ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

TÓPICO DE GRADUACIÓN

TRANSMISIÓN MULTIMEDIA SOBRE IP

Tema:

DISEÑO DE UN SISTEMA INALÁMBRICO DE SEGURIDAD APLICADO A LA URBANIZACIÓN "PUNTA PANORAMA" UTILIZANDO TRANSMISIÓN MULTIMEDIA SOBRE IP

Presentado por:

DENISE IÑIGUEZ

VERÓNICA MEDINA

ADOLFO CAMPUZANO

Director:

Ing. Édgar Leyton

Guayaquil – Ecuador

2006

AGRADECIMIENTO

Agradezco a Dios, a mis padres, profesores y amigos.

Adolfo

Agradezco a Dios, a mis padres, a mi esposo, a mis hermanas, a mis suegros, a mis profesores y a mis compañeros por toda la ayuda brindada en los momentos más necesitados.

Denise

Agradezco a Dios; a los ingenieros Iñiguez, Bravo y Barragán, y Arq. Flores por la información y conocimientos facilitados para el desarrollo del proyecto. Y al Ing. Leyton por la guía realizada para el presente trabajo.

Verónica

DEDICATORIA

A Dios, a mi querida Abuela que desde el cielo guía mis pasos, a mi Madre, a mi Hermana, a mi querida Elva y a mis dos amados hijos: Rommel y Nadége.

Adolfo

Esta tesis esta dedicada para mi hermana Daysi, mis hijos Vicente, Nicolás y Milena, y a mis sobrinos.

Denise

A Dios, a mi esposo y a mis padres, por su apoyo incondicional y ayuda oportuna. Y a mis familiares por su granito de arena.

Verónica

TRIBUNAL DE GRADUACIÓN

ING. MIGUEL YAPUR
Subdecano de la FIEC

ING. EDGAR LEYTON
Director de Tópico

ING. FRANCISCO NOVILLO
Tribunal

ING. CÉSAR YÉPEZ
Tribunal

DECLARACIÓN EXPRESA

¨ La responsabilidad por los hechos, ideas y doctrinas expuestas en esta tesis, nos corresponden exclusivamente; y el patrimonio intelectual de la misma, a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL ¨

Verónica Alexandra Medina Sánchez

Denise Lorena Iñiguez Moreno

Adolfo Campuzano Yánez

RESUMEN

En este proyecto se van a establecer las bases del funcionamiento de un sistema de seguridad aplicado a una urbanización utilizando tecnología IP, como una alternativa a los servicios tradicionales de seguridad electrónica que al momento ofrecen las empresas especializadas en seguridad existentes en el mercado.

El proyecto se encuentra dividido en 5 capítulos en los que se exponen de forma ordenada los principios teóricos del diseño y funcionamiento del sistema propuesto. De esta forma.

En el Capítulo 1 se describirán conceptos básicos de los que son las redes de área local inalámbricas (WLAN), se empezará dando una explicación de su funcionamiento, el estándar que las define (IEEE 802.11), con todas sus aplicaciones, tecnologías, configuraciones y ventajas con respecto de las redes cableadas.

En este capitulo también se tratará de los protocolos asociados a los servicios de voz sobre IP (VoIP). Nuestro estudio se basará en el protocolo de señalización H.323, sus componentes y del establecimiento de una llamada H.323.

En el Capítulo 2 se hará un análisis de los sistemas de seguridad en el mercado para lo cual se exponen los conceptos básicos y generales concernientes a la seguridad, después se hará un estudio sobre la estructura de una empresa de seguridad y se culminará con la descripción de algunos sistemas de seguridad existentes en el mercado.

En el Capítulo 3 se hará una descripción de la ubicación geográfica de la urbanización, así como de su infraestructura y se hablará de la situación en que la empresa de seguridad actual se encuentra.

En el capítulo 4 se realizará una descripción de los equipos que se utilizarán en el desarrollo de este proyecto, sus características técnicas, configuración, etc. También se determinará la ubicación física de los mismos mediante los planos de la urbanización, y mediante un diagrama general del proyecto se hará una explicación de la funcionalidad del sistema de seguridad utilizando tecnología IP.

En el Capítulo 5 se realizará el análisis de la inversión del proyecto y cómo será financiado dicha inversión por medio del Banco Guayaquil, considerando que hay que basarse de los costos del mismo sistema actual pero eficiente, es decir, como debería ser para asegurarnos de la vigilancia de la urbanización.

ÍNDICE GENERAL

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

TABLA	DESCRIPCIÓN	PÁG

INTRODUCCIÓN

Las redes inalámbricas WLAN (Wireless Local Área Network), en los últimos años han ganado muchos adeptos y popularidad en mercados tales como bancos, hospitales, fábricas, bodegas, tiendas de autoservicios, tiendas, pequeños negocios y áreas académicas. Las redes inalámbricas permiten a los usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente en dicho lugar.

Con las redes inalámbricas, las redes eliminan la necesidad de usar cables, y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante incrementa la productividad y eficiencia en las actividades diarias de las empresas. Un usuario dentro de una red inalámbrica puede transmitir y recibir voz, datos y video dentro de edificios, o entre edificios, o en un campus universitario e inclusive sobre áreas metropolitanas.

El momento decisivo para la consolidación de estos sistemas, fue la conclusión del estándar IEEE 802.11. En este estándar, se encuentran las especificaciones tanto físicas como a nivel del MAC, las cuales hay que tener en cuenta a la hora de implementar una red de área local inalámbrica.

Las nuevas posibilidades que ofrecen las WLAN son: permitir una fácil incorporación de nuevos usuarios a la red, ofrecer una alternativa de bajo

costo a los sistemas cableados, además de la posibilidad para acceder a cualquier base de datos o a cualquier aplicación localizada dentro de la red.

Justamente, este proyecto tiene como finalidad el *Diseño de un sistema inalámbrico de seguridad aplicado a la urbanización Punta Panorama* utilizando tecnología multimedia sobre IP, según el estándar IEEE 802.11, específicamente el 802.11a definido para trabajar a velocidades de hasta 54 Mbps. Mediante este sistema los bienes de los propietarios de las viviendas podrán ser monitoreados desde el centro de gestión de seguridad.

Para la transmisión de las alarmas se utilizará un módulo de protocolo IP, el mismo que al instalarse en los paneles de control de alarmas en los domicilios nos permitirá el envío a través de una red IP, así también se hará uso de switches no gestionables para garantizar la conectividad de las cámaras que se instalarán en la urbanización y como también las interfaces para la telefonía IP.

El equipamiento inalámbrico que se utilizará para el diseño de la red, mediante el cual se transmitirá la información desde las viviendas hasta el centro de gestión, es de la marca BreezeCom, específicamente del modelo BreezeAccess VL, estos equipos incluyen un software monitor propietario del proveedor para la configuración de los equipos BreezeCom.

A continuación se da a conocer el presente trabajo esperando que en él se encuentre una guía para la implementación de nuevas redes de seguridad, que se adapten a las necesidades de los usuarios.

CAPITULO 1

CONSIDERACIONES TEÓRICAS DEL PROYECTO.

En este capitulo se describen conceptos básicos de lo que son las redes de área local inalámbricas (**WLAN**), la tecnología que utilizan, configuraciones y los estándares definidos por la norma IEEE 802.11.

Luego se realiza la descripción del protocolo de control de acceso al medio (**MAC**), las ventajas con respecto a las redes cableadas y sus aplicaciones.

Y por último, se indicará el protocolo de señalización y los protocolos de transporte de multimedia sobre IP con la descripción de cada uno de ellos. Con este conocimiento describiremos como se realizaría una llamada IP aplicando los protocolos (conexión H.323).

1.1. GENERALIDADES DE LAS REDES DE AREA LOCAL INALAMBRICAS (WLAN).

WLAN son las siglas en inglés de Wireless Local Área Network que traducido al español significa Redes de área local inalámbricas.

Las WLAN son sistemas de comunicación de datos flexible muy utilizado como alternativa a las redes de área local (**LAN**) cableadas o como una extensión de

ésta. Utilizan tecnología de radio frecuencia que permite mayor movilidad a los usuarios al minimizarse las conexiones cableadas.

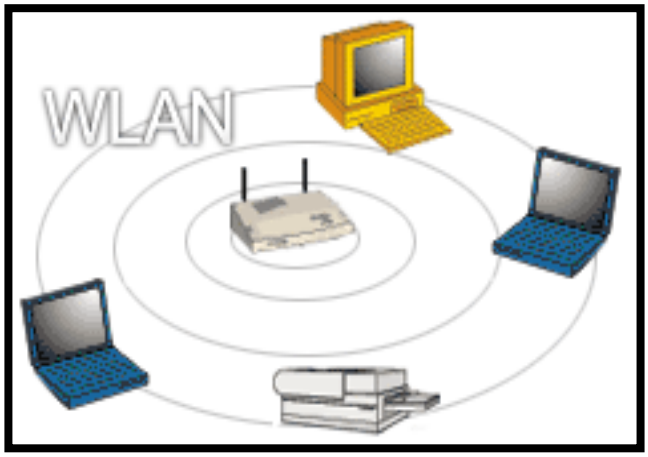


FIG. 1.1 Red de área local inalámbrica (WLAN)

Los orígenes de las redes de área local inalámbricas (**WLAN**) se remontan a los años setenta. Esto se dio en una fábrica suiza donde se obtuvieron los primeros resultados satisfactorios de comunicación inalámbrica dentro de una red local, desde entonces, las actividades hacia la investigación y desarrollo de dispositivos que hacen posible las redes de esta naturaleza se han intensificado.

Tiempo después, en marzo de 1985 la Comisión Federal de Comunicaciones (**FCC**) le asignó a los sistemas WLAN las bandas de frecuencias siguientes (902-928 MHz), (2,400-2,484 GHz) y (5,725-5,850 GHz), dichas bandas se las conoce como: Industrial, Científica y Médica (**ISM)**, que pueden usarse con una licencia administrativa. Esto generó: una mayor actividad industrial y que las redes de área local dejasen de ser meramente experimentales y se empezaran a introducir en el mercado local.

En estos últimos años se ha producido un crecimiento de las redes WLAN de hasta un 100% anual, este hecho es gracias a dos razones principales:

1. El desarrollo del mercado de los equipos portátiles y de las comunicaciones móviles, han facilitado que los usuarios puedan estar en continuo movimiento manteniendo comunicación constante con otros terminales y elementos de la red.

2. La conclusión de la norma IEEE 802.11, que establece un punto de referencia y ha mejorado muchos de los aspectos de este tipo de redes.

La fuerza que a la fecha ha cobrado esta tecnología se debe, en gran medida, a las ventajas de movilidad para los usuarios y al precio competitivo que tienen en relación con las redes alámbricas convencionales, entre otras cuestiones.

1.1.1. TECNOLOGÍAS UTILIZADAS EN LAS REDES INALÁMBRICAS.

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Según el diseño requerido se tienen dos distintas tecnologías aplicables:

1.1.1.1. TECNOLOGÍA DE RADIO FRECUENCIA.

Por el otro lado para las Redes Inalámbricas de Radio Frecuencia, la FCC permitió la operación sin licencia de dispositivos que utilizan 1

Watt de energía o menos, en tres bandas de frecuencia: 902 a 928 MHz, 2,400 a 2,483.5 MHz y 5,725 a 5,850 Mhz. Estas bandas de frecuencia, llamadas bandas ISM, estaban anteriormente limitadas a instrumentos científicos, médicos e industriales. Esta banda, a diferencia de la ARDIS y MOBITEX, está abierta para cualquiera. Para minimizar la interferencia, las regulaciones de FCC estipulan que una técnica de señal de transmisión llamada spread-spectrum modulation, la cual tiene potencia de transmisión máxima de 1 Watt. deberá ser utilizada en la banda ISM. Esta técnica ha sido utilizada en aplicaciones militares. La idea es tomar una señal de banda convencional y distribuir su energía en un dominio más amplio de frecuencia. Así, la densidad promedio de energía es menor en el espectro equivalente de la señal original. En aplicaciones militares el objetivo es reducir la densidad de energía abajo del nivel de ruido ambiental de tal manera que la señal no sea detectable. La idea en las redes es que la señal sea transmitida y recibida con un mínimo de interferencia. Existen dos tecnologías para distribuir la señal convencional en un espectro de propagación equivalente:

- **TECNOLOGÍA DE BANDA ESTRECHA.**

En esta tecnología se transmite y recibe en una específica banda de frecuencia lo más estrecha posible para el paso de información. Los usuarios tienen distintas frecuencias de comunicación de modo que se evitan las interferencias. Así mismo un filtro en el receptor de radio se

encarga de dejar pasar únicamente la señal esperada en la frecuencia asignada.

- **TECNOLOGÍA DE BANDA ANCHA.**

Esta tecnología es la usada por la mayor parte de los sistemas sin cable. Fue desarrollada por los militares para una comunicación segura, fiable y en misiones críticas. Se emplea más ancho de banda pero la señal es más difícil de interceptar.

Hay dos tipos de tecnología en banda ancha:

1. **Tecnología de Espectro Ensanchado por Secuencia Directa (DSSS)**

Esta técnica consiste en la generación de un patrón de bits redundante llamado señal de chip para cada uno de los bits que componen la señal de información y la posterior modulación de la señal resultante mediante una portadora de radio frecuencia. En la recepción es necesario realizar el proceso inverso para obtener la señal de información original.

La tecnología DSSS tiene definidos dos tipos de modulaciones a aplicar a la señal de información una vez que se sobrepone la señal de chip tal y como especifica el estándar IEEE 802.11, los tipos de modulación pueden ser: transmisión por desplazamiento de fase binaria diferencial (**DBPSK**) y transmisión por desplazamiento de fase

cuaternaria diferencial (**DQPSK**); proporcionando unas velocidades de transferencia de 1 y 2 Mbps respectivamente.

2. Tecnología de Espectro Ensanchado por Salto en Frecuencia (FHSS)

La tecnología de espectro ensanchado por salto en frecuencia (FHSS), consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo inferior a los 400 ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo.

Cada una de las transmisiones a una frecuencia concreta se realiza utilizando una portadora de banda estrecha que va cambiando (saltando) a lo largo del tiempo. Este procedimiento equivale a realizar una partición de la información en el dominio temporal.

El orden en los saltos en frecuencia que el emisor debe realizar viene determinado según una secuencia seudo aleatoria que se encuentra definida en unas tablas que tanto el emisor como el receptor deben conocer.

La ventaja de estos sistemas frente a los sistemas DSSS es que con esta tecnología podemos tener más de un punto de acceso en la misma zona geográfica sin que existan interferencias así se cumple

que dos comunicaciones distintas no utilizan la misma frecuencia portadora en un mismo instante de tiempo.

1.1.1.3. TECNOLOGÍA DE INFRARROJOS.

Esta tecnología es por el momento la menos utilizada a nivel comercial para implementar WLANs. Los sistemas de infrarrojos se sitúan en altas frecuencias, justo por debajo del rango de frecuencias de la luz visible. Las propiedades de los infrarrojos son, por tanto, las mismas que tiene la luz visible. De esta forma los infrarrojos no pueden pasar a través de objetos opacos pero se pueden reflejar en determinadas superficies.

Los sistemas que funcionan mediante infrarrojos se clasifican según el ángulo de apertura con el que se emite la información en el emisor en:

Sistemas de corta apertura: de haz dirigido o de visibilidad directa que funcionan de manera similar a los mandos a distancia de los equipos de televisión (controles remotos). Esto supone que el emisor y el receptor tienen que estar orientados adecuadamente antes de empezar a transmitirse información.

Sistemas de gran apertura: reflejados o de difusión que radian tal y como lo haría una bombilla, permitiendo el intercambio de información en un rango más amplio.

Esta tecnología se aplica típicamente en entornos de interior para implementar enlaces punto a punto de corto alcance o redes locales en entornos muy localizados como puede ser una aula concreta o un laboratorio.

1.1.2. CONFIGURACIONES DE LAS REDES DE ÁREA LOCAL INALÁMBRICAS (WLAN).

Las redes LAN inalámbricas se construyen utilizando dos topologías básicas. Estas topologías son conocidas como: Configuración Punto a Punto y Configuración Multipunto. Estos términos están relacionados, esencialmente, con las mismas distinciones básicas de topología.

1.1.2.1. CONFIGURACIÓN PUNTO A PUNTO.

FIG. 1.2 Configuración Punto a Punto

Esta es la más básica de las configuraciones, la cual se da entre dos ordenadores equipados con tarjetas adaptadoras para redes

inalámbricas, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno.

Cada cliente tiene únicamente acceso a los recursos de otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o preconfiguración.

1.1.2.2. CONFIGURACIÓN MULTIPUNTO.

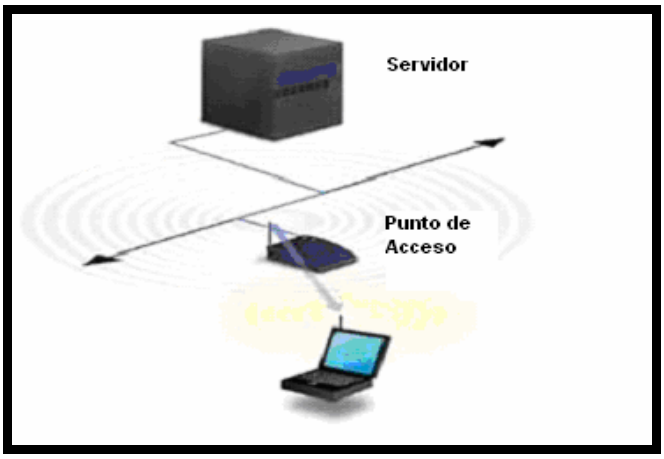


FIG. 1.3 Configuración Multipunto

Para aumentar el alcance de una red del tipo anterior hace falta la instalación de un punto de acceso. Con este nuevo elemento doblamos el alcance de la red inalámbrica (ahora la distancia máxima permitida no es entre estaciones, sino entre cada estación y el punto de acceso). En la figura 1.3 mostramos un ejemplo. Además, los puntos de acceso se pueden conectar a otras redes, y en particular a una red fija, con lo cual un usuario puede tener acceso desde su terminal móvil a otros recursos.

Para dar cobertura en una zona determinada habrá que instalar varios puntos de acceso de tal manera que podamos cubrir la superficie necesaria con las celdas de cobertura que proporciona cada punto de acceso y ligeramente solapadas para permitir el paso de una celda a otra sin perder la comunicación.

1.1.3. LOS ESTÁNDARES IEEE.802.11 PARA LAS REDES INALÁMBRICAS.

Los estándares para las redes inalámbricas son desarrollados por organismos reconocidos internacionalmente, tal es el caso del Instituto de Ingenieros Eléctricos y Electrónicos (**IEEE**) y el Instituto Europeo de normalización de las telecomunicaciones (**ETSI**). Una vez desarrollados se convierten en la base de los fabricantes para desarrollar sus productos. Entre los principales estándares se encuentran:

IEEE 802.11: es el estándar original de las redes inalámbricas que soporta velocidades entre 1 y 2 Mbps. La especificación base del 802.11 incluye:

- La descripción del MAC 802.11.
- La especificación de dos capas físicas: transmisión con Espectro ensanchado por salto de frecuencia (**FHSS**) y Espectro ensanchado por secuencia directa (**DSSS**), con una velocidad de hasta 2 Mbps, en la banda ISM de 2.4 Ghz. (ISM, Banda industrial, científica y medica entre los 2.4 Ghz y 5 Ghz, en las que se permite hasta 1 W de potencia de transmisión por equipo).

Desafortunadamente la fuerte demanda de soluciones inalámbricas con mayor ancho de banda, originó de que el estándar IEEE.802.11 quede obsoleto y descontinuado, y que se generen nuevas derivaciones de éste, producto de ello tenemos:

IEEE 802.11a: estándar de alta velocidad que soporta modulación por Multiplexación por división en frecuencias ortogonales (**OFDM**), la cual permite la transmisión aunque no exista línea de vista; y velocidades de hasta 54 Mbps en la banda de 5 Ghz.

IEEE 802.11b: estándar dominante de las redes inalámbricas (conocido también como Wi-Fi) que soporta modulación DSSS y velocidades de hasta 11 Mbps en la banda de 2.4 Ghz. utilizadas actualmente.

IEEE 802.11g: es otro estándar de alta velocidad que soporta modulación OFDM/DSSS y con velocidades de hasta 54 Mbps en la banda de 2.4 Ghz. Los equipos con esta norma son compatibles con los del estándar IEEE.802.b.

La siguiente tabla muestra un resumen de los principales estándares de las redes inalámbricas y sus características:

ESTANDAR	VEL. MAX	INTERFASE DE AIRE	ANCHO DE BANDA DE CANAL	FRECUENCIA	ESTATUS
802.11	1.2 Mbps	DSSS, FHSS	25 MHz	2.4 GHz	Actualmente obsoleta
802.11b	11 Mbps	DSSS	25 MHz	2.4 GHz	La mas difundida
802.11a	54 Mbps	OFDM	25 MHz	5.8 GHz	Gran aceptación
802.11g	54 Mbps	OFDM, DSSS	25 MHz	2.4 GHz	En experimentación

Tabla 1.1 Principales estándares de las redes inalámbricas (WLAN)

De lo anterior podemos decir que:

- Si bien la norma 802.11b, es la que actualmente se comercializa en forma masiva a través de una gran variedad de productos y aplicaciones también es cierto de que los equipos definidos en los estándares 802.11a y 802.11g del IEEE en la actualidad están teniendo una gran aceptación en el mercado de las redes inalámbricas gracias a que ofrecen velocidades de hasta 54 Mbps y sistemas de seguridad que garantizan la inviolabilidad en cada transmisión.

- Los productos que trabajan bajo este estándar IEEE.802.11a, funciona en la banda de frecuencia de 5 Ghz y utilizan la modulación OFDM, gozan de dos notables ventajas respecto al 802.11b. como son: Incrementan la velocidad máxima de transferencia de datos por canal (de 11 Mbps a 54Mbps) y aumentan el número de canales disponibles.

- La banda de los 5 GHz (llamada banda UNII) esta formada por tres sub-bandas, UNII1(5.15-5.25Ghz), UNII2(5.25-5.35Ghz) y UNI3(5.75-5.825Ghz). Cuando se utilizan tanto UNII1 como UNII2, hay 8 canales disponibles; mientras que con la banda de 2,4Ghz solo hay 3. El ancho de banda total disponible en la banda de 5Ghz. también es mayor que en la banda de 2,4Ghz (300Mhz por 83.5Mhz). Así pues, una red inalámbrica usada en el 802.11a puede admitir un mayor número de usuarios de alta velocidad simultáneamente sin peligro de que surjan conflictos.

- El IEEE 802.11g en comparación con el estándar IEEE 802.11a tiene un ancho de banda utilizable mas bajo, lo que redunda en un menor número de usuarios WLAN de alta velocidad. Aunque las modulaciones OFDM permiten una velocidad más alta, el ancho de banda disponible total en la banda de frecuencia de 2.4GHz no varía. El motivo es de que el IEEE 802.11g todavía esta restringido a tres canales en la banda de 2.4 Ghz.

- Cabe mencionar que los estándares 802.11b, 802.11g son tecnologías que utilizan banda de frecuencia de 2.4 Ghz, mientras que la tecnología 802.11a utiliza la banda de frecuencia de los 5.8 Ghz, todas estas son banda que no requieren licencia, lo que significa que su uso es libre para cualquier usuario.

- Los productos IEEE 802.11g poseen un alto grado de compatibilidad con productos ajustados a IEEE802.11 e IEEE 802.11b, y todavía utilizan la banda de frecuencia ISM. Eso significa que las distancias de transmisión de los productos 802.11b y 802.11g son prácticamente las mismas.

