equipos se debe hacer un análisis de la

utilidad que se tendrá a futuro, ya que luego estos serán obsoletos y no se encontrará repuestos, por que las casa fabricantes paran su producción.

- Los equipos que se usaron en el proyecto cumplen con los objetivos planteados y se puede comprobar la funcionalidad del sistema con estos dispositivos, aunque estos equipos no cumplen sólo con la característica de que sean integrados con el sistema de circuito cerrado de televisión y sistema de control de accesos que se hacían referencia en el diseño.

- El sistema de seguridad electrónica funciona de acuerdo a lo esperado y se pudo comprobar el funcionamiento que se tiene en red entre la agencia de recaudación y la matriz de la empresa, la diferencia radica en que si se hubiera implementado el sistema de seguridad electrónica en todas las agencias el flujo de información sería mucho mayor, pero se esperaba que no existiera ningún conflicto en el flujo de información ya que los datos que envía y recibe el sistema de alarma son muy pequeños en comparación al ancho de banda que posee la empresa.

5.2 RECOMENDACIONES

Las recomendaciones que a continuación se presentan describen los inconvenientes presentados en la implementación de este proyecto y las soluciones prestadas a los mismos.

- Debido a que la Empresa Metropolitana de Alcantarillado y Agua Potable de Quito no pudo concretar la instalación y puesta en marcha del sistema por cuestiones financieras, se tuvo que adquirir directamente todos los dispositivos necesarios para demostrar y cumplir el objetivo planteado en el tema de tesis. Razón por la cual, se recomienda a los futuros tesistas contar con el factor presupuesto antes de planificar o elaborar el tema de tesis.

- Dentro de la comunicación ADSL entre el panel de control perteneciente a la agencia Ipiales del Sur y la central de monitoreo en el edificio matriz se tuvo serios inconvenientes en permitir que la misma sea continua, esto debido al sistema de protección Firewall Astaro de la EMAAP-Q, y de igual forma, por las restricciones internas para la instalación de programas y configuración de los mismos sin los respectivos permisos por parte del Departamento de Recursos Informáticos. Para evitar todos estos inconvenientes se tuvo que solicitar a los supervisores de redes que permitan y otorguen accesos totales como administrador hasta poder finalizar las instalaciones y configuraciones necesarias, para posteriormente, volver a subir la barrera de protección firewall del acceso Ipiales del Sur.

- En los sistemas electrónicos de este tipo siempre se debe contemplar utilizar una vía alterna de comunicación, la cual deberá funcionar como un respaldo a los datos que se vayan a transmitir por su vía principal. En este proyecto se recomendó a la EMAAP-Q la implementación del mismo, pero debido a que esta empresa planificó el desarrollo del proyecto con el único fin de abaratar costos, no le interesó el mencionado respaldo de comunicación.

- Un punto muy importante que se debe siempre tener en cuenta es que estos sistemas de seguridad electrónica así como todos los sistemas electrónicos o dispositivos electrónicos necesitan tener un mantenimiento periódico para su óptimo funcionamiento, por tal motivo se recomienda realizar un cronograma para realizar pruebas del equipo y estar seguro de que los dispositivos están trabajando adecuadamente.

- Se debe tener en cuenta que los sucesos de emergencias no ocurren a menudo, es por esta razón que se debería realizar un simulacro de emergencia cada cierto tiempo para que el personal que trabaja esté capacitado a tomar las acciones y precauciones necesarias en estos casos.

- El Departamento de Seguridad Física de la EMAAP-Q debería realizar un manual de procedimientos para el personal que realice el monitoreo del sistema de alarmas de seguridad de forma que cuando ocurra una emergencia ellos sepan los pasos que deben seguir para que la misma sea atendida de inmediato. Además también se deberían realizar simulacros para que las personas que monitoreen estén capacitadas para seguir el procedimiento con eficacia y eficiencia. Además se debería realizar simulacros de manera que se compruebe la capacitación del personal.

REFERENCIAS BIBLIOGRAFICAS

- Honeywell Security & Custom Electronics, Catálogo 2006

- Nassau Security: http://nassausecurity.com/store/shopexd.asp?id=1145

- Manual de instrucciones PC5020: www.dsc.com/download.php?t=1&id=10069

- http://sumanual.com/instrucciones-guia-manual/DSC/PC5020-_E

- SourceSecurity:http://www.sourcesecurity.com/new-products/listing/1/product-profile/intruder-alarms/communicators.1/communicators/dsc-t-link-tl250.html

- Manual de Instrucciones, DSC Power 864 Security System, DSC 2000 Digital Security Controls Ltd., Toronto-Canadá, www.dsc.com, Printed in Canadá 29005222 R001.

- Manual de Instalación, DSC Power 864 Security System, DSC 2000 Digital Security Controls Ltd., Toronto-Canadá, www.dsc.com, Printed in Canadá 29005223 R001

- Hojas de Programación, DSC Power 864 Security System, DSC 2000 Digital Security Controls Ltd., Toronto-Canadá, www.dsc.com, Printed in Canadá 29005224 R001

- The Reporter Software Package, SG Security Communications User Manual, Downsview, Ontario Canadá M3J 3H9

- http://www.marshalllocksystems.com.ar/catalogo-alarmas.pdf