1.1.3.1. PROTOCOLO MAC DEL IEEE 802.11.

Propiedades del medio inalámbrico.

Las propiedades únicas del medio inalámbrico hacen que el diseño de los protocolos de control de acceso al medio sea muy diferente de los protocolos para redes de cable. Estas propiedades son:

1. Funcionamiento Half-Duplex

Es muy difícil transmitir y recibir al mismo tiempo. La señal transmitida produce auto-interferencias, es decir, parte de la señal transmitida se recibe con una potencia de varios órdenes de magnitud mayor que la señal del otro extremo emitida. La detección de una colisión no es, por tanto, posible. Los métodos usados se basan todos en evitar las colisiones, antes que detectarlas.

2. Canal variante en el tiempo

Los mecanismos de propagación (reflexión, difracción y dispersión) producen una superposición de la señal que llega con diferentes retardos y atenuaciones. Es lo que se denomina propagación multi-camino. El resultado de la superposición puede ser la pérdida de la señal, lo que se denomina desvanecimiento. Para evitar las consecuencias de este fenómeno (en el nivel de enlace y superiores) se suelen usar mecanismos de establecimiento de conexión, enviando

mensajes cortos que prueban la calidad del canal antes de la transmisión.

3. Canal con errores de ráfaga

Como consecuencia del canal variante en tiempo, el medio tiene una mayor tasa de error por bit del orden de 10^{-3}.

Además, en medios guiados, el error es debido a ruido aleatorio habitualmente, mientras que en el canal radio, los desvanecimientos producen errores en largas ráfagas de bits.

Para minimizar este problema se usan las siguientes técnicas:

- Paquetes más pequeños.
- Códigos correctores de errores.
- Retransmisiones: la mayoría de los protocolos usan reconocimientos en el nivel de enlace de datos.

Áreas funcionales de la capa MAC del IEEE.802.11.

La capa MAC del estándar IEEE 802.11 cubre tres áreas funcionales, que son:

1. La entrega fiable de datos

Para minimizar los problemas del medio inalámbrico se incorporan dos mecanismos. Por una parte, para evitar el problema de la pérdida de tramas en el canal, se implementa un mecanismo de reconocimiento positivo. Todas las tramas transmitidas deben ser reconocidas (mediante una trama ACK). Este intercambio se trata como una operación fundamental y no puede ser interrumpido por la transmisión de otra estación.

Por otra parte, para solucionar el problema de los nodos ocultos (interferencia en las transmisor entre dos estaciones por una tercera que no puede detectar la transmisión) se utiliza un mecanismo de RTS/CTS (requerimiento de envío/borrar para enviar), las tramas RTS/CTS se transmiten antes de la trama de datos. Las estaciones que escuchan estas tramas ceden el medio durante un tiempo determinado.

2. El Control de acceso al medio y las funciones de coordinación

El acceso al medio está controlado por lo que se denominan “funciones de coordinación” (esta función determina cuándo una estación puede transmitir y/o recibir unidades de datos de protocolo al nivel MAC a través del medio inalámbrico). La misma esta conformada por dos funciones: la Función de coordinación distribuida y la Función de coordinación puntual.

La Función de coordinación distribuida (DCF)

La función de coordinación distribuida se encuentra en el nivel inferior del subnivel MAC de la arquitectura IEEE 802.11y su funcionamiento se basa en técnicas de accesos aleatorias de disputa al medio. Esto lo podemos ver en la siguiente figura 1.4.

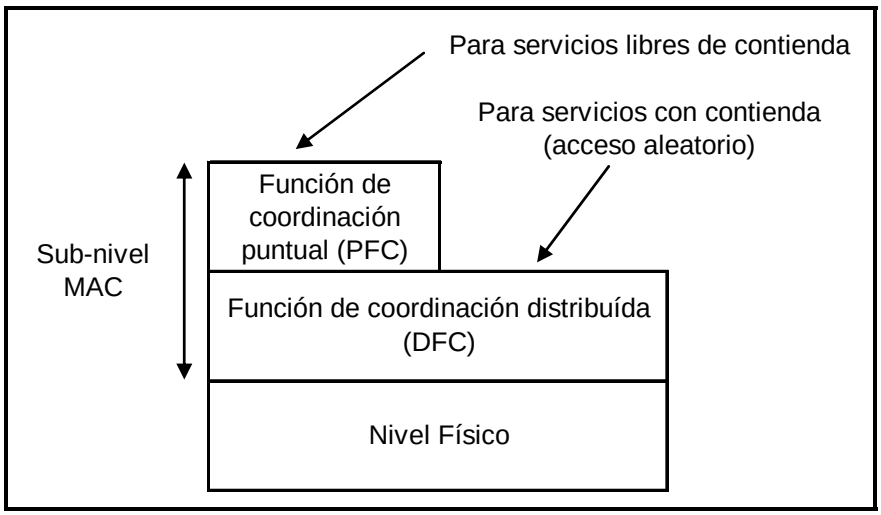


FIG. 1.4 Arquitectura IEEE 802.11 de niveles 1 y 2

El tráfico que se transmite bajo esta funcionalidad es de carácter asíncrono ya que esta técnica de disputa introduce retardos aleatorios y no predecibles.

El algoritmo básico de acceso a este nivel es muy similar al implementado en el estándar IEEE 802.3 de las redes LAN y se llama acceso múltiple por detección de portadora / evadiendo colisiones (**CSMA/CA -** Carrier Sense Multiple Access/Collision Advoidance).

El algoritmo CSMA/CA, se basa en un conjunto de retardos que permiten un cierto esquema de prioridades. La descripción del funcionamiento es la siguiente:

1. Antes de transmitir información, una estación debe hacerle pruebas al medio, o canal inalámbrico, para determinar su estado (libre/ocupado).

2. Si el medio esta libre, la estación ejecuta una espera adicional, llamada: espaciado entre tramas (IFS).

3. Si durante este intervalo temporal, o bien ya desde el principio, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción; si de lo contrario el medio permanece libre durante el intervalo IFS la estación iniciará el proceso de transmisión una vez que finalice el mismo.

4. Una vez que finaliza esta espera, debida a la ocupación del medio, la estación ejecuta el llamado algoritmo de Backoff (proceso de generación de tiempos de espera adicionales y aleatorios), el cual tiene como función reducir la probabilidad de colisiones que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir.

5. Mientras se ejecuta la espera marcada por el algoritmo de Backoff, se continúa escuchando el medio, de tal manera que si el medio se

determina libre, la estación espera el tiempo restante y luego de esto transmite. En cambio, si el medio no permanece libre el algoritmo de Backoff queda suspendido hasta que se cumpla esta condición.

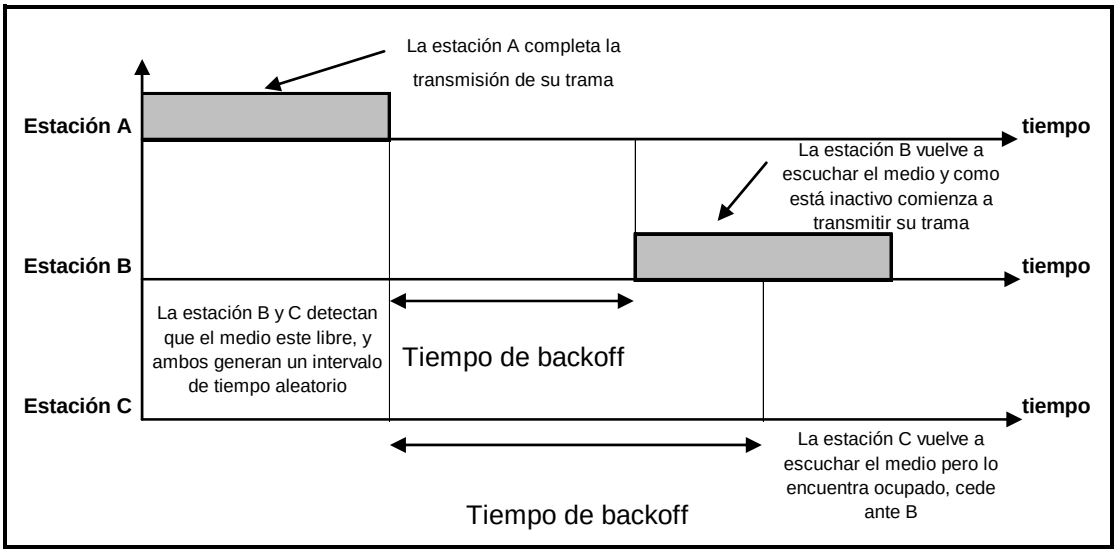


FIG. 1.5 Funcionamiento del Protocolo CSMA/CA

Cabe recalcar que en la figura 1.5, podemos observar que en lugar de iniciar la transmisión de una trama inmediatamente después que el canal queda inactivo, la estación espera un intervalo de tiempo aleatorio adicional corto (generado por el algoritmo de Backoff), y solo si después de este intervalo el canal libre comienza a transmitir. De esta manera si hay estaciones en espera, la que calcule el tiempo mas corto obtendrá el acceso primero.

Para concluir la técnica que se aplica entonces es intentar evitar las colisiones, que es a lo que se refiere el método CSMA/CA (CSMA con

anulación de colisiones), descrito anteriormente y que se puede puntualizar en:

- Si el canal esta ocupado se espera a que esté libre.
- Si esta libre, se espera un tiempo aleatorio y si sigue libre se transmite.

Función de coordinación puntual (PCF)

Esta función de coordinación puntual se sitúa por encima de la función de coordinación distribuida en el subnivel MAC, como se puedo observar en la figura 2.4. Esta función esta asociada a las transmisiones libres de disputas que utilizan técnicas específicas de acceso al medio. Esta funcionalidad esta pensada para servicios que no toleran retardos aleatorios en el acceso al medio.

3. La seguridad en la transmisión

La seguridad en la transmisión de los datos se realiza por medio del protocolo WEP (Wired Equivalent Privacy-Privacidad equivalente al cable), el cual se basa en la encriptación de los datos para protegerlos durante su transmisión de un punto a otro, usando claves de 64 bits, 128 o 256 bits, y el algoritmo de encriptación RC4 (el algoritmo RC4, es utilizado para proteger las transmisiones realizadas a través del aire, es un algoritmo Cifrador de flujo y no de bloques). Cuando WEP

se habilita, sólo protege la información del paquete de datos y no el encabezamiento del mismo.

1.1.4. VENTAJAS DE LAS REDES LOCALES INALÁMBRICAS SOBRE LAS CABLEADAS.

Frente a las redes tradicionales se tienen las siguientes ventajas más importantes en cuanto a productividad, comodidad y costos.

- **Movilidad:** Información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. El que se obtenga en tiempo real supone mayor productividad y posibilidades de servicio.

- **Facilidad de instalación:** Evita obras para tirar cable por muros y techos.

- **Flexibilidad:** Permite llegar donde el cable no puede.

- **Reducción de costos:** Cuando se dan cambios frecuentes o el entorno es muy dinámico el coste inicialmente más alto de la red sin cable es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación.

- **Escalabilidad:** El cambio de topología de red es sencillo y trata igual a pequeñas y grandes redes.

1.1.5. APLICACIONES DE LOS SISTEMAS INALÁMBRICOS EN LA ACTUALIDAD.

Hoy en día vemos las redes inalámbricas en:

- **Las Corporaciones:** Con WLAN los empleados pueden beneficiarse de una red móvil para el correo electrónico, compartición de ficheros, y visualización de paginas Web, independientemente de dónde se encuentren en la oficina.

- **La Educación:** Las instituciones académicas que soportan este tipo de conexión móvil permiten a los usuarios con consolas de ordenador conectarse a la red de la universidad para intercambio de opiniones en las clases, para acceso a Internet, etc.

- **Las Finanzas:** Mediante un PC portátil y un adaptador a la red WLAN, los representantes pueden recibir información desde una base de datos en tiempo real y mejorar la velocidad y calidad de los negocios. Los grupos de auditorias contables incrementan su productividad con una rápida puesta a punto de una red.

- **El Cuidado de la Salud:** WLAN permite obtener información en tiempo real, por lo que proporciona un incremento de la productividad y calidad del cuidado del paciente eliminando el retardo en el tratamiento del paciente, los papeles redundantes, los posibles errores de trascripción, etc.

- **La Hotelería y locales de ventas:** Los servicios de hotelería pueden utilizar WLAN para directamente entrar y enviar los pedidos de comida a la mesa y de otros servicios a los huéspedes en cualquier lugar del recinto hotelero. En los almacenes de ventas WLAN se puede usar para actualizar temporalmente registros para eventos especiales.

- **Las Empresas Manufactureras:** WLAN ayuda al enlace entre las estaciones de trabajo de los pisos de la fábrica con los dispositivos de adquisición de datos de la red de la compañía.

- **Los Almacenes:** En los almacenes, terminales de datos con lectores de código de barras y enlaces con redes WLAN, son usados para introducir datos y mantener la posición de las paletas y cajas. WLAN mejora el seguimiento del inventario y reduce los costes del escrutinio de un inventario físico.

1.2. PROTOCOLOS DE SEÑALIZACIÓN Y TRANSPORTE DE MULTIMEDIA SOBRE IP.

Estudiaremos el protocolo de señalización H.323, el cual es un estándar muy importante para la comunicación de audio, video y datos; así también los elementos que lo conforman.

Además de los protocolos de transporte multimedia como es el protocolo de transporte rápido “RTP” y del protocolo de control RTP “RTCP” (protocolos de ruteo de multimedia universalmente aceptados) y por último haremos un análisis del proceso del establecimiento de una conexión H.323.

1.2.1. EL PROTOCOLO DE SEÑALIZACIÓN: H.323.

La recomendación H.323 también llamado, Sistema de comunicación multimedia basada en paquetes (Packet-Based Multimedia Communication Systems), es el mejor conjunto de estándares y formatos para las comunicaciones multimedia multipunto.

H.323 es un protocolo que contiene referencias de los protocolos y formatos de mensaje descritos en otros documentos de normas, y explica cómo interactúan los distintos protocolos con los elementos del sistema definidos en una estructura común.

Además de las funciones de señalización, la estructura H.323 incorpora una variedad de formatos de medios y estructuras de aplicación, tal y como aparece en la Tabla 1.2.

MEDIO	FORMATOS
Audio	G.711, G.722, G.723.1, G.728, G.729, GSM, ISO/IEC 11172-3 y ISO/IEC 13818-3.
Vídeo	H.261, H.262, H.263.
Protocolos de datos	Series T.120.

Tabla 1.2 Formatos de medios apoyados por la ITU-T para H.323

Los protocolos de señalización más importantes utilizados en el seno de la H.323 son:

- H.225.0 o RAS: que define las interacciones entre un terminal H.323 y un gatekeeper H.323. También define la señalización para

establecimiento y liberación de la conexión o llamada que va por el canal de señalización. En este caso se utiliza un subconjunto de las funciones proporcionadas por la Q.931.

- H.245: Señalización de control extremo a extremo. La función principal es el intercambio de capacidades entre los terminales H.323 previa a la transmisión de información.

- H.235: trata sobre la seguridad en la comunicación incluyendo autentificación, autorización, control de llamada seguro y privacidad de los canales de voz.

- H.450: señalización para el control de todos los servicios suplementarios (desvío de llamada, llamada en espera, etc.).

Los codecs más importantes utilizados en el seno de la H.323 son:

- T.120: la recomendación T.120 define la tecnología de conferencia de documentos que puede existir dentro de la trama H.323. El T.120 está basado en una aproximación multicapa, la cual define los protocolos y servicios entre niveles. Cada nivel dentro de la arquitectura asume la existencia de los otros.

- G.711: Modulación por Codificación de Pulsos (**PCM**) de las frecuencias de voz. La recomendación G.711 describe la codificación de audio de 3.1 KHz en un canal digital de 64 kbps.

- G.722: Codificación de Audio de 7 KHz en 64 Kbps. La recomendación G.722 describe el uso de la modulación adaptativa diferencial de pulsos para transmitir audio de alta calidad 7 KHz en 48, 56 o 64 Kbps. Esta recomendación también permite la transmisión de datos a 16 Kbps sobre un canal de 64 Kbps, con los 48 Kbps restantes para audio.

- G.728: la recomendación G.728 describe el método para la codificación de audio que permite una calidad próxima a 3.1 KHz usando 16 Kbps de ancho de banda. El algoritmo G.728 usa sólo 16 kbps para compresión de audio, lo cual da mayor espacio para el vídeo y opcionalmente para los datos. El resultado es una significativa mejor calidad de vídeo cuando se utilizan algoritmos de audio convencionales. Es especialmente recomendable cuando se trabaje sobre líneas de 128 Kbps.

- H.261: Codificación de Vídeo para Servicio Audiovisuales a 64 kbps. La recomendación H.261 describe el método de compresión de la señal de vídeo para transmisión sobre medios digitales. El H.261 también especifica el rango de velocidades utilizables para transportar la información de vídeo.

La arquitectura de protocolos utilizada por H.323 es la mostrada en la siguiente figura:

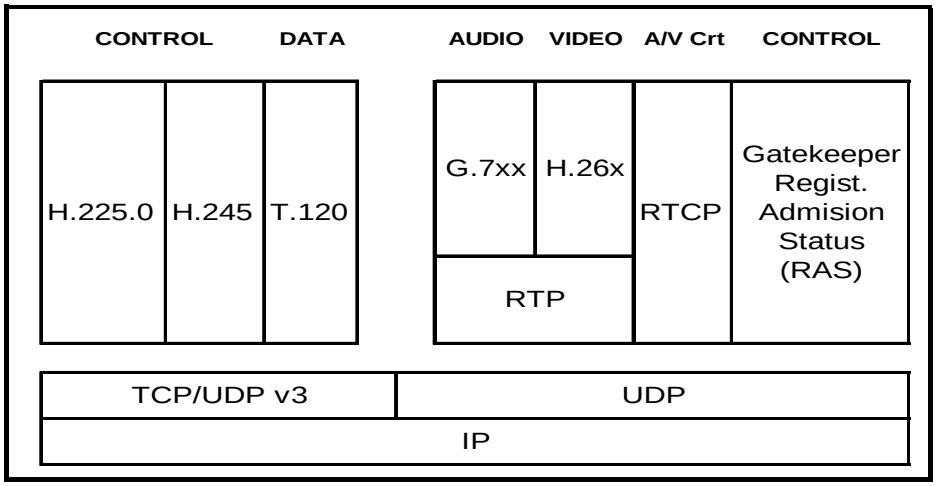


FIG. 1.6 Arquitectura de Protocolos en H.323

1.2.1.1. COMPONENTES DEL ESTÁNDAR H.323.

Este protocolo define los siguientes componentes lógicos:

Las Terminales, las Pasarelas o Gateways, los porteros o Gatekeepers y las Unidades de Control Multipunto o MCUs.

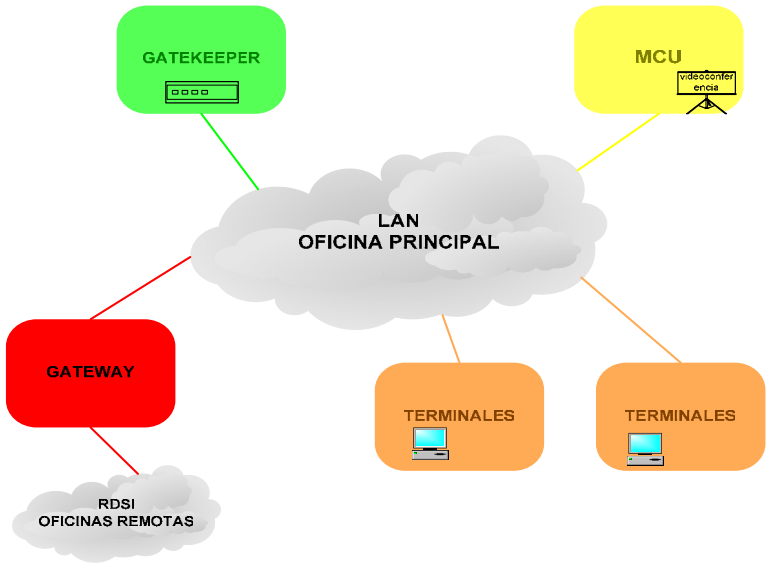


FIG.1.7 Componentes del estándar H.323

1. Los Terminales H.323.

Estos son los puntos finales de la red que proporcionan la comunicación bidireccional en tiempo real con otro terminal H.323, Gateway o MCU (Unidad de Control Multipunto). El intercambio de información incluye controles, indicaciones, audio, video y datos. Un terminal debe soportar al menos transmisión de voz, voz y datos, voz y video o voz datos y video.

2. Las Pasarelas o Gateways.

Una Pasarela o Gateway H.323 es un elemento que permite interoperar a los terminales H.323 con terminales en otras redes de circuitos. Las pasarelas se conectan directamente con terminales H.323 o bien con otras pasarelas o terminales en otras redes y realiza las funciones de adaptación entre flujos de información así como entre los protocolos de control de ambos entornos.

La pasarela debe constar al menos de dos interfaces, realizando las funciones de adaptación y convergencia entre ambos interfaces.

3. El Gatekeeper o Portero.

El Gatekeeper o Portero es un elemento de la red H.323 que proporciona servicios al resto de elementos. Este elemento constituye la base para el desarrollo de servicios y para la aplicación de esta

tecnología en entornos con un número de terminales medio-grande. El Gatekeeper es un elemento opcional de la arquitectura, lo que permitió inicialmente el desarrollo de terminales que podían comunicarse directamente entre si sin la necesidad de disponer de un Gatekeeper. Sin embargo la inexistencia de un Gatekeeper limita el servicio de transferencia de medios.

Funciones del Gatekeeper

- **Traducción de la dirección:** Esto es traducir la dirección alias (Ej.: romelito@host.com, o direcciones E.164) a una dirección de transporte.

- **Control de Admisiones:** Los Gatekeepers pueden permitir o denegar el acceso bajo una autorización por llamada, direcciones de fuente y destino o cualquier otro criterio.

- **Señalización de llamada:** Los Gatekeepers pueden completar la señalización de la llamada con los puntos finales y pueden procesar ellos mismos la señalización. Alternamente, los porteros pueden direccionar los puntos finales para conectar el canal de señalización de la llamada directamente uno con el otro.

- **Autorización de Llamada:** Los porteros pueden rechazar llamadas de una terminal debido al fallo del uso de la señalización H.225. Las razones de rechazo pueden ser por el acceso

restringido durante ciertos periodos de tiempo o el acceso restringido de/para terminales particulares o compuertas.

- **Control o manejo del ancho de Banda:** Desde el control del acceso del número de terminales H.323 permitidas a la red, hasta el uso de la señalización H.225, los Gateways pueden rechazar llamadas de una terminal debido a las limitaciones del ancho de banda.

- **Manejo de la llamada:** El Gateway puede mantener una lista de llamadas H.323 salientes. Esta información puede ser necesaria para indicar el funcionamiento del manejo del ancho de banda.

4. La Unidad de control multipunto (MCU).

La unidad de control multipunto (**MCU**) es el elemento funcional de la red H.323 que permite soportar comunicaciones multipunto.

Por esta razón, la MCU esta dividida en dos partes: el controlador multipunto (**MC**) que proporciona capacidad de negociación y control de los miembros del grupo y el procesador multipunto (**MP**) que se encarga de realizar las funciones de mezcla de medios (audio, video y datos). La funcionalidad de la MCU puede ser integrada en un terminal H.323.

1.2.2. PROTOCOLOS DE TRANSPORTE MULTIMEDIA.

Estos protocolos son los que transportan los paquetes de información en tiempo real. Por lo que nos referiremos a dos; uno, que no supervisa el envío de información y el otro que supervisa la calidad de servicio de envío de estos paquetes.

A continuación haremos una descripción de cada uno.

1.2.2.1. EL PROTOCOLO DE TRANSPORTE RÁPIDO (RTP).

El Protocolo de transporte en tiempo real (**RTP**), es un protocolo IP que proporciona soporte para el transporte de datos en tiempo real, como video y audio.

Los servicios proporcionados por RTP incluyen la reconstrucción de temporizaciones, la detección de perdidas de paquetes y la seguridad e identificación de contenidos.

RTP se ha diseñado principalmente para la transmisión multicast, pero también puede ser utilizado en unicast. Se puede usar igualmente para transporte unidireccional, por ejemplo el video on demand o para servicios interactivos como la telefonía por Internet.

RTP proporciona marcas temporales, numeración de secuencias y otros mecanismos para tener en cuenta los problemas relativos a la

temporización. Con estos mecanismos, RTP proporciona transporte punto a punto en tiempo real sobre la red de Internet.

Otra función que realiza el protocolo RTP es la identificación de las fuentes de datos, esto le permite a la aplicación receptora conocer de donde vienen los datos, por ejemplo en una audioconferencia, a partir del identificador de la fuente se puede saber quien esta hablando.

Cabe recalcar de que el nombre de “protocolo de transporte “no es del todo cierto, ya que es usado junto con el protocolo UDP, el cual es un protocolo de transporte.

La elección del UDP se debe a varias razones, en primer lugar RTP puede hacer uso de las funciones de multiplexado y checksum de UDP, además RTP fue diseñado pensado para los servicios multicast, para lo cual la conexión UDP es apropiada; en segundo lugar RTP ha sido diseñado para datos en tiempo real, en donde la fiabilidad del transporte no es tan importante, pero si el tiempo adecuado en la recepción.

1.2.2.2. EL PROTOCOLO DE CONTROL DE TRANSPORTE RÁPIDO (RTCP).

Este protocolo permite mejorar al protocolo RTP facilitando la comunicación entre participantes para intercambiar datos y de esta forma monitorear la calidad de servicio y así obtener la información acerca de los participantes de la sesión.

RTCP se fundamenta en la transmisión periódica de paquetes de control a todos los participantes en la sesión usando el mismo mecanismo de RTP de distribución de paquetes de datos.

La función primordial de RTCP es la de proveer una realimentación de la calidad de servicio, esto se relaciona con el control de congestión y flujo de datos.

El protocolo RTCP aporta funciones de identificación de participantes entre diferentes sesiones y sincronización entre distintos flujos RTP, realimentación acerca de la calidad de recepción, estimación del número de participantes en sesiones multimedia y transporte de información de monitorización y control.

La definición de RTCP como componente adicional permite que aplicaciones que requieran un mayor nivel de control que el proporcionado por RTCP lo reemplacen con otros protocolos de control de conferencia específicos. Actualmente se está finalizando la definición de un nuevo perfil complementario al de sonido y vídeo, que amplía los mecanismos de realimentación del RTCP.

1.2.3. ESTABLECIMIENTO DE UNA CONEXIÓN H.323.

Las entidades H.323 establecen conexiones en diferentes fases las mismas que las podemos observar en la siguiente figura 1.8.

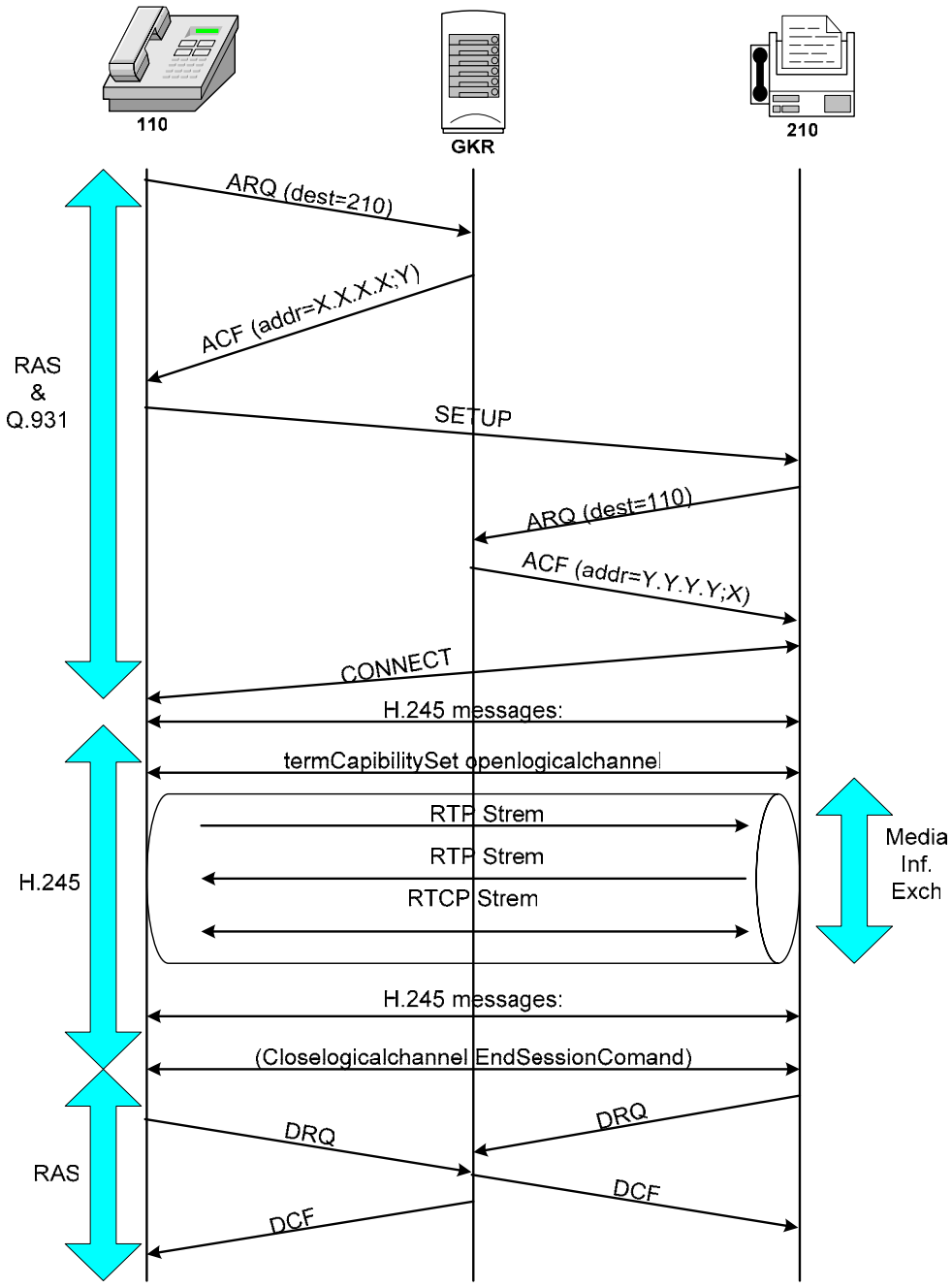


FIG. 1.8 Ejemplo de una conexión H.323

Ahora bien, si consideramos un escenario igual al de la figura 1.8, en el cual exista un Gatekeeper, la conexión entre dos terminales dependientes de este Gatekeeper seguirá las siguientes fases.

1.2.3.1. DESCRIPCIÓN DE LAS FASES DE UNA LLAMADA H.323.

Fase A: *El Establecimiento de la conexión*

La entidad llamante, envía mensajes RAS solicitando la identificación del usuario llamante (Ej.: alias, romelito@host.com, o direcciones E.164) utilizando un mensaje ARQ (admision request, requerimiento de admisión).

El Gatekeeper aceptará la llamada y enviará al terminal llamante un mensaje de confirmación ACF (admision confirm, confirmación de admisión) o bien rechazará la llamada ARJ (admision reject, rechazo de admisión). En caso de que se establezca la llamada, la entidad llamante establecerá una conexión TCP con el terminal llamado para establecer el canal de señalización H.225.0. Para ello utilizará la información (dirección IP y puerto) recibidos del GateKeeper a través del mensaje ACF. La entidad llamada al recibir dicha conexión contactará con su Gatekeeper a través del canal RAS solicitando permiso para poder contestar (ARQ). En caso positivo (ACF), el llamante aceptara la conexión y a través de dicho canal (H.225.0) enviará la dirección (dirección IP y puerto) donde establecer el canal H.245 para negociación de parámetros y control de la comunicación.

Una vez obtenida esta información, la conexión puede ser finalizada, ya que no es necesario intercambiar más parámetros a través de este canal.

Fase B: *El Intercambio de capacidades (canal H.245)*

Establecido el canal H.245 a través de una nueva conexión TCP, las entidades llamante y llamada determinarán los parámetros de la comunicación: codificadores a utilizar, números de conexiones y direcciones a utilizar, puertos, número de muestras por trama, función maestro esclavo, etc., lo que les permite establecer canales para la transmisión de medios (audio, video y datos). Esta conexión debe permanecer mientras intercambien información los terminales y les permita modificar parámetros (codec, número de muestras por tramas, etc.).

Fase C: *El Intercambio de información audiovisual*

En este punto, ambos terminales establecen canales de información a través de la arquitectura RTP/UDP/IP para el transporte de medios, así como canales de control a través de la arquitectura RTCP/UDP/IP para los canales de realimentación, con el al objeto de controlar la calidad de los flujos de información recibida por el otro extremo de la comunicación.

Fase D: *La Terminación de la llamada*

Tras el intercambio de información audiovisual y al objeto de finalizar la llamada, las entidades H.323 deben informarse a través del canal

H.245 mediante el envío de las primitivas de finalización de llamadas, que finalizará con el envío de la primitiva End Session Command que provocará el cierre del canal H.245. Además deberán informar al Gatekeeper mediante el envío del mensaje RAS DRQ (Disengage Request, petición de desacoplamiento) que permitirá al Gatekeeper liberar recursos y proporcionar información de tarificación entre otras, enviando el mensaje DCF (Disengage comfirm, confirmación de desacoplamiento).

Sobre este escenario básico existen múltiples variantes en función de la presencia o no del Gatekeeper y del rol que el mismo realice. El Gatekeeper podría encaminar la información de control (H.225.0 y H.245.0) o no en función del modelo elegido (Directo o Indirecto).

CAPITULO 2

ANÁLISIS DE LOS SISTEMAS DE SEGURIDAD

2.1. CONCEPTOS DE SEGURIDAD INTEGRAL Y SISTEMA DE SEGURIDAD.

Seguridad Integral: es el conjunto de normas preventivas y operativas, con el apoyo de procedimientos, programas, sistemas y equipos de seguridad y protección, orientados a neutralizar, minimizar y controlar los efectos de actos ilícitos o situaciones de emergencia, que afecten y lesionen a las personas y/o bienes que estas poseen.

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

Así, en un siniestro, en principio el sistema lo detectará, luego lo señalizará, para posteriormente iniciar las acciones encaminadas a disminuir o extinguir los efectos.

2.1.1. GENERALIDADES Y APLICACIONES DE LOS SISTEMAS DE SEGURIDAD.

La expresión "sistemas de seguridad “, comúnmente parece alineada con la de “alarmas contra robos”. Pues bien, decir esto no sólo no es decir la verdad, sino que sería una expresión muy simple y deteriorada de lo que en realidad es un “sistema de alarma”.

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

Hoy en día en el mundo de la industria y de los procesos de fabricación, la aplicación de los sistemas de seguridad es un hecho, permitiendo la realización de grandes cadenas de montaje, grandes fábricas, etc., que incorporan múltiples sistemas de seguridad. Estos sistemas tienen como finalidad controlar la cadena de funcionamiento, indicar al operario cualquier anomalía existente, mal funcionamiento, un sobrecalentamiento, etc., direccionando de esta manera en un sentido u otro la actuaciones a realizar una vez detectadas las anomalías.

Los sistemas de seguridad no sólo sirven para proteger a los bienes e inmuebles, protegen a las personas, ahorran tiempo y dinero y en los procesos domésticos e industriales su uso está totalmente generalizado.

Son ejemplos de su aplicación, las siguientes:

- Seguridad en la vivienda.
- Seguridad en los establecimientos.
- Seguridad en las cárceles, centrales nucleares, etc.
- Seguridad activa contra incendios.
- Control de niveles de líquidos.
- Seguridad en calefacción y cuartos de máquinas.
- Control de gases, presiones, humedad, falta de agua.

2.1.2. CLASIFICACIÓN DE LOS SISTEMAS DE SEGURIDAD.

Los tres grandes bloques de aplicación de los sistemas de seguridad son: robo/atraco, incendios y sistemas especiales.

SISTEMAS	TIPOS
ROBO Y ATRACO	Sensores y centrales de alarma
	Defensa física
	Señalización del robo
	Dispositivos de acceso
	Circuito cerrado de TV
	Protección de los artículos de grandes almacenes y pequeños establecimientos
	Detector de inspección por Rayos X
	Arco detector de metales
INCENDIO	Sensores y centrales de incendio
	Accionamiento de dispositivos de extinción
	Accionamiento de dispositivos de aviso y señalización
	Extinción manual
	Bocas de incendio equipadas
	Equipo de bombeo
	Puertas cortafuegos
	Alumbrado de emergencia
ESPECIALES	Detector de explosivos
	Detector de metales
	Sonda detectora de niveles
	Sonda detectora de humedad
	Detector de sustancias químicas
	Detector de presión
	Detector de drogas
	Detector de gas, etc.

TABLA 2.1 Clasificación de los sistemas de seguridad

2.1.3. ESTRUCTURA DE UN SISTEMA DE SEGURIDAD.

Una instalación se compone de varias partes básicas como son:

La central de alarmas o unidad de control, los sensores, los sistemas de aviso y señalización. A estos se les puede sumar un cuarto elemento que sería el intercomunicador con la central receptora de alarmas y que siempre en todo caso es opcional su colocación en la instalación, aunque es absolutamente aconsejable su utilización.

A continuación se hará una descripción de cada uno de los componentes que forman parte de la estructura de un sistema de seguridad.

2.1.3.1. CENTRAL DE ALARMAS O PANEL DE CONTROL DE ALARMAS.

La central de Alarmas es el cerebro de la instalación que está en estado de vigilancia continuamente, recibiendo información constantemente de los circuitos detectores que componen el sistema, accionando los dispositivos de aviso (sirenas, conexiones al Centro de Recepción de Alarmas o ***CRA***, si la hubiera), en el momento que sea activado cualquier detector o alguna anomalía en el mismo (intentos de vulneración del sistema de seguridad).

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

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

Una central se puede dividir en los siguientes componentes:

Componentes de la central de alarmas:

1. Fuente de Alimentación

Proporciona la tensión de funcionamiento necesaria de los circuitos electrónicos que componen la central.

Transforma los 220 o 120 Voltios de la red en tensión continua, que puede variar desde 6 hasta 24 Voltios, según necesitemos, para obtener la tensión continúa no solo a la central, sino a los detectores, bobinas etc.

2. Baterías

Se colocan para prevenir cualquier fallo del fluido eléctrico, bien por manipulación intencionada, bien por fallo del sistema que lo suministra.

FIG 2.1 .Batería de 12 Volt 1.2 Amp.

3. Teclado

El teclado nos permite que el programador de la central pueda seleccionar y programar las funciones a realizar por medio de la central de alarmas o panel de control. El teclado se conecta directamente al panel y por lo general se ubica en un lugar de fácil acceso para el usuario.

FIG. 2.2 Teclado de programación de la central

4. Microprocesador

Es el cerebro de la instalación. Necesita una programación previa para efectuar un funcionamiento a medida de las características de instalaciones a proteger.

Recibe información continuamente del estado de los detectores instalados en el sistema, accionando las diferentes salidas en caso de incendio en el sistema, sirenas, luces, avisador telefónico, etc.

5. Memoria EPROM ((Memoria de solo lectura programable y borrable).

La memoria Eprom es un chip electrónico donde se encuentran almacenados todas las instrucciones y datos necesarios para que funcione el microprocesador. Estas instrucciones han sido introducidas al sistema previamente por medio del teclado.

6. Marcador Telefónico

El marcador telefónico es un circuito electrónico que se encarga de marcar automáticamente el número de teléfonos previamente fijado en la memoria eprom, posibilitando de esta forma la conexión con la central receptora de alarmas.

En este sentido hay que decir que si en el momento de la activación de la alarma, la línea telefónica estuviese ocupada, el circuito automáticamente la corta, estableciendo de esta forma prioridad en su comunicación.

FIG. 2.3 Central de Alarmas o Panel de Control

2.1.3.2. LOS SENSORES.

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

Son de reducido tamaño y se alimentan a través de una fuente de alimentación de baja tensión (6v. a 12v.) normalmente incorporada en la propia central de alarmas. Los sensores son capaces de detectar:

- Apertura de puertas, ventanas, persianas.
- Paso por lugares determinados.
- Rotura en escaparates o cristaleras.
- Agujeros en paredes.
- Cajas fuertes, etc.

Clasificación de los Sensores:

Los sensores se pueden clasificar en: sensores de intrusión y en sensores especiales. A continuación describiremos esta clasificación.

1. Sensores de Intrusión

Los sensores de intrusión tienen por misión detectar las entradas de elementos extraños (personas), por los lugares en que estén

colocados, entendiendo por lugares todos aquellos que sean factibles de intrusión.

Los sensores de intrusión pueden ser: perimetrales, volumétricos y lineales.

- **Sensores Perimetrales:** Estos sensores están encargados de vigilar el perímetro de una instalación. Son como una barrera colocada alrededor del edificio protegido y se activan cuando algo o alguien la atraviesa.

  Se sitúan en la periferia del edificio a proteger, puertas, ventanas, vallas, etc.

  Por el hecho de estar colocadas en el exterior, detectan al intruso antes de que penetre en el edificio. Pero por este hecho deben ser capaces de soportar las inclemencias del tiempo y lo que es mas, no responder a alguno de sus efectos, viento lluvia, niebla, etc.

  Debido a todo esto, existe una gran variedad de sensores y se aconseja estudiar muy bien sus características antes de realizar el diseño de la instalación de seguridad.

- **Sensores Volumétricos:** Los sensores volumétricos son aquellos que actúan por detección de movimiento, dentro de un volumen determinado, generalmente colocados en locales tales como oficinas, despachos etc.

Su alcance es limitado, por lo que se tendrá que usar más de uno cuando la zona a proteger sea amplia o formada por varios recintos o habitaciones (algo que puede ser normal). Se suelen instalar en el interior de los recintos y detectan el paso de las personas que por allí pasan. Vigilan así el volumen del local.

- **Sensores Lineales:** Los sensores lineales son sensores que actúan al romperse una determinada barrera debido al paso por ella de un individuo u objeto.

  Se suele componer de un elemento emisor (infrarrojos o microondas) y otro receptor.

  En condiciones normales, el receptor recoge las emisiones del emisor y al pasar “algo o alguien” por su campo de actuación, deja de recoger momentáneamente la emisión o detecta que hay una variación determinada de la señal recibida, activando de esta forma la alarma.

  Por último, decir que las características de funcionamiento radican en que cubren una estrecha zona y alargada, aprovechando estas posibilidades para diseñar y realizar el sistema de alarma.

2. Sensores Especiales

Existen en el mercado, por necesidades de realización de instalaciones de seguridad, numerosos sensores que nos permiten

adentrarnos, no sólo en el campo de la protección contra robos y atracos, sino en los campos de la protección contra incendios, que mas adelante veremos, y en sistemas especiales que tienen su aplicación en el mundo del consumo y sobre todo de la industria.

Su utilización de esta forma está encaminada a realizar ciertas actuaciones que le interesen al sistema o a la cadena de funcionamiento, no teniendo nada que ver con lo que hasta ahora hemos tratado en cuestión de centrales contra robos o atracos.

Un ejemplo de estos detectores son los siguientes:

- Detector de metales.
- Sonda detectora de nivel de líquidos.
- Sonda detectora de humedad.
- Detector de substancias químicas.
- Detector de rayos ultravioleta.
- Detector de cortes de corriente eléctrica.
- Detector de funcionamiento de ordenadores.

Por ser detectores muy determinados, siendo su uso muy específico a la aplicación en la industria (cadenas de montaje, almacenes, etc.), pueden llegar a alcanzar precios muy respetables y su uso es muy

específico y determinado a las aplicaciones para las que se han creado.

2.1.3.3. SISTEMAS DE AVISO Y SEÑALIZACIÓN.

Son dispositivos encargados de avisar de las variaciones detectadas por los sensores dentro de un sistema de seguridad. Como culminación a los elementos anteriores, son los que dan sentidos a los sistemas de seguridad, ya que si no estuvieran a punto, no serviría de nada poner de forma estudiada los detectores y central de alarma.

Pueden ser acústicos (sirenas), ópticos (luces), marcadores telefónicos y computadores de monitoreo ubicados generalmente en la Central de Recepción de Alarmas.

2.1.3.4. CENTRAL RECEPTORA DE ALARMAS.

La Central Receptora de Alarmas o ***CRA,*** está ubicada en los locales de las empresas de seguridad que se ocupan de “vigilar” los recintos donde se han instalado sistemas de seguridad.

FIG 2.4 La Central Receptora de Alarmas

Su cometido consiste en recibir, vía teléfono o bajo la vía que utilice el sistema, la señal de activación de alarma (bien sea robo, atraco, incendio, etc.) y comunicar al vigilante la existencia de la misma, para que este ponga en marcha los mecanismos establecidos en cada instalación particular, que puede variar según el tipo de alarma activado.

- *Si es de robo o atraco*: de aviso a la policía y personarse con ella en el edificio.

- *Si es de incendios*: de aviso a los bomberos y se persona en el lugar concreto.

A la Central Receptora de Alarmas están conectados todos los sistemas de seguridad vigilados a distancia. En el momento de la activación de cualquiera de ellas, nos proporciona la información exacta de la alarma activada (lugar exacto dentro de la instalación).

Si dado el volumen de instalaciones diferentes en puntos geográficos distintos conectados a ella, se producen varias a la vez, ésta efectúa una selección de las alarmas más importantes (incendios, atraco, robos, etc.) y las posiciona en pantalla, mostrándosela al vigilante, para posteriormente ir pasando el resto de los avisos de alarma.

Esto se hace con la intención de no “fatigar” con mucha información al vigilante en un solo momento, ya que este no podría atender tantos casos a la vez.

La CRA está conectada a un ordenador central que se encarga de almacenar toda la información que le va llegando de las instalaciones, conexión desconexión, aviso de alarma, avisos de prealarma, avisos de avería, etc.

Estos datos se van registrando automáticamente en el ordenador y se van imprimiendo en papel continuo para su observación, tratamiento, seguimiento y conservación.

El lugar en el que está ubicada la CRA es un bunker, que está protegido por las cuatro paredes, suelo, techo, para previsión de posibles sabotajes. Igualmente, la línea telefónica está protegida de cortes y sabotaje, ya que es fundamental su funcionamiento correcto las 24Horas del día.

2.1.3.5. DISPOSITIVOS DE CONEXIÓN Y DESCONEXIÓN.

En este apartado podemos considerar a todos aquellos mecanismos necesarios que nos permite la conexión y desconexión de los sistemas de seguridad los mismos que pueden ser de tipo mecánico, como las llaves, o de tipo electrónico, como el teclado.

2.1.3.6. ACTIVACION DE OTROS DISPOSITIVOS.

El sistema empleado puede proporcionarnos ciertas posibilidades a la hora de la activación de la alarma:

- Activación de luces de emergencia.
- Activación de electroimanes de puertas cortafuegos para cerrar las puertas.
- Señal de alarma a central, sin activar sirenas y elementos ópticos.

En todo caso, siempre dependerá de las centrales de alarma utilizadas, que cuanto mas sofisticadas y completas sean, más posibilidades externas nos darán, posibilitando así la realización de un sistema de seguridad fiable y seguro.

2.2. DESCRIPCION DE LOS SISTEMAS DE SEGURIDAD.

Aunque el mercado de los sistemas de seguridad, hoy en día parecería infinito gracias a los avances en el campo de la electrónica, en esta sección trataremos de dar a conocer algunos dispositivos y sistemas existentes a los cuales podemos acceder.

Esto lo haremos de una manera general, puesto que lo que queremos, es darle al lector una idea sobre los productos y sistemas de seguridad con los que actualmente contamos y podemos hacer uso en el momento de la implementación de un sistema de seguridad.

2.2.1. SISTEMAS DE SEGURIDAD CONTRA ROBOS Y ATRACOS.

Para esta clasificación tenemos:

1. Sensor de puertas y ventanas vía RF (Radio frecuencia)

FIG. 2.5 Sensor Puerta/Ventana RF

Este módulo tiene un sensor magnético que detecta la apertura de cualquier puerta o ventana. En caso de una apertura de puerta o ventana el módulo envía una señal de RF codificada de 16 bits (inviolable e inimitable) a la consola de seguridad, que activa la alarma. Este aparato es monitoreado por la consola para verificar su estado y la buena carga de las pilas. En el caso de un problema la consola lo señala. Es posible adaptar este módulo para detectar la rotura de un cristal, un incendio, una inundación, etc. Simplemente reemplazando el sensor magnético por otro apropiado (no incluido). Las pilas tienen una duración de 2 años, el alcance de la emisión de radiofrecuencias es de 30 metros en terreno descubierto.

2. Detector de Movimiento Interno

FIG. 2.6 Detector de Movimiento Interno

Este detector es utilizado para funcionar dentro de una habitación y tiene la función de detectar cualquier movimiento dentro de la misma. Frecuentemente se utiliza en una zona equipada con un detector de apertura de puertas/ventanas. Cuando este detector capta un movimiento, envía por radio frecuencia (RF), una señal codificada a la consola que activa la alarma. Este módulo está equipado con un interruptor con dos posiciones que permiten seleccionar la sensibilidad de detección. Esto es útil cuando se tienen animales domésticos (perros, gatos) ya que evita que la alarma salte inesperadamente. Las pilas de este dispositivo son de una duración aproximada de un año. La consola revisa el detector para avisar cuando se han agotado las pilas. El alcance de este detector es de 12 metros con un ángulo de detección de 90º. Se puede colocar a más de 30 metros de la consola. Un máximo de 16 detectores se pueden instalar con la misma consola.

3. Sirena Remota

FIG. 2.7 Sirena Remota

Esta sirena se utiliza junto con el cuadro del módulo adicional de las alarmas. Tiene una potencia de unos 100 Db cuando la alarma se activa. Solo es necesario conectarla a una toma de corriente y ya esta preparada para funcionar. Responde a las órdenes enviadas por la alarma (todas las luces On/Off).

Aplicaciones

- Protección contra el robo
- Sirena transportable que permite multiplicar el número de puntos sonoros
- Completamente compatible con todos los sistemas de alarmas existentes en el mercado, la misma que puede ser activada en modo "pánico" por cualquier emisor convencional.

4. Detectores de cristales rotos

FIG.2.8 Detector de Vidrio Roto

Los detectores de cristales rotos deben tener dos características importantes: como detectan todos los sonidos y que tan efectivo resulta al detectar sonidos que representen alguna amenaza. En los dos aspectos nada se le acerca al nuevo detector de cristales rotos, el cual posee Análisis de Sonido Dinámico; este sistema de detección es tan novedoso que es reconocido por dos patentes. Posee un sistema avanzado de micrófonos capaz de capturar sonido que va más allá del oído humano si se pone en bajo volumen y a más de 25 pies de distancia. Cuando se capta el sonido, este se analiza en detalle digitalmente en sólo una fracción de segundo. Posee Inmunidad RF con protección de descarga estática y de transeúntes.

5. Alarma personal en el llavero

FIG. 2.9 Alarma personal en el llavero

Este llavero activa una potente sirena en caso de cualquier tipo de temor ante una agresión que hará huir a su posible agresor. Es un producto imprescindible para jóvenes que salgan de noche, ancianos o cualquier tipo de persona. Es mejor que los spray ya que es mas preventivo, se puede utilizar ante cualquier duda ante la presencia de gente sospechosa, y el posible agresor no se sentirá atacado.

Descripción

Alarma personal compacta en caja de plástico negro resistente. Su pequeño tamaño nos permite llevarla en un bolsillo. La unidad es accionada por dos baterías de 1.5V.

Dimensiones totales: 80 x 60 peso de x 18mm

6. Protección Personal

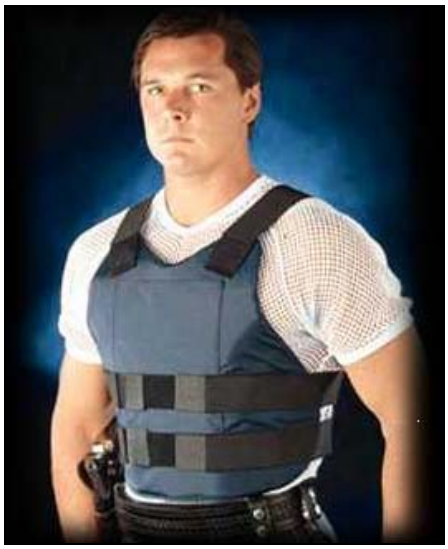


FIG. 2.10 Protección Personal

Protección completa para el cuerpo del hombre; optima protección frontal, posterior y lateral, es liviano, le da comodidad al mismo tiempo que lo protege.

Brinda una protección completa ya que su diseño implementa cubrimiento desde la parte posterior a la parte frontal con ajuste extremo. Su línea de curvas y finos bordes sirven para aliviar los "puntos de presión" que pueden ocasionar irritación en la piel. Este chaleco es anatómicamente correcto y cómodo para usar por prolongados periodos de tiempo. Los hay disponibles para lavar a máquina, portadores desprendibles de poly-algodón. Disponible en negro, azul oscuro, crema y blanco.

7. Escáner de Inspección por rayos X

FIG. 2.11 Escáner de Inspección por rayos X

Equipo de tecnología escáner especialmente diseñado para inspección de correspondencia personal. Sus reducidas dimensiones y peso facilitan su ubicación en cualquier espacio. El tamaño de su túnel de inspección permite cubrir las necesidades en materia de seguridad de pequeñas empresas, altos directivos, organismos oficiales, residencias privadas de personas públicas, partidos políticos, etc.

Características técnicas

Máximo tamaño del objeto a inspeccionar: 300 x 100 x 370 mm.

Peso máximo del objeto a inspeccionar: 4,5 Kg.

Peso del equipo: 39kg.

Funciones para evaluación de armas, cartas y explosivos: dispone además de la función de destello automático de alta densidad.

Monitor en color: 15" de alta resolución y baja radiación.

Presentación en B/N y HI-CAT pseudocolor.

Zoom electrónico: ampliación de 2,3 y 4 veces.

Resolución: hilo metálico de 0,1 mm de diámetro.

Seguridad contra radiaciones: cumple con todas las normativas sanitarias y de radiación aplicables a estos dispositivos.

Seguridad fotográfica: garantizada incluso para películas de alta sensibilidad.

Alimentación: estándar (230VAC±10%).

8. Equipos anti-hurto

FIG. 2.12 Equipos anti-hurto

Los sistemas anti-hurto son el arma más eficaz para poder evitar pequeños hurtos en tiendas y supermercados. Estos sistemas pueden venir equipados con activadores y desactivadores de señal, pueden trabajar con etiquetas duras o blandas, etc. pudiéndose combinar además varias antenas juntas para poder cubrir diferentes anchuras de salidas. Se ha puesto especial atención en que dicho sistema garantice el paso de

productos y personal de forma rápida disminuyendo al máximo el número de falsas señales y evitando así situaciones embarazosas, cuidando la estética de las antenas para no desentonar en su entorno.

9. Sistemas de alarmas

Los sistemas de alarmas, constituyen en la actualidad los sistemas más potentes, más avanzados y más fáciles de usar disponible hoy en día. Incorporan las últimas novedades en cuanto a control y seguridad, aportando todos los avances técnicos que se han ido incorporando en el campo de la seguridad en los últimos tiempos. Las centrales están diseñadas para darle la mayor protección, facilidad y control, con más características de seguridad que cualquier otro sistema de alarma. Además cuentan con la facilidad de instalación de un sistema inalámbrico y la sencillez de manejo gracias a sus mensajes hablados.

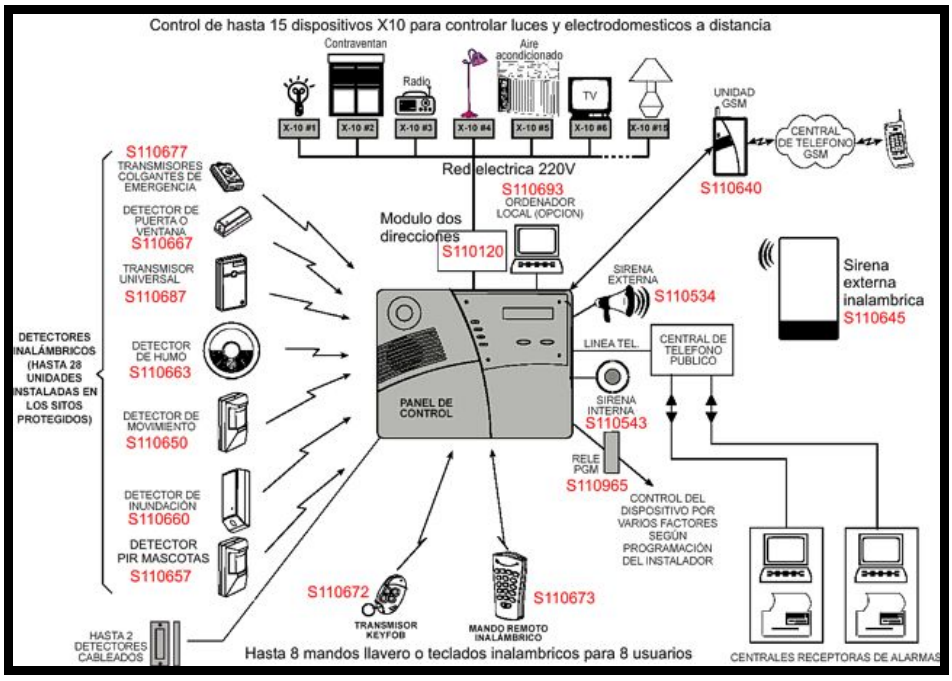


FIG. 2.13 Sistema de alarmas de la marca Power Plus

Características del Sistema de Alarmas Power Plus

28 Zonas vía radio, 2 cableadas, control remoto por teléfono, compatible con central receptora de alarmas, aviso por teléfono y/o busca, sintetizador de voz, grabación de mensajes, alarma de robo e incendio, control de luces y electrodomésticos, compatible x10, display multifunción, batería de respaldo, etc. y todo ello en un módulo pequeño y elegante que puede instalar en cuestión de minutos. Incluyen un mando llavero, 2 sensores infrarrojos, 1 sensor magnético, baterías recargables y la consola central.

10. Sistema de Televigilancia y control

La televigilancia nos permite visualizar en tiempo real cualquier instalación, recinto o evento, básicamente a través de Internet (protocolos TCP/IP).

La televigilancia también se puede realizar a través de RTB (línea convencional), GSM (Sistema global de comunicaciones móviles), aunque estos sistemas plantean un mayor costo de mantenimiento y en algunas ocasiones una baja calidad en el servicio, por lo que siempre que sea posible es preferible basarse en redes TCP/IP.

En general, el abanico de posibilidades es muy amplio y las aplicaciones que podemos desarrollar prácticamente infinitas. Básicamente podemos distinguir dos aplicaciones:

Televigilancia

FIG. 2.14 Grabador digital DVR con disco duro

A parte de explorar la instalación en tiempo real, podemos necesitar ver eventos ocurridos en tiempo anterior, con lo cual necesitamos tener las imágenes grabadas en un disco duro. Normalmente estas instalaciones demandan obtener varias fuentes de imágenes con lo cual hay que instalar varias cámaras. El equipo adecuado para estas aplicaciones es un grabador digital DVR con disco duro. Presentan entradas para varias cámaras (normalmente en grupos de 4: 4/8/16) y aparte de la tarjeta de red, aportan mejoras importantes como la grabación por eventos, detección de movimiento, back up a CD o DVD, niveles de acceso para usuarios, etc.

Control

FIG. 2.15 Cámara de red con servidor Web

Si únicamente necesitamos visualizar de forma aleatoria la instalación, no es necesario tener almacenadas las imágenes en disco duro.

Aplicaciones: control domestico y pequeños negocios. Suele ser suficiente la instalación de una sola cámara. Las cámaras de red con servidor Web incorporado suelen ser el equipo ideal para este tipo de necesidades.

11. Sistema de circuito cerrado de televisión (CCTV)

El sistema de CCTV digital, nos permite conectar cámaras para visualizar/grabar simultáneamente en un computador. Este sistema usa tecnología de detección de movimientos (sin necesidad de contar con sensores) y puede ser configurado para grabar solo cuando son detectados cambios en las imágenes, se ahorra tiempo y costo de grabación continua como en los sistemas tradicionales de CCTV. Estos datos de video son digitalizados, capturados con fecha y hora, comprimidos y conservados en el disco duro de la PC como un archivo para inspección posterior.

Aquí se descarta la grabación permanente en cintas de video (VHS) como los sistemas de video convencionales. Esto también permite la visualización remota y play back por MODEM externo, TCP/IP, IP Multicast e IPX con la aplicación de vista remota o a través de un navegador Web, actuando igual que una Web Cam.

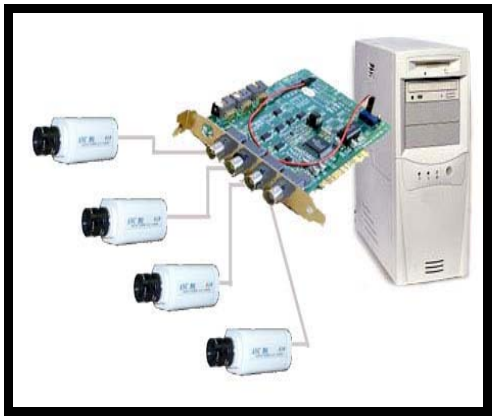


FIG. 2.16 Conexión de las cámaras al CPU de la PC. Receptora

FIG. 2.17 Monitor Receptor de las Imágenes

12. Sistema de control de Acceso Magnético

FIG. 2.18 Control de acceso vía tarjeta magnética

Este sistema consiste en que cada usuario del sistema mediante su tarjeta magnética, de proximidad o SmartCard se identifica en el sistema de acceso de Seguridad.

Estos sistemas responden de una manera rápida y eficaz y pueden ser programados en función de los permisos para cada usuario y dentro de distintos tramos horarios, diarios y semanales. Además, se puede programar el sistema para dar accesos de forma temporal, a usuarios invitados, e incluso avisar mediante mensajes en el display de eventos o recordatorios. Estos sistemas son monitorizados por el sistema de alarma e intrusión.

El software de seguridad permite monitorizar, grabar y archivar cada intento de entrada, cada acceso y cada denegación del mismo. Estos datos se pueden recuperar cuando se desee y ver que áreas han sido accedidas.

FIG. 2.19 Control de acceso vía tarjeta de proximidad o SmartCard

2.2.2. SISTEMA DE SEGURIDAD CONTRA INCENDIOS.

FIG. 2.20 Sensores anti-incendios

Todos los sistemas de seguridad deben incorporan la posibilidad de conectar detectores de humo y de incendio. Estos detectores se monitorizan 24 horas al día, y de esta forma tomar las acciones precisas en caso de emergencia.

Estos sistemas se pueden suministrar como sistemas independientes o integrados dentro del sistema de alarma centralizado.

1. Sistema de corte de gas

FIG. 2.21 Sistema de corte de gas

Este equipo nos avisa automáticamente al recibir una señal del sensor para corte de fluidos avisando de una fuga de GAS y accionando el motor de corte de llave de 1/4 de vuelta

2. Detector óptico analógico de humo

FIG. 2.22 Detector óptico analógico de humo

Los detectores ópticos analógicos de humos ofrecen una sólida base para el desarrollo de instalaciones de protección contra incendios, por su fiabilidad, su atractivo diseño y su perfil reducido de 43 mm incluida la base. Son compatibles con todas las bases analógicas.

El consumo en reposo es altamente reducido por lo que no se sobrecargan las capacidades del lazo. La respuesta ante partículas de humo, hace que el mismo sea un sensor muy eficaz para la mayor parte de los fuegos.

El revolucionario diseño de la cámara ayuda a detectar las partículas de humo, eliminando corrientes y partículas confusas del aire, dotando al dispositivo de la máxima fiabilidad.

La protección ante suciedades y partículas extrañas, se realiza mediante un filtro de lámina desmontable que reduce la suciedad del equipo y facilita su

mantenimiento. La localización del equipo en alarma es muy sencilla al disponer de un doble LED de alarma, haciendo visible en todo momento el estado del equipo de alarma y comunicación. El parpadeo de comunicación puede eliminarse por software.

3. Sistemas de Bombas Contra Incendios y extintores de fuego

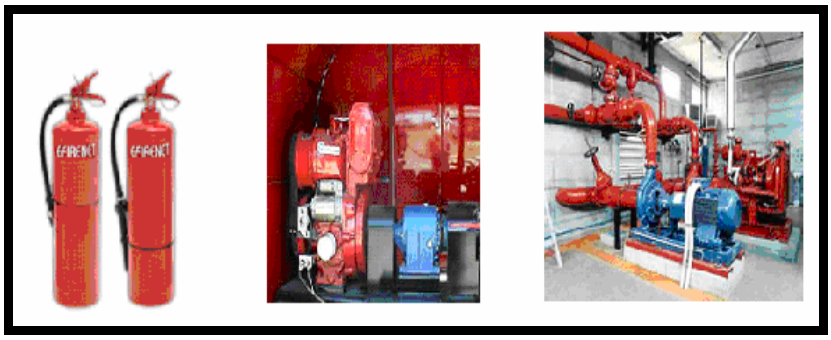


FIG. 2.23 Sistemas de Bombas Contra Incendios y extintores de fuego

Los sistemas de bombeos o casa de bombas así como los denominados extintores se utilizan para extinguir los grandes y pequeños incendios.

Los extintores tienen eficacia para lograr el control de un fuego en los primeros momentos de producido pero de no ser así se debe de hacer uso de las bombas contra incendios las que deben estar minuciosamente estudiados en cuanto a su caudal y presión para poder eliminar el incendio.

Su selección y uso para cada tipo de fuego, deber ser conocida y practicada por la mayor cantidad de personas posibles.

De ello dependerá que el principio de incendio no se propague, evitando la posible pérdida de vidas y de bienes. Los extintores deben ser colocados

en lugares accesibles, libres de toda clase de obstáculos, donde habitualmente no se almacenen mercaderías, cajones o equipajes, que impidan o dificulten el empleo de los mismos.

4. Sistemas detectores de llama

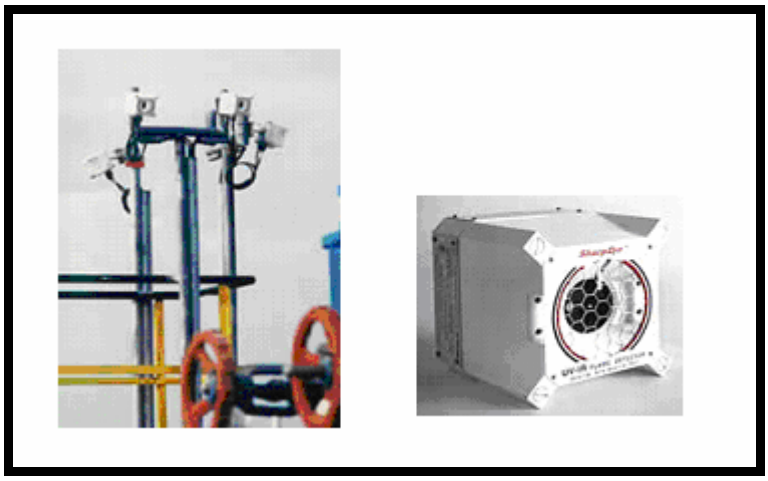


Fig. 2.24 Sistemas detectores de llama.

Los detectores de llama permiten una rápida y segura captación del fuego por medio de la sensibilidad a la radiación emitida por la llama.

Los principales usos de los detectores de llama son los siguientes:

- Detección de incendios en áreas de líquidos y gases inflamables de combustión pura como petróleo, solventes polares, kerosén y butano, donde existe un crecimiento rápido de fuego intenso.

- Los sistemas de detección de llama son adecuados para la protección de instalaciones petroquímicas, plataformas de petróleo, cabinas de pintura, etc.

2.2.3. SISTEMAS DE SEGURIDAD ESPECIAL.

Generalmente al pensar en seguridad se nos viene a la mente solo la seguridad de nuestros bienes (sea casa o una empresa, si fuera el caso), pero nos olvidamos de la seguridad pública la cual también afecta a nuestra integridad.

Si consideramos el hecho que, cuando viajamos, sería bueno que las personas fueran revisadas para asegurarnos que no porten armas o drogas; o en el caso de un gran escape de gas (de cualquier tipo), etc. Estos y muchos más ejemplos son los que estamos considerando como Seguridad Especial.

1. Detector de metales de mano

FIG. 2.25 Detector de metales manual

Detector de metales fabricado en plástico antigolpes especialmente diseñado para detección de armas y metales, recomendado para todos los lugares de gran afluencia de publico, como los estadios de fútbol, pabellón de deportes en general, discotecas, teatros etc.

Detecta el lugar donde se esconden pistolas, cuchillos, joyas y metales.

Un indicador sonoro avisa de la detección en el punto exacto donde se oculta, al mismo tiempo se enciende un led rojo.

2. Detector de Monóxido de Carbono (CO)

FIG. 2.26 Detector de monóxido de carbono

Todos los años fallecen personas por culpa del monóxido, cuando es tan sencillo disponer de un detector. El Monóxido de Carbono es un gas insípido, inodoro, y de una toxicidad mortal, imposible de percibir por el ser humano.

Este detector le avisa de la más mínima concentración de monóxido de carbono que se pueda producir en la vivienda ó lugar cerrado. No necesita batería, se alimenta directamente a 220VCA 50/60Hz.

No debe de faltar en cualquier instalación de los sistemas de seguridad, avisándonos de posibles riesgos mortales.

3. Sensor para corte de motor de fluidos (agua, gas)

FIG. 2.27 Sensor para Corte de motor de Fluidos

Características

- Corta al instante los suministros de agua ó gas de la vivienda al recibir una señal de fuga.
- Adaptable a cualquier tipo de tubería.
- Fácil instalación.
- Protección contra radiaciones electromagnéticas.
- Tres modelos adaptables a las distintas posibles tuberías.
- No se requiere intervención en las instalaciones, debido a su uso externo.
- Botón de rearme MANUAL disponible.

Especificaciones

Alimentación: 12 V DC

Consumo: 0,75W

Temperatura de Trabajo: -20/50º C

Humedad de Trabajo: 0/95% humedad relativa

Peso: 370gr.

Tiempo de Maniobra: aproximadamente 8 seg.

Angulo de Giro: 90º

Fuerza de rotación: 70Kg/cm.

Chasis ABS

4. Sensor Detector de inundaciones

FIG. 2.28 Sensor detector de inundaciones

Detecta la más mínima fuga de agua, es de fácil y cómoda instalación, funciona con pila de 9 ó 12 Voltios. No debe de faltar en cualquier instalación de un sistema de seguridad, avisándonos de posibles inundaciones.

Ideal para ser instalada en: viviendas, colegios, hoteles, residencias, etc. Dispone de alarma acústica (80db) y señal de reemplazo de pila.

5. Detector de drogas y explosivos

FIG. 2.29 Detector de drogas y explosivos

Este equipo está basado en la espectrometría de movilidad iónica. Mediante esta técnica innovadora se consigue identificar drogas y explosivos escondidos en bolsos, maletas, maletines con gran fiabilidad, precisión y exactitud. Y todo ello a tiempo real, ya que estos equipos sólo necesitan 6 segundos para detectar e identificar drogas y explosivos. Además el equipo destaca por su gran flexibilidad, pudiendo programarse fácilmente para la localización de nuevas sustancias

CAPITULO 3

SITUACIÓN ACTUAL DE LA URBANIZACIÓN “PUNTA PANORAMA”.

En este capítulo se dará una descripción de la ubicación geográfica de la urbanización, así como de su infraestructura y se hablará sobre la empresa que actualmente presta los servicios de seguridad.

3.1. DESCRIPCIÓN DE LA UBICACIÓN DE LA URBANIZACIÓN.

La Urbanización Punta Panorama se encuentra en el Cantón de Duran parroquia Eloy Alfaro en el Km. 5 1/2 de la vía Duran-Babahoyo frente a la Feria Ganadera de Duran y tiene un área total de 15.100 m^2, lo cual se puede observar en el siguiente plano.

Posterior a la figura detallaremos la ubicación de la urbanización.

A la izquierda de la urbanización está la ciudadela Panorama, aquí encontramos nueve viviendas cuyo frente lindera con la ciudadela antes mencionada, dichas viviendas no están dentro del cerramiento de la urbanización.

A la derecha de la Urbanización lindera con unos terrenos baldíos.

Y por ultimo en la parte posterior de la urbanización encontramos la ciudadela Panorama.

FIG. 3.2 Entrada Principal a la urbanización

FIG. 3.3 Lindero lateral posterior derecho de la urbanización

FIG. 3.4 Lindero lateral frontal derecho colindante con la urbanización Punta Panorama

FIG. 3.5 Lindero derecho de la ciudadela

FIG. 3.6 Salida de emergencia, ubicada en el lindero izquierdo de la ciudadela

3.2. CARACTERÍSTICAS E INFRAESTRUCTURA DE LA URBANIZACIÓN.

La ciudadela Punta Panorama cuenta con los servicios públicos básicos como son: energía eléctrica, servicio de agua potable y alcantarillado.

Esta urbanización tiene un cerramiento de aproximadamente dos metros y medio, el mismo que nos sirve de limitador y como medio de protección para la gran mayoría de las viviendas excepto para nueve, que son de una planta y que su ingreso principal da hacia la ciudadela Panorama.

La urbanización tiene una garita en la entrada principal y una salida de emergencia en la parte lateral derecha de la urbanización.

Está urbanización está conformada por sesenta y ocho viviendas de tres modelos, las cuales están distribuidas de la siguiente manera: 18 viviendas de una planta con dos dormitorios (modelo Carla), 41 viviendas de una planta con tres dormitorios (modelo Camila) y 9 viviendas de dos plantas con tres dormitorios (modelo Karina), además de una casa comunal.

A continuación tenemos la distribución y ubicación de los modelos antes mencionados y las fotografías de cada una de ellas:

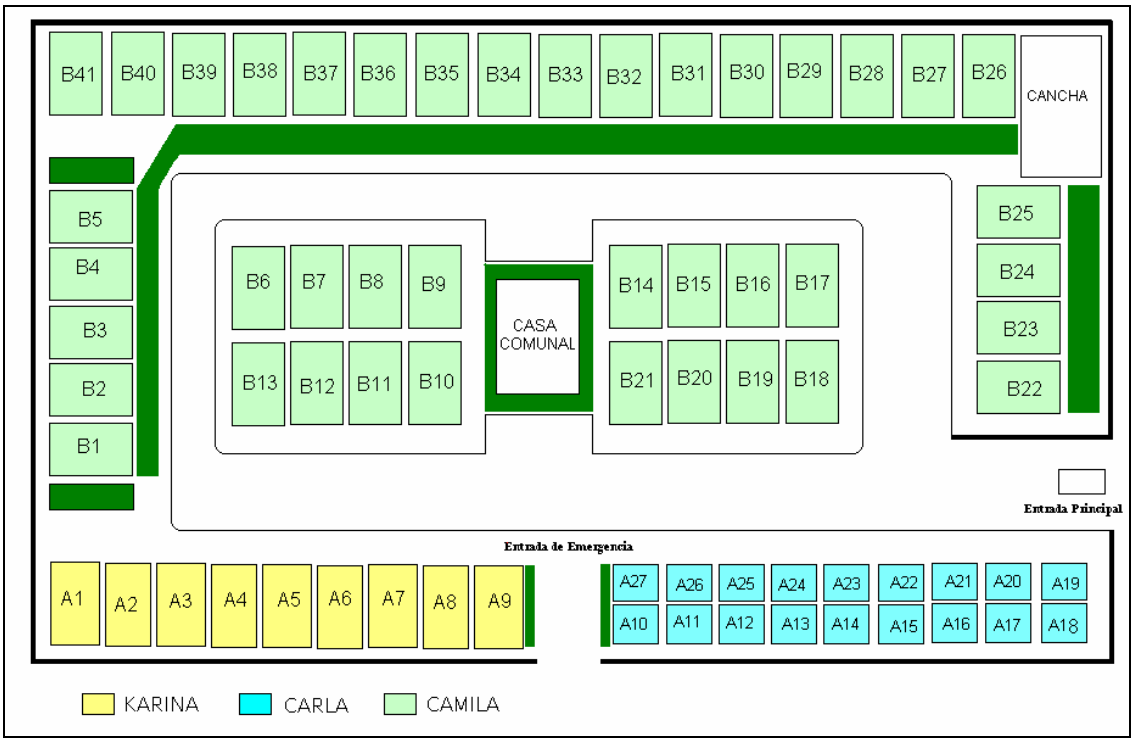


FIG. 3.7 Distribución de las viviendas por modelo

FIG. 3.8 Vivienda de dos dormitorios - CARLA

FIG. 3.9 Vivienda de tres dormitorios – CAMILA

FIG. 3.10 Viviendas de dos plantas y tres dormitorios - KARINA

3.2.1. DESCRIPCIÓN DEL ÁREA COMUNAL.

FIG. 3.11 *Vista frontal del* Área Comunal.

Esta urbanización tiene una casa comunal, donde se realizan las reuniones de la cooperativa, también se realizan eventos sociales como cumpleaños, misas y en el futuro se construirá un dispensario médico para los habitantes de la urbanización; además cuenta con un área para juegos infantiles, como se puede observar en las figuras 3.11 y 3.12.

FIG. 3.12 Parte Posterior del área comunal

3.3. SITUACIÓN ACTUAL DE LA SEGURIDAD.

En la urbanización la seguridad esta dada por la vigilancia de dos guardias, uno en la entrada principal mientras que el otro vigila por cierto periodo de tiempo la salida de emergencia y ronda alrededor de la ciudadela.

La guardianía es durante veinticuatro horas en turnos rotativos que son de seis y media de la mañana a seis de la tarde en grupo de dos. Los guardias pertenecen al empresa SEGUEN S.A., es una empresa líder en la prestación de servicios profesionales de Seguridad Física, Seguridad Electrónica, consultoría, auditoria, capacitación y manejo de crisis en el área de la seguridad integral, a personas naturales o jurídicas, combinan sus conocimientos con la experiencia adquirida durante el tiempo que estuvieron al servicio de Instituciones de Seguridad Nacional e Inteligencia Militar del Estado Ecuatoriano.

Para otorgar estos servicios de vigilancia la empresa cuenta con los siguientes permisos de funcionamiento:

- Permiso de frecuencias.
- Permiso del Comando Conjunto de las FF.AA.
- Autorización otorgada por el Ministerio de Gobierno.
- Permiso de Tenencia de Armas.
- Superintendencia de compañías.
- RUC actualizado.
- Contraloría (Certificado de no ser contratista incumplido).

3.3.1. COSTOS.

Cada propietario que a su vez es empleado del Banco de Guayaquil tiene que pagar mensualmente treinta dólares por la guardianía, estos son descontados del rol de pago de dicho empleado.

3.3.2. FALLAS DE LA SEGURIDAD.

A pesar que se cuenta con la vigilancia física esto no es suficiente para la protección de las viviendas ya que por el costo solo tenemos dos vigilantes. Mientras uno de ellos esta en la garita y el otro guardia cuida la puerta de emergencia no hay quien vigile la parte izquierda de la ciudadela. Estos

guardias tienen que subirse en escaleras para poder ver el lindero izquierdo de la urbanización y como no hay reflectores hacia fuera de la urbanización, por la noche no se puede divisar bien esta parte de la urbanización.

Otra de las fallas que tiene es que se necesitan puntos de vigilancias altas es decir panorámicas de esta manera la cobertura de vigilancia seria mayor

Aun así es complicada la vigilancia por lo que creemos que un sistema de seguridad híbrido (cableada e inalámbrica) con tecnología IP es una de las mejores opciones para proteger la urbanización, en este momento donde ningún punto de la ciudad es completamente seguro justificará su implementación y costo.

3.3.2.1. ESTADÍSTICAS DE LOS ROBOS.

Esta ciudadela fue inaugurada en el mes de Marzo del 2004, desde esa fecha hasta hoy han ocurrido cuatro robos en las casa ubicadas al lado derecho de la ciudadela que lindera con unos terrenos desocupados o baldíos.

Primer asalto

Ubicación: Vivienda B30

Fecha: Junio de 20004

Hora: 21 horas

Objetos sustraídos: dvd, licuadora, arrocera, radio, ropas con maletas.

Segundo asalto

Ubicación: vivienda B12

Fecha: Octubre de 2004

Hora: 14 horas

Objetos sustraídos: Dvd, ropa, canguilera, licuadora.

Tercer asalto

Ubicación: Vivienda A27

Fecha: Enero de 2005

Hora: 11 horas

Objetos sustraídos: dvd

Cuarto asalto

Ubicación: Vivienda B40

Fecha: Enero de 2005

Hora: 02 horas

Objetos sustraídos: televisor, grabadora, radio, ropa, licuadora.

La cantidad de objetos sustraídos no llegaron a ser mayores debido a que tenían que ser pasados por encima del muro que sirve de cerramiento que lindera con los terrenos baldíos.

Debido a no contar con una iluminación adecuada y una vigilancia directa sobre este muro sucedieron estos robos.

3.4. MEJORAS ACTUALES A LA SEGURIDAD.

Por los robos que han sucedido, los miembros de la cooperativa del Banco de Guayaquil y propietarios de las viviendas de la urbanización decidieron colocar sobre el cerramiento (excepto en la parte frontal) de la urbanización, un cerco eléctrico para así poder salvaguardar sus intereses y reducir la frecuencia de los atracos, lo que se puede observar en la siguiente figura 3.12.

Cercado eléctrico

FIG. 3.13 Muro con cerco eléctrico

CAPITULO 4

DISEÑO DEL SISTEMA DE SEGURIDAD PARA LA URBANIZACIÓN UTILIZANDO TECNOLOGÍA IP: INALÁMBRICA Y CABLEADA.

En este capítulo se empezará con un enfoque del diseño general del sistema para poder tener una idea a lo que se desea llegar, se realizará una descripción del sistema de seguridad aplicado a la urbanización, en donde para su entendimiento se lo ha dividido en tres bloques.

Luego se tratarán los componentes a utilizarse tanto en la vivienda como en el centro de gestión y en el área perimetral, sus características, configuración, etc. Así como también se determinará su ubicación física mediante los planos, tanto de cada uno de los modelos de las viviendas como del plano general de la urbanización.

Y por último se deducirán dos parámetros importantes que se deben de considerar para la elaboración del diseño del sistema de seguridad.

4.1. DISEÑO GENERAL DEL SISTEMA DE SEGURIDAD.

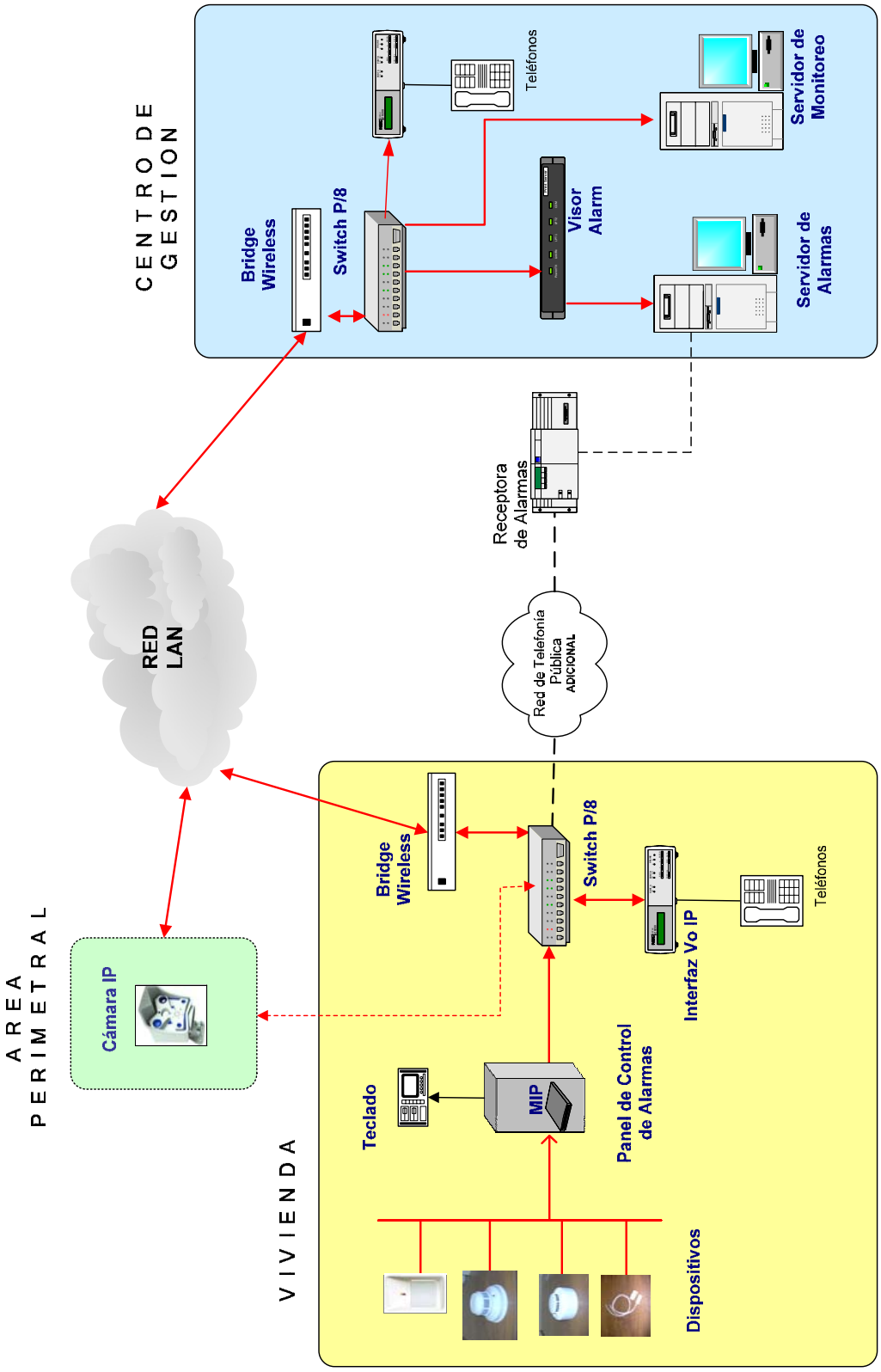


FIG. 4.1 Diseño general del sistema de seguridad

El diseño del sistema de seguridad está basado en la transmisión multimedia con tecnología IP, para la urbanización Punta Panorama, el mismo que debe cumplir con lo siguiente:

- Captación de las señales emitidas por los sensores de seguridad instalados en las viviendas de dicha urbanización.
- Emisión de dichas señales, mediante una red inalámbrica desde cada vivienda hasta el centro de gestión para su monitoreo.
- Captación de las señales de video por medio de cámaras IP.
- Emisión de las señales de video, vía inalámbrica hasta el centro de gestión.
- Comunicación entre el centro de gestión y cada vivienda vía interfaz IP.

Por lo tanto el desarrollo de este trabajo, comprende en la recepción de las señales: vía sensores, cámaras e intercomunicadores IP; las mismas que serán transmitidas hacia el centro de gestión, para su respectiva decodificación y monitoreo de las mismas. Basándonos en esto, el proyecto se lo divide en tres bloques los mismos que están entrelazados por el sistema de transmisión señales IP:

- ***Descripción y diseño del sistema de seguridad de la vivienda.***
- ***Descripción y diseño del sistema del centro de gestión.***
- ***Descripción y diseño del sistema de seguridad perimetral.***

4.1.1. DESCRIPCIÓN DEL SISTEMA APLICADO A LAS VIVIENDAS.

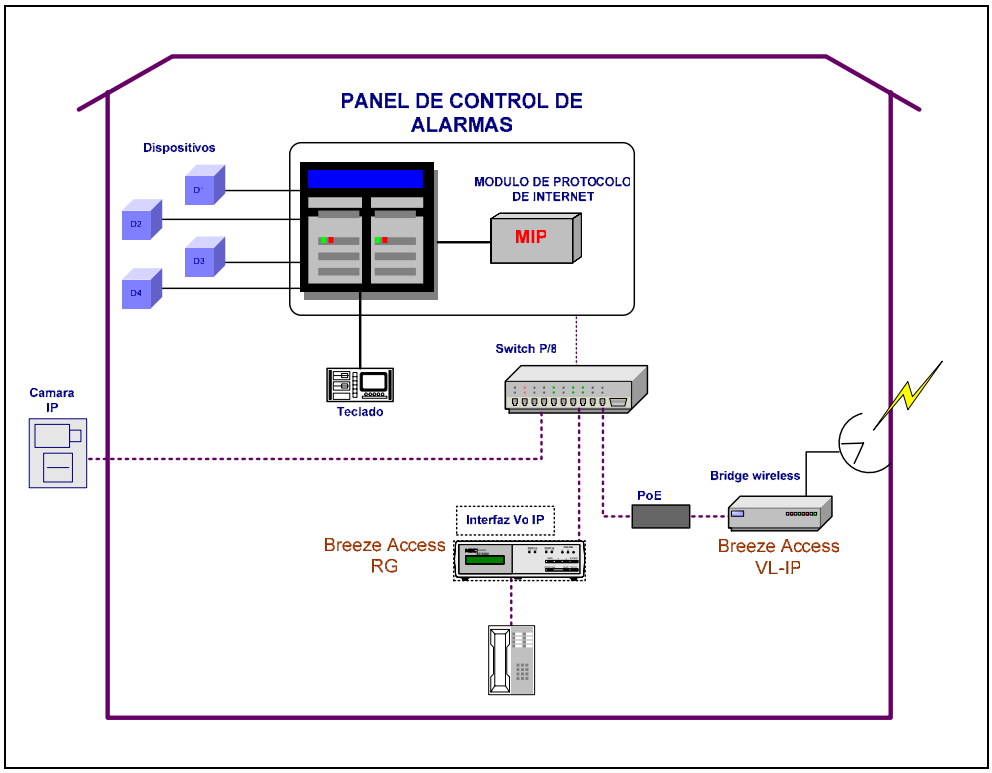


FIG. 4.2 Diagrama del sistema de seguridad aplicado en la vivienda

Este primer bloque consiste de un sistema de alarmas alámbrico, el cual estará conformado con dispositivos de alarmas como son: detector de movimiento, detector de humo, detector térmico y contactos magnéticos; los cuales su conexión será llevada al panel control.

En el panel de control se instalará una tarjeta que servirá de interfase con los demás equipos, llamada MIP (Módulo de protocolo de internet), y adicionalmente se conectará el teclado de mando que servirá para las diferentes programaciones que el usuario disponga, así como su activación y desactivación del sistema.

Esta tarjeta MIP realizará dos tareas:

1. Capturar las alarmas que envía el panel de alarmas y mandarlas por la red IP a la que se conecta. Estas alarmas son recibidas por el equipo receptor para su envío al correspondiente software de automatización (Sw. de Automatización).

2. Generar el tráfico de supervisión para que ambos extremos del entorno de seguridad comprueben la conectividad IP, que es la que permite que se pueda realizar la tarea anterior.

Este dispositivo también interceptará la conexión telefónica del panel de alarmas con dos fines, detectar cuando el panel envía una alarma y así capturarla para enviarla por la red IP a la que se conecta y por otra parte permitir el uso de de la línea telefónica al mismo tiempo que se envían las alarmas.

Para esto se instalará una interfaz telefónica que servirá para la intercomunicación entre copropietarios y el centro de gestión. Este equipo tiene la particularidad de permitir instalar un teléfono convencional o IP.

Considerados los equipos de servicios para las viviendas, se adicionó la instalación de las cámaras IP en ciertas casas, esto dependerá de la cercanía en que se encuentra la cámara preubicada a la vivienda.

Con esto solo faltaría el envió de las señales al centro de gestión. Para ello, se utilizará un bridge inalámbrico, el cual por medio de una antena omnidireccional se transmitirán o receptarán (dependiendo del caso) las señales al centro de gestión.

Finalmente se instalará un switch de 8 puertos, el cual permitirá la convergencia de las señales de los diferentes equipos instalados (panel, interfaz telefónica, bridge inalámbrico y en ciertos casos la cámara IP).

4.1.2. DESCRIPCIÓN DEL SISTEMA APLICADO AL CENTRO DE GESTIÓN.

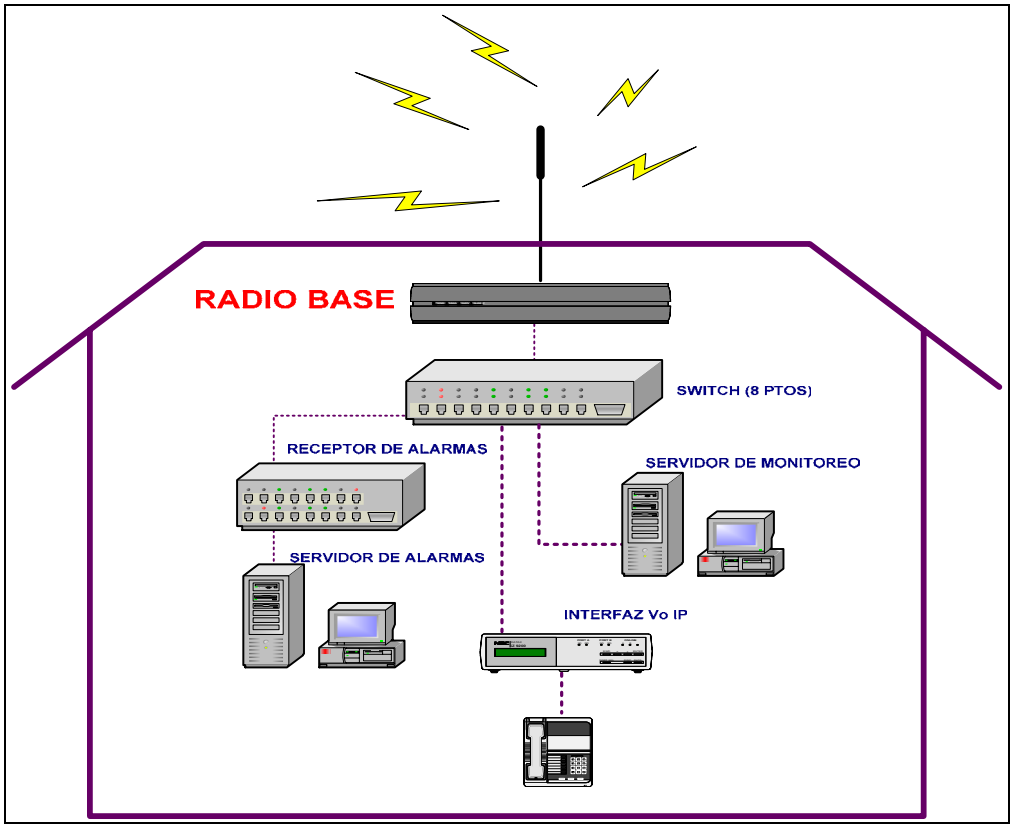


FIG 4.3 Diagrama del sistema aplicado al centro de gestión

Una vez de que las señales emitidas desde las viviendas son recibidas por el punto de acceso o radio base, éste las envía a los equipos decodificadores, a través del switch marca Dlink modelo DES-1008D de 8 puertos no gestionable vía interfaz RJ45, el cual garantiza la disponibilidad de puertos de conexión para la conexión de los siguientes equipos:

La conexión del equipo Receptor de Alarmas (VisorALARM), equipo que mediante un software de automatización propietario nos permitirá la recepción de las alarmas desde los equipos suscriptores. Este receptor de alarmas previo a su uso se debió haber configurado para que funcione como una receptora Ademco según la marca del sistema de alarmas instalado en la vivienda del usuario. Para nuestro proyecto se ha elegido un sistema de alarmas de la marca Ademco que funciona mediante el sistema operativo Contact ID, así también se debió haber configurado los MIPs que serán monitoreados desde la receptora VisorALARM.

Una vez instalado el receptor de alarmas VisorALARM, se procederá a instalar la interfaz de telefonía IP que administrará al resto de interfaces instaladas del lado de los usuarios, dicha configuración se logrará mediante un software propietario el mismo que nos permitirá la comunicación inalámbrica entre todos los miembros suscriptores de la vivienda sin tarifación para los propietarios de las mismas. Esta interfaz mediante el software de gestión, podrá realizar el ruteo de la comunicación entre un usuario que haga una llamada y el usuario con el cual se desee comunicar, todo ello administrado desde el centro de gestión.

Para finalizar, se conectará el servidor de video, el cual previa la instalación de un software de configuración del proveedor de las cámaras IP, nos permitirá tener acceso a todas las imágenes en tiempo real transmitidas desde dichos dispositivos previamente instalados en los puntos estratégicos de la urbanización.

4.1.3. DESCRIPCIÓN DEL SISTEMA APLICADO AL AREA PERIMETRAL.

Además de la seguridad que se aplica a cada uno de las viviendas o subscriptores, se aplicará seguridad perimetral, inicialmente con un cerco electrificado (el cual ya se encuentra instalado) y ahora con un sistema de monitoreo el cual constará de 6 cámaras IP que supervisarán las 24 horas, éstas serán conectadas a la red de la urbanización en zonas específicas previamente analizadas.

Esto se lo puede observar en las figuras 4.1 y 4.2.

A continuación detallamos cada uno de estos sistemas con sus componentes, características y diseño, además de su ubicación.

4.2. EQUIPAMIENTO UTILIZADO EN EL DISEÑO.

A continuación se detallará las diferentes características, funciones y forma de conexión de los dispositivos y equipos que van hacer instalados en los tres bloques antes ya mencionados. Las especificaciones técnicas e información complementaria se las indicará en un apéndice adjunto.

4.2.1. COMPONENTES DEL SISTEMA DE SEGURIDAD PARA LAS VIVIENDAS.

Debemos dar a conocer la lista de los dispositivos y equipos a instalarse en las viviendas, estos equipos son de seguridad, transmisión multimedia y transmisión inalámbrica.

4.2.1.1. PANEL DE CONTROL DE LAS ALARMAS.

En el mercado existe una gran gama de paneles de control, los cuales satisfacen los diferentes requerimientos que el usuario necesita facilitando de esta manera la elección del mismo.

Para nuestro diseño se escogió la marca Ademco debido a su liderazgo en el mercado ecuatoriano, además de cumplir con uno de nuestros principales requerimientos, que es la compatibilidad con el módulo de protocolo de internet el cual maneja el protocolo Contact ID.

A continuación se mostrará un cuadro comparativo entre 3 marcas y 3 parámetros principales, para así reforzar nuestra elección.

MARCA	PROTOCOLO CONTACT ID	# ZONAS	# CODIGOS
PIMA	Bajo	Medio	Bajo
SYSCOM	Alto	Medio	Medio
ADEMCO	alto	alto	Alto

Tabla 4.1 Cuadro comparativo de tres diferentes Paneles de Control

Luego de está introducción procedemos a la descripción de este equipo.

FIG. 4.4 Panel de Control de alarmas

Este panel de control de alarmas es un equipo que va a controlar los diferentes dispositivos alámbricos, es donde se determina las distintas zonas (particiones) de armado y supervisión y va conectado el módulo de protocolo de Internet.

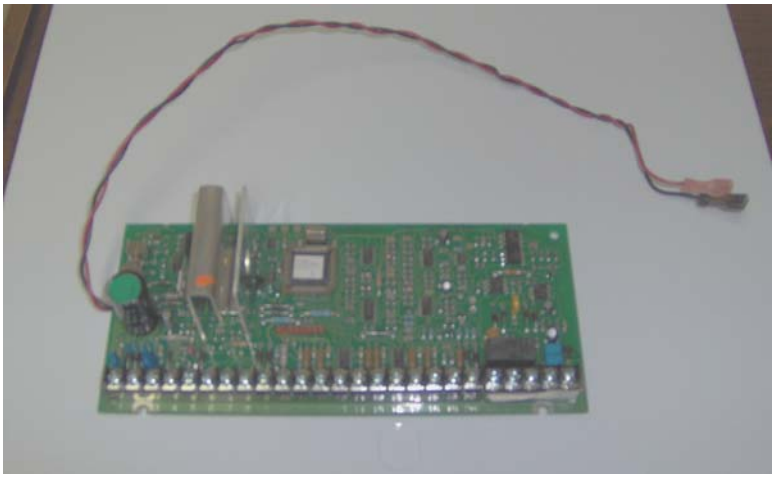


FIG. 4.5 Tarjeta principal del panel de control

MARCA: ADEMCO Internacional

MODELO: VISTA-48

Características

- 8 zonas básicas alámbricas, expandible hasta 48 zonas en total (alámbricas o inalámbricas).
- 3 áreas independientes, de las cuales una puede ser seleccionada como área común.
- 48 códigos de usuario, cada uno con niveles asignables de autoridad.
- Código de emergencia (en caso de sabotaje).
- Compatible con dispositivos inalámbricos de la serie 5800 de Ademco (hasta 40 zonas).
- Controlado por reloj de tiempo real y con capacidad en memoria de 250 eventos.
- Monitoreo de falla mediante línea telefónica.
- Agendas Hora/Día para usuarios: entradas, salidas; con periodos de tiempo para activación/desactivación automática.
- 2 Salidas programable de voltaje en la tarjeta principal.

Conexión de los Teclados

1. Conectar los teclados a los terminales de la unidad de control como se muestra en la siguiente figura :

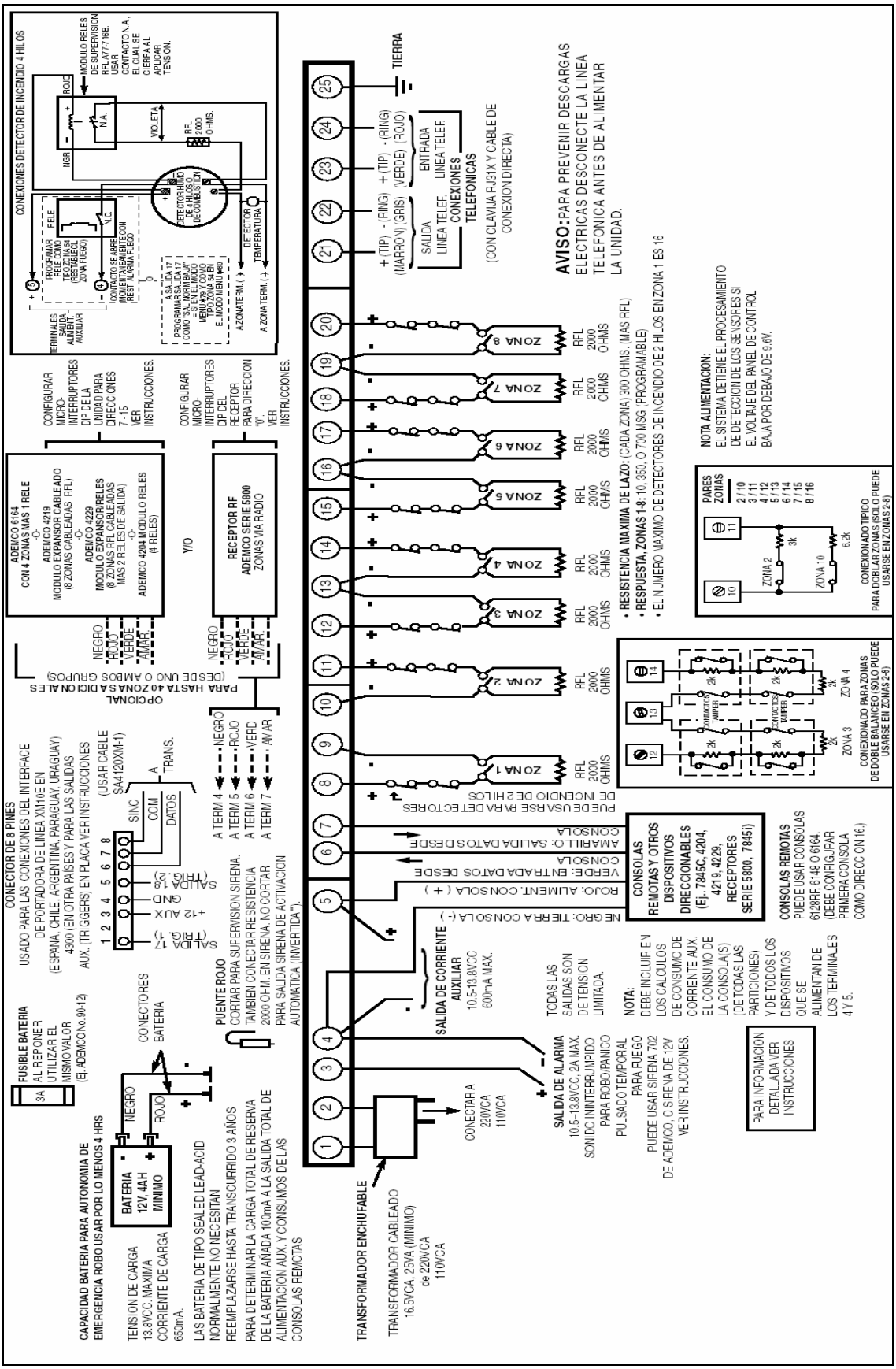


FIG. 4.6 Diagrama de conexiones del Panel de Control

Y determinar el tamaño del cable en base a la tabla de tendidos de cables mostrada a continuación:

Sección Cable	Consumo total de todos los dispositivos conectados al mismo tendido de cable				
	50 mA o menos	100 mA	300 mA	500 mA	600 mA
0.6 mm OD	152 m	76 m	24 m	15 m	13 m
0.8 mm OD	228.6 m	116 m	40 m	24 m	20 m
1.0 mm OD	396 m	198 m	67 m	40 m	35 m
1.2 mm OD	457 m	305 m	100 m	70 m	52 m

Tabla 4.2 Tabla tendidos de cable para equipos – consumiendo alimentación auxiliar del Panel de Control (12 V_+ y 12 V_-)

2. Configurar la dirección de las consolas. Refiérase a las instrucciones de configuración de direcciones incluidas con las consolas y configure la dirección de equipo de cada consola según la tabla siguiente:

CONSOLA	DIRECCION
No. 1	16*
No. 2	17
No. 3	18
No. 4	19
No. 5	20
No. 6	21
No. 7	22
No. 8	23

Tabla 4.3 Direcciones de consolas

***** La dirección de la primera consola es 16, que está siempre habilitada y configurada para la partición 1 con todas las opciones acústicas activadas (on).

3. Programar las direcciones de la consola, asignación de particiones y opciones acústicas en los campos de datos del *190-*196.

Alimentación Suplementaria (opcional)

1. Conecte como se indica. Asegúrese de conectar el terminal negativo (–) en la fuente de alimentación al terminal 4 (AUX –) en el panel de control.

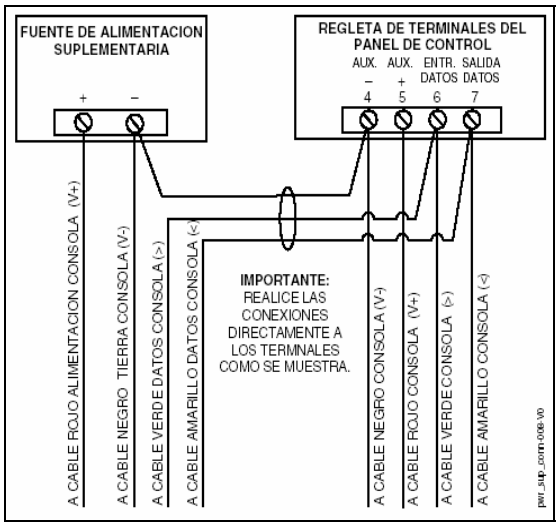


FIG. 4.7 Fuente de alimentación suplementaria

Las consolas alimentadas desde fuentes que no tienen una batería de reserva no funcionarán si se pierde la alimentación C.A. Hay que asegurarse de alimentar por lo menos una consola de cada partición desde la salida de alimentación auxiliar del panel de control.

Zonas Cableadas Básicas

Zonas Normalmente Abiertas /Normalmente Abiertas RFL

1. Los dispositivos de circuito abierto se conectan en paralelo a través del lazo; para zonas RFL, se conecta la RFL entre los hilos del lazo en el último dispositivo.

2. Se habilita zonas normalmente abiertas/RFL usando el modo de Programación de Zonas, en la pantalla “Tipo Cableado”.

Zonas Normalmente Cerradas/Normalmente Cerradas RFL

1. Los dispositivos de circuitos cerrados se conectan en serie con el lado positivo (+) del bucle; para zonas RFL, conectar la RFL en serie después del último dispositivo.

2. Se habilita zonas normalmente cerradas/RFL usando el modo de Programación de Zonas, pantalla “Tipo Cableado”.

Doble-Balanceo: son conexiones según se muestra en la figura a continuación (las resistencias son facilitadas para un dispositivo en los modelos seleccionados); donde su capacidad máxima es de 8 detectores en cada zona de doble balanceo.

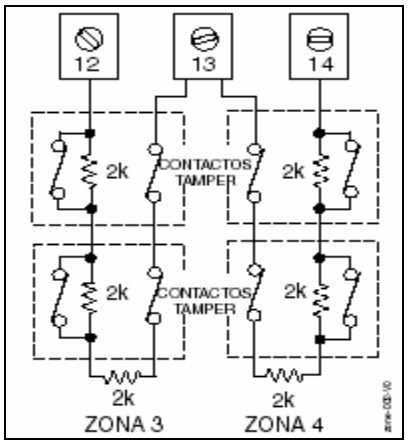


FIG. 4.8 Zonas de doble balanceo

IMPORTANTE: Las zonas de doble balanceo proporcionan una señal de sabotaje (tamper) única en los mismos 2 hilos utilizados para las

señales de alarma, y sólo deberían utilizarse como zonas de robo o de emergencia. No utilizar zonas de doble balanceo en las zonas asignadas para la activación de los detectores de humo.

Duplicación de Zonas: Esta característica proporciona dos identificaciones de zona únicas para detectores normalmente cerrados conectados a cada zona cableada básica (pero no aumenta el número total de zonas soportado por la unidad de control). Si se habilita (modo Programación de Zonas, pantalla “Tipo Cableado”, opción “3”), las zonas cableadas básicas se emparejan automáticamente como sigue:

Zona	Emparejada con Zona
2	10
3	11
4	12
5	13
6	14
7	15
8	16

Tabla 4.4 Emparejamiento de zonas

Conexiones según se muestra (resistencias suministradas):

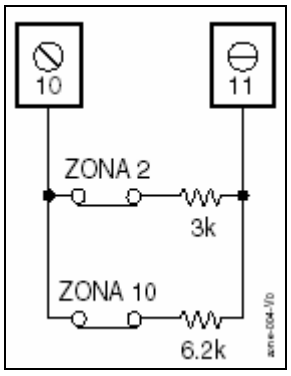


FIG. 4.9 Duplicación de zonas

Conexiones de Medio de Comunicación Alternativo (ACM)

Conecte los terminales de entrada de datos/salida de datos y de entrada de voltaje del ACM a los puntos de conexión de la consola del panel de control. Configure la dirección del ACM como “03” siguiendo las instrucciones incluidas con el ACM.

ADEMCO Contact ID

Los Informes de ADEMCO y Robofon Contact ID tienen el siguiente formato:

CCCC(CCCCCC) Q EEE GG ZZZ, donde:

CCCC(CCCCCC): Identificación (ID) Cliente (abonado) de 4 dígitos o 10 dígitos

Q: Cualificador de Evento de 1 dígito, donde:

E = Nuevo Evento, y R = Restablecimiento

EEE: Código Evento de 3 dígitos (hexadecimal) para una lista completa de códigos de eventos)

GG: Número de Partición de 2 dígitos (los mensajes del sistema muestran “00”)

ZZZ: Zona de 3 dígitos/número contact ID transmitiendo la alarma, ó número de usuario para informes de apertura/cierre. Los mensajes de estado del sistema (Pérdida C.A., Prueba de Paso, etc.) contienen ceros en la localización de la ZZZ.

Código	Definición
110	Alarma incendio
121	Coacción
122	Alarma, 24 horas silenciosa
123	Alarma, 24 horas audible
131	Alarma, perímetro
132	Alarma, interior
134	Alarma, Entrada/Salida
135	Alarma, tipo zona 5
143	Alarma, módulo expansor
144	Alarma sabotaje sensor
145	Alarma sabotaje tapa módulo ECP
146	Alarma Robo silencioso
150	Alarma, 14 H auxiliar/zona supervisión
162	Alarma gas
301	Pérdida alimentación CA
302	Baja batería sistema/fallo Test batería
305	Reposición sistema (sólo registro)
321	Fallo supervisión sirena
333	Avería, supervisión módulo expansor
341	Avería, sabotaje tapa ECP
344	Detección Jam receptor RF
351	Fallo línea telefónica
353	Avería medio comunicación alternativo
354	Fallo de comunicación (sólo registro)
373	Avería lazo fuego
374	Alarma error salida
380	Avería tipo zona 5
381	Supervisión transmisor RF

Código	Definición
383	Sabotaje transmisor RF y sabotaje Zona Doble-Balanceo
384	Baja batería Transmisor RF
393	Alerta limpieza (sólo detectores humo ESL)
401	Desconexión, conexión Total, conexión máxima
403	Conexión/desconexión Total Calendarios
406	Cancelación por usuario
407	Conexión/desconexión remota
408	Conexión rápida Total
409	Conexión/desconexión mediante llave Total
441	Desconexión/conexión Parcial/Instant, conexión rápida Parcial/Instant
442	Conexión/desconexión mediante llave Parcial
461	Código incorrecto (bloqueo teclado activado)
570	Anulación
601	Prueba comunicador manual
602	Prueba comunicador periódica
606	Sigue verificación audible de alarmas (AAV)
607	Modo prueba de paso acceso/salida
623	Registro de eventos lleno al 80%
625	Ajuste reloj interno (sólo registro)
627	Acceso al modo programación (sólo registro)
628	Salida del modo programación (sólo registro)
750-789	Reservado para códigos de informe de tipos de zona configurables
801	Ignorar conexión tamper (sólo registro)
802	Ignorar conexión baja batería (sólo registro)
803	Ignorar conexión pérdida CA (sólo registro)
804	Ignorar conexión supervisión (sólo registro)
999	Fallo tipo zona 23 (sólo registro)
382	Supervisión zona cableada auxiliar (enviada después de que se envié código 333)

Tabla 4.5 Códigos de eventos Contact ID

Información General sobre la Programación

Puede programar el sistema en cualquier momento, incluso en las oficinas del instalador antes de la instalación real. La programación también puede hacerse remotamente desde las oficinas del instalador, usando un ordenador compatible IBM, un módem CIA/CIA-EU, y el software bidireccional Compass. A continuación listamos los distintos modos de Programación utilizados para programar este sistema:

Modo de programación	Usado para:
Programación Campos de datos	Programar campos de datos básicos utilizados para configurar las diferentes opciones del sistema. La mayoría de los campos de datos en este sistema han sido programados con valores por defecto de fábrica. Sin embargo, algunos campos deberán ser programados para cada instalación en particular para establecer sus opciones específicas de alarma e informes.
*56 Programación de Zonas	Asignar características de zona, códigos de informe, descriptores alfanuméricos, y números de serie para los transmisores RF.
*57 Programación Teclas de Función	Programar cada una de las 4 teclas de función para realizar una operación del sistema.
*58 Programación de Zonas	Asignar atributos de zonas, similar al modo *56, pero facilita un procedimiento de programación mas rápido y para ser utilizado por instaladores familiarizados con la programación de estas unidades de control.
*79 Programación dispositivos de salida (Mapa o y trazado)	Asignar direcciones de equipo usadas por los módulos 4229/4204 o consola 6164 y trazar relés específicos y salidas de equipos, y asignar códigos de unidad para los dispositivos de portadora de línea.
*80 Definición de salidas	Definir hasta 48 definiciones de salidas que pueden controlar los relés de salida utilizando el modo *79.
*81 Programación Lista de Zonas	Crear listas de zona para zonas de relés/dispositivos de portadora de línea, zonas de aviso, noche-parcial, zonas de ruta de salida, zona de puerta de salida final, y zonas del localizador.
*82 Programación Alfanumérica	Crear descriptores alfanuméricos para una fácil identificación de zona.
Modo calendarios (código+[#]+64)	Crear calendarios para automatizar diversas funciones del sistema o para determinar el acceso de usuarios.

Tabla 4.6 Modos de programación para el sistema

Zonas y Particiones

Cada zona de protección necesita ser programada con diversos atributos usando el modo de Programación de Zonas *56 o el modo de Programación Avanzado *58.

El sistema puede controlar tres áreas independientes de protección (conocidas como particiones) para ser utilizadas por usuarios independientes, simplemente asignando zonas a una de las particiones durante la programación de zonas. El sistema, por defecto, automáticamente distribuye a los usuarios entre las tres particiones. El usuario maestro puede cambiar la distribución de los números de usuario.

Las zonas también pueden ser asignadas a una partición de área común si la partición 3 ha sido designada como tal, esta es un área compartida por los usuarios de las otras dos particiones (como el vestíbulo de un edificio). Esto permite que cualquiera de las particiones independientes se conecte, mientras que el área común permanece desconectada para poder acceder a la otra partición.

A continuación se describe el funcionamiento del área común, si se utiliza:

- El área común activa y transmite informes de alarma solo cuando las otras dos particiones están conectadas. Si solo está conectada una partición, el sistema ignora los fallos en el área común.
- Cualquiera de las dos particiones puede conectar su sistema aunque el área común esté en fallo, pero una vez armada, la otra partición no podrá conectarse hasta que se anulen o corrijan los fallos de las zonas del área común.

- Los fallos en el área común se muestran en las pantallas de las consolas del área común, y también se mostrarán en la consola de otra partición cuando la si esa partición está conectada.

- Cualquiera de las particiones puede borrar y restaurar el área común después de una alarma.

Definiciones de Tipos de Zona

Deberá asignar un tipo de zona a cada zona, el cual define como responde el sistema a los fallos de esa zona. Los tipos de zona se definen a continuación:

Tipo de zona	Descripción
Tipo 00 No usada	Programar una zona con este tipo de zona si la misma no va a ser utilizada.
Tipo 01 Entrada/Salida 01	• Asignar a zonas usadas para entrada y salida principal. • Proporciona un tiempo de entrada cuando se activa este tipo de zona si el panel de control está conectado en los modos Total, Parcial, o Parcial-Noche. • No proporciona tiempo de entrada si el panel está conectado en modo Instant/Máximo. • El tiempo de entrada 1 se puede programar para cada partición. • El tiempo de salida empieza cuando se conecta el panel de control, sin importar el modo de conexión seleccionado, y es programable para cada partición. (Si la opción de Conexión Contacto Final está habilitada en el campo *88, el tiempo de salida continua indefinidamente hasta que la última zona de la lista de zonas 8 se restablezca; una vez restablecida la última zona, el tiempo de salida será entonces 5 segundos.).
Tipo 02 Entrada/Salida 02	• Asignar a zonas utilizadas para entrada y salida y que necesiten más tiempo del asignado a los puntos de entrada/salida primarios. • Proporciona un tiempo de entrada secundario, igual que el tiempo de entrada 1. • Se puede programar el tiempo de entrada 2 para cada partición. • El tiempo de salida es el mismo que el descrito para el Tipo 01.
Tipo 03 Perímetro	• Asignar a todos los detectores o contactos en ventanas y puertas exteriores poco usadas. • Proporciona una alarma instantánea si se activa la zona cuando el panel está conectado en los modos Total, Parcial, Noche-Parcial, Instantáneo o Máximo.
Tipo 04 Ruta de entrada interior	• Asignar a zonas cubriendo un área como un vestíbulo o pasillo por el que uno tiene que pasar al entrar (para llegar hasta la consola). • Proporciona una alarma retardada (usando el tiempo de entrada 1 programado) si primero se activa la zona entrada/salida. En caso contrario este tipo zona proporciona una alarma instantánea. • Activa cuando el panel está conectado en modo Total. • Anulada automáticamente cuando se conecta el panel en modo Parcial o Instant; En modo Noche-Parcial, las zonas asignadas a lista de zonas 05 (lista zonas noche parcial) no se anulan cuando se conecta el sistema en modo Noche-Parcial.

Tipo 05 Aviso día/Alarma noche	• Asignar a una zona que proteja un área sensible como un almacén, cuarto de fármacos, puerta de salida de emergencia, etc. • También puede utilizarse con un detector o contacto en una zona donde se desee tener una notificación inmediata de entrada. • Asignar para usar con detectores, equipos o sirenas con protección antisabotaje. • Proporciona una alarma instantánea si se activa cuando el sistema está conectado en modo Total, Parcial, Noche-Parcial, Instantáneo o Máximo. • Durante el estado de desconexión, el sistema facilitará un sonido potente de avería desde la consola (y un informe a la Central Receptora, si se desea).
Tipo 06 24 horas silencioso	• Se asigna normalmente a zonas con pulsadores de emergencia. • Envía un informe a la Central Receptora pero no proporciona ningún mensaje en pantalla ni sonido de consola.
Tipo 07 24 horas audible	• Asignar a zonas con pulsadores de emergencia. • Envía un informe a la Central Receptora, proporciona un sonido de alarma en la consola, y una alarma audible en la sirena auxiliar.
Tipo 08 24 horas auxiliar	• Asignar a zonas con pulsadores de emergencia, o a zonas con dispositivos de supervisión como detectores de agua o temperatura. • Envía un informe a la Central Receptora y proporciona un sonido de alarma en la consola. (No se facilita salida a sirena auxiliar.)
Tipo 09 Fuego supervisado	• Proporciona una alarma de fuego con corto circuitos y una condición de avería con circuito abierto. Una alarma de fuego proporciona un sonido pulsado en la sirena. • Este tipo de zona siempre está activo y no puede anularse.
Tipo 10 Interior c/retardo	• Proporciona un tiempo de entrada (usando el tiempo de entrada programado), si se activa cuando el panel está conectado en modo Total. • El Tiempo de Entrada 1 se inicia cuando se activan los detectores de esta zona, independientemente de que se active una zona de tiempo entrada/salida antes. • Anulada cuando el panel está conectado en modo Parcial o Instant; en modo Noche-Parcial, las zonas asignadas a la lista de zonas 05 (lista zonas noche-parcial) no se anulan cuando el sistema está conectado en modo Noche-Parcial.
Tipo 12 Zona Supervisión	• Funciona como una supervisión dinámica de un fallo/avería de zona (no alarma). En caso de corto/apertura, el mensaje, "*ALARMA*-24 Hr. No-Robo -#XXX " (donde XXX es el número de zona) será enviado a la Central Receptora. La consola del sistema mostrará el mensaje “COMPROBAR” indicando la zona apropiada (pero la consola no emitirá ningún pitido). Cuando se restablezca la zona, se enviará el mensaje, "*RESTABL.*-24 Hr. No-Robo. -#XXX " a la Central Receptora. • El mensaje “COMPROBAR” desaparecerá automáticamente de la consola, cuando se restablezca la zona; no es necesaria una secuencia código usuario + paro para restablecer la zona. • Los fallos de este tipo de zona son independientes del sistema, y pueden existir a la hora de la conexión sin interferir. • Ya que esto es un tipo de zona de “avería”, no utilice este tipo de zona con relés programados para activarse con “alarmas.”
Tipo 14 24 horas supervisión Gas	• Asignada a cualquier zona con detectores de gas. • La salida de sirena estará pulsada cuando este tipo de zona esté en alarma. • Siempre activa y no se puede anular.
Tipo 16 Fuego c/verificación	• Proporciona una alarma de fuego cuando la zona tiene un corto, pero sólo después que la alarma haya sido verificada. • El sistema verifica la alarma rearmando las zonas durante 12 segundos después de detectar un corto. Un corto circuito dentro de los 90 segundos siguientes activará la alarma de fuego. • Proporciona una respuesta de avería cuando la zona está abierta.
Tipo 20 Conexión-Parcial (solo equipos RF BR)	• Conecta el sistema en modo Parcial cuando se activa la zona. • Las unidades tipo botón envían un número de usuario a la central receptora al conectar/desconectar. • El pulsador debe tener asignado un número de usuario.
Tipo 21 Conexión Total (solo equipos RF BR)	• Conecta el sistema en modo Total cuando se activa la zona. • Las unidades de pulsadores envían el número de usuario a la central receptora al conectar/desconectar. • Debe asignar un número de usuario para el pulsador.
Tipo 22 Desconexión (solo equipos RF BR)	• Desconecta el sistema cuando se activa la zona. • Debe asignar un número de usuario para el pulsador.
Tipo 23 * Respuesta de No Alarma	• Puede utilizarse en una zona cuando desea utilizar una acción de relé, pero sin que le acompañe una alarma (Ej., acceso a la puerta del vestíbulo). • Los fallos/restablecimientos de zona se guardan en el registro de eventos. * El sistema se puede conectar aunque estos tipos de zona están en condición de fallo.
Tipo 24 Robo Silencioso	• Normalmente se asigna a todos los detectores o contactos en ventanas y puertas exteriores poco usadas donde NO se quiere que se active la sirena para las alarmas. • Proporciona una alarma instantánea, SIN indicación audible en ninguna consola o sirena auxiliar, si se activa la zona cuando el sistema está conectado en modo Total, Parcial, Instant, o Máximo. • Se envía un informe a la Central Receptora.

Tipo 77 Módulo Conexión/Desconexión mediante Llave	• Asignado a una zona conectada a un módulo de conexión/desconexión mediante llave. • No utilizar dispositivos asignados como tipo sensor “BR” con este tipo de zona.
Tipo 81 Zona Supervisión AVV	• Asignado a una zona conectada a un módulo AAV. • Supervisa las sesiones de audio (voz) bidireccional como sigue: - Cuando se activa la zona, todos los sonidos de alarma y transmisión de informes se detiene, excepto las alarmas de incendio, las cuales terminan inmediatamente la sesión de audio y generan el envío de un informe de fuego. - Cuando se restablece la zona (sesión terminada), se resumen los sonidos (si el tiempo de sirena no ha expirado) y los informes detenidos se transmiten.
Tipo 82 Bockschloss	• Utilizado con cerraduras y llaves blockschloss especiales. • El sistema se conecta 5 segundos después de que la llave esté completamente girada (se conecta en modo MAXIMO); la llave puede entonces extraerse. • Cuando está conectado, la zona blockschloss está en corto. Un circuito abierto de esta zona provoca una condición de avería. • Si las zonas están “no listas,” la llave no girará completamente y el sistema no se conectará. • El código de informe Contact ID es 409. • Una vez conectado el sistema utilizando la cerradura blockschloss, solo podrá desconectarse con la llave; las consolas cableadas, consolas RF, y llaves vía radio no podrán utilizarse para desconectar. • Si se asigna el tipo de zona blockschloss a cualquier zona del sistema, el sistema no se conectará en modo TOTAL. El sistema podrá, sin embargo, ser conectado en modo PARCIAL o INSTANT desde los teclados y llaves vía radio incluso aunque la zona blockschloss esté en fallo.
Tipo 90-93 Configurable	• Permite varias respuestas personalizadas. • Las opciones incluyen respuesta a tiempos de entrada/salida, respuesta a aperturas/cortos, tipos de sonido de alarmas/averías, retardo comunicación, y códigos de informe Contact ID únicos. • Utilice el Modo Menú *83 para programar estos tipos de zona configurables.

Tabla 4.7 Tipos de Zonas

Códigos de Seguridad

El sistema soporta hasta 48 códigos de seguridad, a los que se les puede asignar uno de 5 niveles de autorización. El nivel de autorización determina las funciones que puede realizar cada código.

Niveles de Autorización (los niveles de autorización pueden asignarse sólo a los usuarios 3 al 49; los usuarios 1 y 2 no pueden modificarse)

Nivel	Nº Usuario	Funciones
Instalador	01	realizar todas las funciones de seguridad excepto que sólo puede desconectar si se utilizo para conectar el sistema; puede acceder al modo de programación; puede modificar el Código Maestro del Sistema; no puede asignar ningún otro código de usuario (por defecto= 4112)
Maestro Sistema	02	sólo un código maestro por sistema; puede realizar todas las funciones de seguridad, añadir/borrar usuarios en todas las particiones, modificar el código maestro del sistema, ver registro de eventos, ajustar reloj, programar teclas macro, programar eventos por calendarios, activar equipos de salida (triggers/relés) (por defecto= 1234)
Maestro Partición (por defecto)	P1 = 03 P2 = 25 P3 = 41	Igual que el Maestro, excepto que sólo puede añadir/borrar usuarios de la partición asignada, (puede asignar diferentes niveles de autorización a estos usuarios, si se desea; se puede asignar el nivel de autorización de maestro partición a cualquier usuario)
0-Usuario	03-49	sólo realizar funciones de seguridad (conectar, desconectar, etc.); no puede añadir/borrar usuarios, ver registro, ajustar reloj ni programar eventos por calendarios
1-Sólo Arm.	ver "usuario"	sólo conectar el sistema
2-Invitado	ver "usuario"	sólo puede desconectar el sistema si se utilizo para conectarlo
3-Coacción	ver "usuario"	realiza funciones de seguridad, y también envía un mensaje silencioso de coacción a la CRA; reporta con número usuario de código coacción.
4-Maestro Partición	ver "usuario"	Ver párrafo anterior de Maestro Partición; utilizado para asignar a otros números de usuarios nivel de maestros partición

Tabla 4.8 Códigos de seguridad

A continuación se incluye una breve descripción de cómo añadir códigos de usuarios:

Añadir un Código Usuario: Código Maestro + [8] + nº usuario de 2 dígitos + código de usuario.

Borrar un Código Usuario: Código Maestro + [8] + nº usuario de 2 dígitos + [#] [0].

Asignar Atributos: Código Maestro + [8] + nº usuario de 2 dígitos + [#] [nº atributo] + valor.

Atributos	Valores
1 = nivel de autorización	0-4 (ver tabla 4.6)
2 = grupo de acceso	0-8 (0 = no asignado a un grupo)
3 = partición(es) activa(s) para este usuario	1, 2, 3 Introduzca las particiones consecutivamente si es mas de una pulse [#] para terminar
4 = número zona RF	Asigna número de usuario a zona de tipo botón para conexión/desconexión (llave RF debe haber sido registrada en el sistema)
5 = busca apertura/cierre	1 para Si, 0 para No
6 = informe apertura/cierre a central receptora	1 para Si (por defecto=si para todos los usuarios), 0 para No

Tabla 4.9 Asignación de atributos

4.2.1.2. TECLADO DE MANDO.

FIG. 4.10 Teclado de mando del panel de control

El teclado de mando es el dispositivo en el cual se activa y desactiva los distintos dispositivos (contactos magnéticos y de movimiento) agrupados en las zonas de protección, es por esta razón que su ubicación es a lado de la puerta principal de la vivienda.

En el display se puede mostrar los eventos que suceden en tiempo real, como una ventana abierta, puerta, alarma de incendio o de movimiento.

El teclado de mando debe ser cableado hasta el panel de control de alarma (PA).

La consola o teclado de mando con pantalla de cristal de líquido (**LCD**) modelo 6148SP de Ademco, es fácil de instalar y utilizar. Los mensajes prefijados en español facilitan el control del sistema. El atractivo diseño blanco de la consola se adapta perfectamente a

cualquier entorno, y además incorpora una tapa contorneada extraíble que oculta las teclas retroiluminadas. Esta consola se caracteriza por una pantalla de LCD que utiliza números de zona de 2 dígitos más un tercer dígito parcial.

MARCA: ADEMCO

MODELO: 6148SP

Características

- Consola de fácil manejo
- Teclas de plástico retroiluminadas
- Zumbador con pitidos audibles para notificar: tiempos de entrada/salida y situaciones de alarma
- Estado del sistema indicado mediante textos prefijados en español
- Teclas de funciones del sistema claramente identificadas
- Tapa blanca extraíble para cubrir teclas

Funciones

A continuación se listan los comandos del sistema:

Función	Descripción
Silenciar Alarmas	Pulsar cualquier tecla para silenciar el zumbador de la consola durante 10 segundos. Desconectar el sistema para silenciar tanto zumbador como sirenas auxiliares.
Conexión Rápida	Si está habilitado (campo *21), podrá pulsar la tecla [#] en vez de su código de seguridad, junto con la tecla de conexión deseada (Total, Parcial, Instant, Máximo)
Conexión un Solo Botón	Si está programado (Modo Menú *57 Teclas de Función), las teclas con letras A-D podrán utilizarse para conectar, usando las opciones 3-TOTAL, 4-PARCIAL, 5-NOCHE-PARCIAL, o 6-Conexión Escalonada. Con esta opción no será necesario el código de seguridad para conectar el sistema.
Memoria de Alarma	Cuando el sistema está desconectado, se mostrará en pantalla cualquier zona que estuviera en condición de alarma durante el periodo de conexión. Para borrar este mensaje, repita la secuencia de desconexión (código de seguridad + tecla PARO).
Conexión Total	Introduzca código + TOTAL [2] o simplemente pulse la tecla con letra apropiada en la consola (ver "Conexión un Solo Botón" descrita anteriormente). Si la opción de "Auto-Conexión Parcial" está habilitada y la puerta de entrada/salida **no se** abre y cierra dentro del periodo de tiempo de salida programado, el sistema se conectará automáticamente en modo PARCIAL si se realiza la conexión desde un teclado cableado (no un dispositivo RF). Si la puerta **se** abre y cierra dentro del tiempo de salida, el sistema se conectará en modo TOTAL.
Conexión Parcial	Introduzca código + PARCIAL [3] o simplemente pulse la tecla con letra apropiada en la consola (ver "Conexión un Solo Botón" descrita anteriormente). Ver "Conexión Total" descrita en el paso anterior para la opción de Conexión Auto-Parcial
Conexión Noche-Parcial	Introduzca código + PARCIAL [3] + PARCIAL [3] o simplemente pulse la tecla adecuada en la consola (ver "Conexión un Solo Botón" descrita anteriormente).
Conexión Instant	Introduzca código + INSTANT [7].
Conexión Máxima	Introduzca código + MAXIMO [4] o simplemente pulse la tecla con letra apropiada de la consola (ver "Conexión un Solo Botón" descrita anteriormente).
Desconexión	Introduzca código + PARO [1]. Si el tiempo de entrada o una alarma están activos, no necesitará pulsar la tecla PARO; bastará con introducir el código de seguridad para desconectar el sistema.
Anular Zonas	Introduzca código + ANULAR [6] + números de zona (s). Se puede anular mientras el sistema está conectado/desconectado.
Anulación Forzada (Rápida)	Para anular automáticamente todas las zonas en fallo, utilice el método de "Anulación Rápida". Introduzca el código + ANULAR + [#], luego espere a que todas las zonas abiertas se muestren en pantalla. Conecte cuando la pantalla muestre el mensaje "ZONA ANULADA" y "LISTO PARA ARMAR".
Modo Aviso	Introduzca código + AVISO [9]. Para desactivarlo, introduzca código + AVISO otra vez.
Activar Equipos de Salida	Si está utilizando salidas de relé (4204, 4229, o 6164), o Dispositivos de Portadora de Línea, se incluyen dos cadenas de teclas para el usuario. Si están programadas, estas cadenas pueden utilizarse para activar o desactivar manualmente el(los) equipo(s) para iniciar o detener alguna acción, como el encendido u apagado de luces, etc. Estas cadenas de teclas son: [Código seguridad] + # + 7 + [nº Equipo de 2 dígitos] activa (inicia) el equipo. [Código seguridad] + # + 8 + [nº Equipo de 2 dígitos] desactiva (para) el equipo.

Tabla 4.10 Comandos del teclado

4.2.1.3. DETECTOR DE MOVIMIENTO.

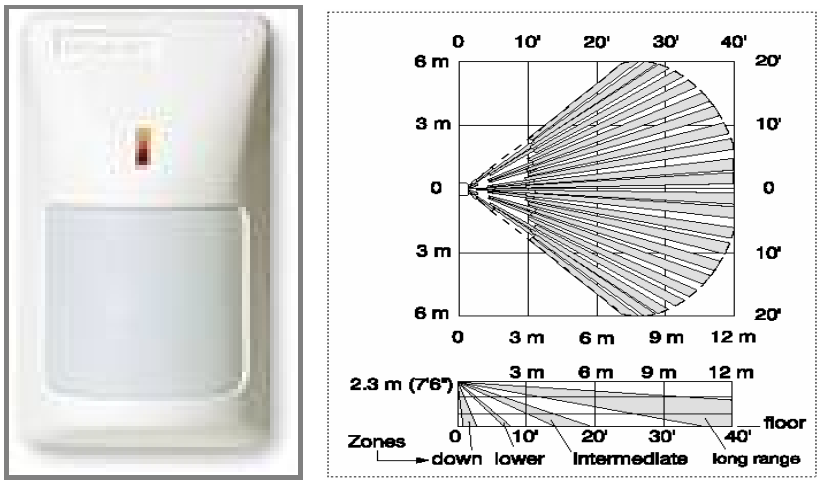


FIG. 4.11 Detector de movimiento y el rango de detección

Este dispositivo censa el movimiento y se basa en la tecnología infrarroja. Debe ser instalado en las áreas que se desee supervisar el ingreso de personas, en las viviendas han sido ubicados en las puertas: principal y posterior.

El rango de cobertura de este dispositivo es de 144m^2 y su grado de sensibilidad es ajustable.

MARCA: IntelliSense (Grupo Ademco)

MODELO: IS-215T

<u>Características</u>

- *Diseño atractivo y elegante de color blanco, pudiendo ser aplicado a cualquier* ambiente.

- *Cableado superficia*l: haciendo rápida su instalación.

- *Zonas abajo del sensor*: cubre la zona debajo del sensor mediante un espejo patentado permitiendo la cobertura de la parte inferior del sensor.

- *Flexibilidad al montaje*: es de fácil ubicación en paredes o esquinas sin perder su rango de cobertura y manteniendo la estética del ambiente.

- *Diseño de lente resistente a sabotaje*: los lentes están fijados dentro de un retenedor, haciéndolos más estables y difíciles de sabotear.

- *Sensibilidad ajustable*: puede ser ajustada acorde a los requerimientos de instalación y del ambiente.

- *Tamper*: este tamper sellado conmuta señales antes de que cualquier manipulación del mismo sea posible.

- *Anti insecto*: previene el acceso de insectos dentro del sensor óptico, reduciendo así las falsas alarmas.

- *Aplicaciones*: diseñado para aplicaciones residenciales y semicomerciales.

4.2.1.4. DETECTOR DE HUMO.

FIG. 4.12 Detector de humo

El detector de humo es de tipo fotoelectrónico o una combinación fotoelectrónica/térmica con sensor térmico a 135^{o}F fabricado por System Sensor.

Las conexiones del cableado son hechas con tornillos SEMS. El detector tiene un led visible el cual parpadeará en espera y se mantendrá encendido en caso de alarma.

El detector tiene una sensibilidad nominal de 3%/pie como medida en las cajas de humo de la UL. Este dispositivo es de fácil limpieza y permite hacer pruebas sin la necesidad de tener humo en el ambiente.

Tiene un chequeo automático de cada 40 seg. para verificar su integridad funcional. Si falla el led del dispositivo dejará de parpadear. Posee un brazo para montaje, el cual es compatible con las cajas metálicas eléctricas estándares.

Los detectores de humo se instalaran en cada una de los dormitorios, sala y comedor.

Estos dispositivos son alámbricos y están conectados al Panel de control de alarmas PA en los terminales designados para este servicio.

MARCA: System Sensor

MODELO: 2400 de la serie 400

Características

- Funciona a 12 o 24 V
- Gabinete para sensor óptico único
- Cubierta y pantalla contra insectos removible para fácil limpieza
- Su cubierta es sellada contra suciedad, insectos y jalones
- Medición del campo de sensibilidad del detector cumple con las normas NFPA 72
- Garantía de 3 años

4.2.1.5. DETECTOR TÉRMICO.

FIG. 4.13 Detector térmico

Este dispositivo térmico será instalado en la cocina de las viviendas para protección de incendios, por lo que no es fotoeléctrico debido a los vapores que se emanan en esta área. Igual que los dispositivos fotoeléctricos serán conectados al PA.

MARCA: Honeywell

MODELO: ECO1005

Características

- Modelo foto térmico
- Unidad remota de prueba basada en láser
- Certificación EN 54 (edición 2000)
- Fotoeléctrico, foto térmico y detector térmico
- Compatible con sistemas de incendios y seguridad

- Rango de temperatura de operación: -20^{o} a 60^{o} C

4.2.1.6. CONTACTOS MAGNÉTICOS.

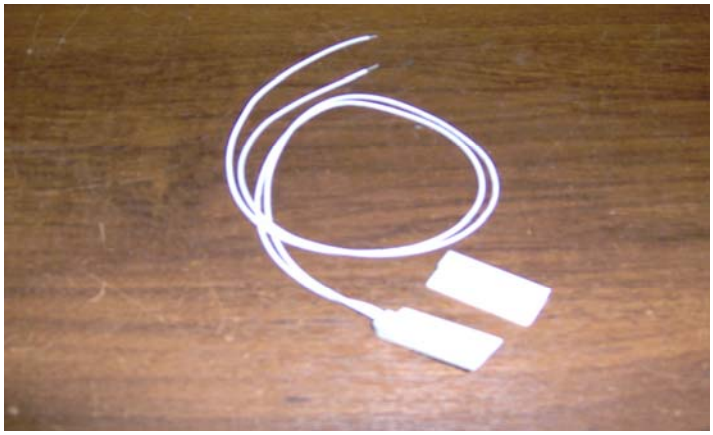


FIG. 4.14 Contactos magnéticos

Se ha considerado la instalación de los contactos magnéticos en cada una de las ventanas de las viviendas y las puertas principal y posterior.

La operación de estos dispositivos consiste en mantener su campo magnético sin alterarse, al haber una modificación de este, emite una señal al PA activando la alarma.

De esta manera protegemos cada uno de los ingresos a la vivienda.

Características

- Mini superficie montable con cables de conexión

- Espacio estándar entre los sensores: 1 ¼”

- Tamaño pequeño para fácil limpieza
- Longitud del cable conductor: 18”
- Montaje atornillado o con adhesivo

4.2.1.7. EL MODULO DE PROTOCOLO INTERNET (MIP).

FIG. 4.15 Vista del Módulo de Protocolo Internet MIP. Marca Telsec

El Módulo de Protocolo de Internet (**MIP**), es un módulo ajustable para paneles de alarmas diseñado para enviar cualquier tipo de alarma o señal generada por el panel de control de alarmas a través de redes de datos como Internet.

Este módulo es compatible con cualquier panel de alarmas que haga uso del protocolo Contact-ID, el MIP permite transmisiones de alarmas con una mayor velocidad de transmisión y con mayor seguridad a las Centrales Receptoras de Alarmas.

Principales ventajas del MIP.

Compatibilidad con el parque de paneles de alarmas ya instalados.

El MIP es "independiente del fabricante y marcar del panel de alarmas", lo que significa que podrá operar con cualquier panel de control que esté configurado para usar el protocolo Contact-ID. Con este dispositivo se puede utilizar cualquier panel de alarmas del mercado, ya instalado.

Ahorra tiempo de instalación.

Añadiendo el MIP al panel de alarmas, se reduce el tiempo de instalación. No es necesario reemplazar el panel ni rehacer la instalación de todos los detectores. Programando y conectando el MIP, según la guía de instalación estaremos listos para usar este equipo.

No se requiere dirección IP pública.

A pesar de que los paneles digitales son productos similares al MIP, el MIP es capaz de operar sobre su propia red de datos sin modificaciones, esto significa que el MIP es capaz de ahorrarnos el costo de pagar por una dirección IP pública fija.

Transmisión de alarmas a mayor velocidad.

El MIP recibe la alarma del panel y la transmite a través de la intranet o de Internet en menos de un segundo. Además, la transmisión de la

alarma es inmediata en comparación con el tiempo requerido por los paneles de alarmas tradicionales (los cuales tienen que esperar a tener tono, llamar al destino, esperar a que se establezca la conexión, transmitir la alarma y esperar la negociación).

Ahorro de costos en llamadas telefónicas.

Las alarmas pueden ser transmitidas a través de Internet, para ello se hace uso de una línea de comunicaciones compartida con el acceso a Internet que normalmente se usa para que los usuarios naveguen por Internet, en el momento en que se implemente este servicio en la urbanización.

Funcionalidades de línea segura y detección de sabotajes.

El MIP está continuamente en comunicación con la Central Receptora de Alarmas, enviando señales periódicas que indican a la receptora de la central que el MIP está activo, en línea. En el caso de que el MIP o el panel queden fuera de uso por cualquier motivo, sabotaje por ejemplo, la receptora detectará esta situación y generará una alarma indicando la pérdida de conexión con el MIP remoto.

Configuración automática de IP (en desarrollo).

El MIP, soportará la configuración por el Protocolo de configuración dinámica de host (**DHCP** - Dynamic Host Configuration Protocol,). El protocolo DHCP cliente implementado en el MIP permitirá a éste obtener de forma automática la dirección IP, máscara de red y router

por defecto de forma que en el futuro no tendremos que preocuparnos de estos tediosos parámetros de configuración.

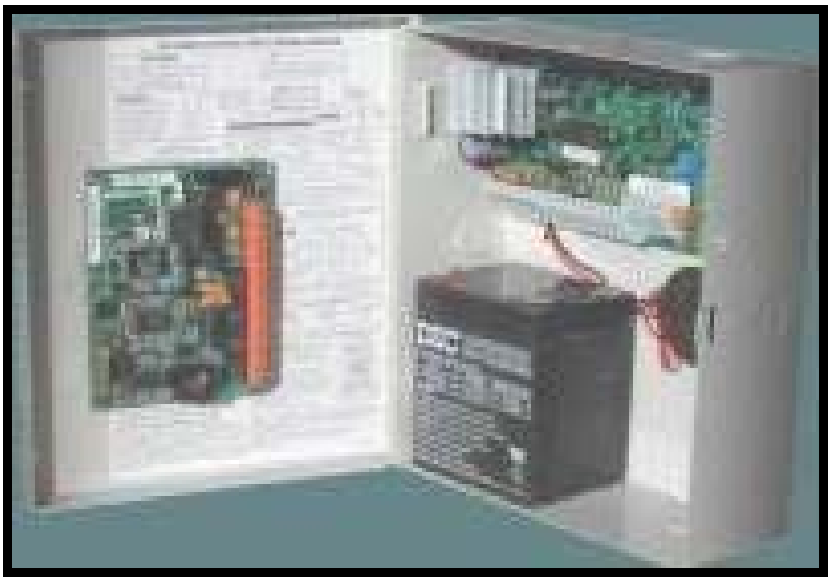


FIG. 4.16 Instalación del MIP en el Panel de Alarmas

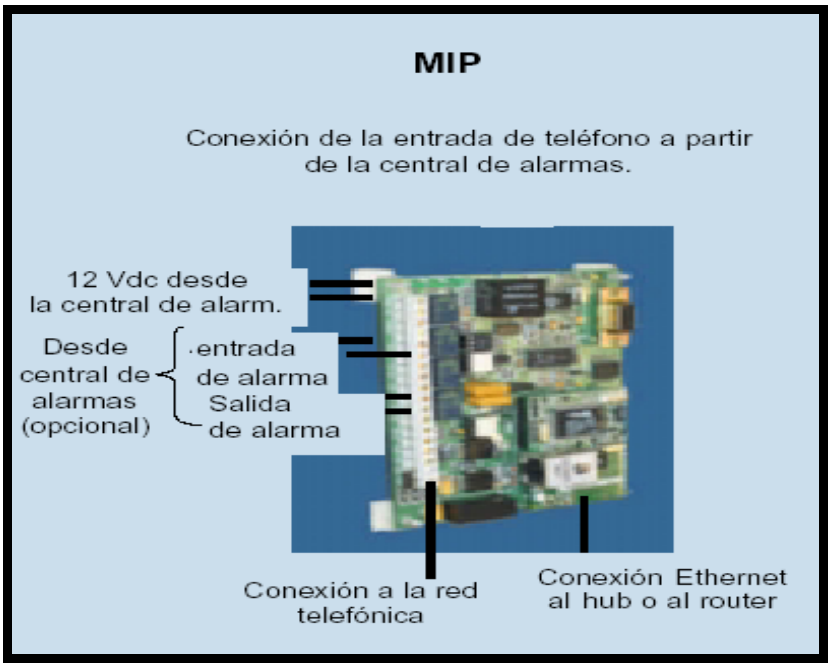


FIG. 4.17 Conexiones de la tarjeta MIP

La funcionalidad del MIP en la transmisión de las alarmas.

Cuando el MIP tiene conectividad con el equipo receptor de alarmas, el equipo VisorALARM, intercepta la línea telefónica y procesa todas las llamadas entrantes y salientes que tienen lugar desde el panel de alarmas.

El VisorALARM será instalado en la consola de control. A continuación detallamos los intercambios de información entre el MIP y el VisorALARM.

El protocolo de envío de alarmas soportadas es el Contact-ID. Este formato envía las alarmas mediante dígitos, según el formato:

AAAA MM Q EEE GG CCC S

Donde:

AAAA es el número de cliente

MM es el tipo de mensaje

Q es un cualificador del evento

EEE es el tipo de alarma

GG es el grupo de partición

CCC es el número de zona, y finalmente

S es un número de validación de la trama.

Cuando el panel descuelga para enviar una alarma el MIP le da alimentación y emite el tono de invitación a marcar. Cuando el panel

de alarmas marca el número de teléfono de la central de alarma se emite el handshake del Contact-ID y recibe la trama con la alarma. A partir de este momento el MIP se encarga de enviar esa alarma al VisorALARM.

Al panel de alarmas no se le da el asentimiento de trama enviada (Kissoff) hasta que dicha confirmación sea reciba desde el equipo receptor de alarmas VisorALARM. Si el MIP no recibe el mensaje de asentimiento en dos segundos este reintenta el envío un número configurable de veces, tras el cual a conexión con el VisorALARM se da por perdida y esto permite que el panel de alarmas haga el envío por la línea telefónica, a partir de este punto el MIP intentará restablecer la comunicación con el VisorALARM.

La receptora IP VisorALARM cuando recibe una llamada de un MIP la almacena en una memoria interna no volátil. Cuando ha terminado la operación satisfactoriamente envía al MIP que la originó el asentimiento para que a su vez se lo envíe al panel de alarmas asociado. Si la memoria de almacenamiento de las alarmas no puede almacenar la alarma no da asentimiento alguno.

Por otra parte, de cara al Software de automatización, el equipo VisorALARM se comporta como una receptora de alarmas que envía las alarmas recibidas por un puerto serial.

El equipo VisorALARM puede emular tres modelos de receptoras de alarmas, tales como son: La receptora Sur-Gard, una Radionics 6500 o una Ademco 685, para nuestro proyecto se utilizara la última. Los parámetros para las mismas son configurables, así como los relativos a la receptora emulada (link-test, identificadores de receptora y de línea, caracteres de inicio y fin de trama, etc.).

Configuración de un MIP.

El procedimiento de instalación es configurar todos los parámetros en el MIP y crear una configuración del MIP en el equipo receptor de las alarmas VisorALARM con los mismos parámetros. En este caso, basta con conectar el MIP en la red del cliente y se pondrá en funcionamiento.

Para crear una configuración de MIP teclear:

```
RECEPTORA ARLY-1 Cfg>mip número-de-cuenta Default
```

Para configurar cada uno de los parámetros se utiliza la sintaxis:

```
RECEPTORA ARLY-1 Cfg>mip número-de-cuenta opcion valor
```

Todas las opciones del patrón de configuración excepto el password de instalador se admiten en este comando. Además, este comando admite la siguiente opción:

Serial-number: configura el número de serie del MIP. Un número de serie del MIP tiene el formatos 8209/XXXXX

A continuación se muestra la configuración de una MIP con número de cuenta 9999.

```
RECEPTORA ARLY-1 Cfg> mip 9999 default
RECEPTORA ARLY-1 Cfg> mip 9999 serial-number 8209/01101
RECEPTORA ARLY-1 Cfg> mip 9999 usr-password 1234
RECEPTORA ARLY-1 Cfg> mip 9999 mip-password 1234567890
RECEPTORA ARLY-1 Cfg> mip 9999 receiver-password 0987654321
RECEPTORA ARLY-1 Cfg> mip 9999 keep-alive-timer 35
RECEPTORA ARLY-1 Cfg> mip 9999 keep-alive-retries 7
RECEPTORA ARLY-1 Cfg> mip 9999 keep-alive-retries-timer 3
RECEPTORA ARLY-1 Cfg> mip 9999 phone-length 2
RECEPTORA ARLY-1 Cfg> mip 9999 alarm-tx-retries 2
RECEPTORA ARLY-1 Cfg> mip 9999 callback-phone 77
RECEPTORA ARLY-1 Cfg>
```

Si se desea cambiar una de las opciones basta con introducir el comando que la configura con un nuevo valor. Por ejemplo:

```
RECEPTORA ARLY-1 Cfg>mip 9999 keep-alive-retries-timer 2
RECEPTORA ARLY-1 Cfg>
```

Si se desea dejar una de las opciones con su valor por defecto, se debe teclear “no” seguido del comando que se utilizo para configurarlo. Por ejemplo:

```
RECEPTORA ARLY-1 Cfg>no mip 9999 keep-alive-retries-timer 2
RECEPTORA ARLY-1 Cfg>
```

Por último, para borrar toda la configuración de un MIP, se debe teclearse el comando:

```
RECEPTORA ARLY-1 Cfg>no mip 9999 default
RECEPTORA ARLY-1 Cfg>
```

Actualización de un MIP.

Para simplificar la tarea de mantenimiento de los MIPs, el VisorALARM permite actualizar la configuración de los MIPs. El comando de actualización de un parámetro es el mismo que el usado

para configurarlo, añadiendo “UPDATE” (actualización) antes del comando. Por ejemplo:

```
RECEPTORA ARLY-1 Cfg>update mip 9999 keep-alive-retries-timer 3
RECEPTORA ARLY-1 Cfg>
```

Actualiza la configuración del tiempo entre intentos de keepalive, para este caso en el ejemplo este puede fallar al valor dado de 3. Cabe destacar que el número de serie del MIP no se puede modificar por este mecanismo.

Conexiones Físicas de un MIP.

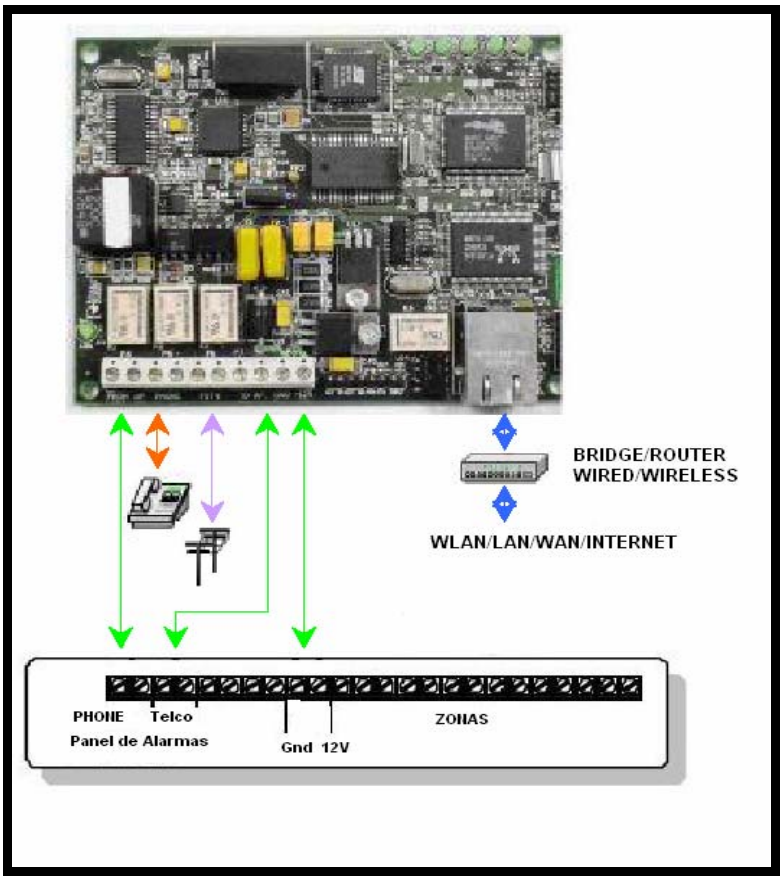


FIG. 4.18 Conexiones físicas del MIP

A continuación se hará una descripción de las conexiones del MIP, la misma que se realizará desde la izquierda hacia la derecha de la figura 4.18

Conexión número 1.-

La primera es entre el primer par de puntos de conexión del MIP y el punto de conexión llamado PHONE en el Panel de Alarmas, esto es para lograr la transmisión de las alarmas del Panel de Alarmas al MIP.

Conexión número 2.-

La segunda conexión es entre el segundo par de Puntos de conexión de MIP y el sistema de telefonía interno del lugar o vivienda.

Conexión número 3.-

La tercera conexión es entre el tercer par de puntos de conexión del MIP y la red de telefonía pública (**PSTN**) en el caso de que esta existiera.

Conexión número 4.-

La cuarta conexión es entre el cuarto par de puntos de conexión del MIP y el punto de conexión TELCO (conexión telefónica) del Panel de Alarmas o hacia un teléfono análogo, lo cual se realiza para lograr la configuración del equipo.

Conexión número 5.-

La quinta conexión es entre el quinto par de puntos de conexión del MIP y el punto de conexión llamado GND /+12V, el cual son los

terminales de una fuente de alimentación de 12 Vdc desde el Panel de Alarmas

Conexión número 6.-

La sexta conexión es entre un puerto RJ45 para la conexión entre el MIP y la red Ethernet.

Ajustes finales.

Para finalizar el proceso, se recomienda habilitar eventos de la interfaz ARLY que esta representada por los puertos seriales WAN1, WAN2 y WAN3 del VisorAlam y que serán de ayuda en el diagnóstico de posibles problemas. Para ello, ejecuta los comandos que se presentan a continuación:

```
RECEPTORA ARLY-1 Cfg>exit
RECEPTORA Config>event
-- ELS Config --
RECEPTORA ELS config>enable trace subsystem arly all
RECEPTORA ELS config>exit
RECEPTORA Config>
```

Finalmente, se debe grabar la configuración y reiniciar para que se tome efecto. Para salir del menú de configuración después de grabar pulsar simultáneamente las teclas “CTRL” y la “P”.

```
RECEPTORA Config>save
Save configuration (Yes/No) [No]? y
OK on Flash (not saved in SmartCard)
RECEPTORA Config>
RECEPTORA *restart
Are you sure to restart the system(Yes/No)? y
Restarting. Please wait
APP DATA DUMP..
Running application

Flash configuration read
Initializing
User:
```

4.2.1.8. INTERFAZ DE TELEFONÍA IP: EL BREEZEACCESS RG.

La interfaz telefónica que será instalada en cada una de las viviendas dará un servicio de voz independiente de la línea de pacifictel de tal forma que cada una de las viviendas tendrá un número y podrán comunicarse entre ellas y la consola de control sin generar costos adicionales.

FIG. 4.19 Interfaz para telefonía IP (BreezeAccess RG)

El BreezeAccess RG (nombre comercial), es una interfaz telefónica que trabaja conjuntamente con una interfaz de gestión instalada en el lado de la estación base, la misma que nos permitirá obtener en el momento de su instalación al equipo BreezeAccess VL, la capacidad de poder contar con VoIP. Esta es una interfaz que posee una entrada vía RJ45, la misma que conectándola con el equipo suscriptor nos permitirá contar con dos interfaces de telefonía estándar RJ11 con comunicación full-duplex, este equipo soporta llamada en espera,

conferencia tri-compartida además de ser un equipo que goza de total compatibilidad con el BreezeAccess VL solo basta de conectarlos y automáticamente contaremos con el servicio telefónico IP (plug and play).

La interfaz de gestión BreezeAccess RG es configurable para administrar las interfaces conectadas en los equipos suscriptores, a través de un software propietario, el mismo que nos permite la programación de las extensiones para la comunicación full-duplex.

El sistema BreezeAccess RG posee un sistema de autentificación antes de proveer los servicios de voz, posee un sistema de filtrado VLAN (separación del tráfico de información, gestión y telefonía) y firewall activo, compatibilidad con el estándar T.38 para fax G3 a velocidades de 14.4 Kbps, tiene mecanismos para otorgar QoS para las aplicaciones.

La autentificación de cada registro de llamada se lo logra mediante el protocolo H.225.0.0 o RAS, al respecto de la calidad de voz, se la logra mediante la aplicación del codec G.711, G.729ab (G.723.1).

La flexibilidad y fácil adaptación de este equipo se logra gracias a la compatibilidad del mismo a los siguientes estándares:

Ipv4, TCP, UDP, RTP, DHCP, RTCP, SNMP, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1P, IEEE 802.2, IEEE 802.3X, H323v2, G711, G729ab, (G723.1), G.165, G.167, G.168, T.38, G3, FSK y DTMF.

4.2.1.9. SWITCH NO GESTIONABLE.

FIG. 4.20 Switch no gestionable de 8 Puertos.

El switch será instalado para garantizar la conexión de los diferentes dispositivos, como el Módulo de protocolo Internet, la interfaz telefónica (Breeze Access RG), El Adaptador de alimentación vía cable UTP (PoE) equipo que es parte de sistema de transmisión inalámbrica, y en algunos casos las cámaras IP.

Cabe recalcar que este dispositivo será instalado en cada vivienda y en el centro de gestión.

El switch que a continuación se analizará, de marca D-link ha sido diseñado para mejorar las prestaciones en entornos de pequeñas empresas y oficinas periféricas, garantizando la flexibilidad de conexiones a 10/100Mbps. Gracias a sus 8 puertos, el conmutador también se puede destinar a grupos de trabajo de pequeñas dimensiones. Este es un dispositivo potente pero fácil de utilizar, permite que los usuarios conecten un puerto de cualquier tipo a un

nodo a 10Mbps o 100Mbps para multiplicar el ancho de banda, mejorar los tiempos de respuesta y realizar pesadas cargas de trabajo.

Descripción del Switch (DES-1008D).

El conmutador proporciona 8 puertos, todos ellos con soporte del estándar N-Way. Los puertos pueden negociar tanto la velocidad de conexión en entornos de red 10BASE-T y 100BASE-TX como el modo de transmisión full-dúplex o half-dúplex.

Características

- Conmutador Nivel 2
- Puertos 10/100Mbps
- Soporte full-dúplex y half-dúplex para cada puerto
- Puerto de interconexión MDI para expansiones sencillas
- Auto corrección de la inversión de polaridad rx
- Gama completa de LEDs de diagnosis
- De pequeñas dimensiones, ligero
- FCC (Federal Comunications Comisión) Clase A, Marca de la CE, VCCI Clase A, C-Tick, BSMI Clase A
- UL, CSA

4.2.1.10. EQUIPO SUSCRIPTOR.

FIG. 4.21 Equipo Suscriptor (BreezeAccess VL)

Para la transmisión de las señales de datos, voz y video, desde las viviendas hasta el centro de gestión se utilizará un bridge inalámbrico marca BreezeCom modelo BreezeAccess VL fabricado por Alvarion Company, el cual es un sistema de acceso inalámbrico que trabaja con el protocolo IP el mismo que nos proporciona seguridad en la transmisión de la información mediante el uso del protocolo de Encriptación WEP de 64/128-bits, además posee control de acceso SNMP (Protocolo de gestión de red simple) lo que nos previene el manejo desautorizado de los parámetros del equipo inalámbrico.

El BreezeAccess VL es un sistema que opera bajo el estándar IEEE 802.11a, nos provee de una ancho de banda por canal de 20MHz con una velocidad de 54 Mbps operando en las bandas 5.725 - 5.850 GHz y 5.47 - 5.725GHz, las mismas que son bandas de uso libre por lo cual no se requiere de una licencia para hacer uso de este equipo, estas

son configurables, la transmisión se realiza mediante la tecnología Multiplexación por división de frecuencia ortogonal (**OFDM** - Ortogonal Frecuency Division Multiplexing) lo que nos garantiza el enlace aunque no exista una línea de vista entre los equipos suscriptores y la estación base.

El equipo en si se compone de un equipo suscriptor que se instala en el domicilio de cada usuario y de una radio base instalada del lado del operador del centro de gestión.

El equipo suscriptor consta de:

- Una antena direccional incorporada a un radio-modem, por medio del cual se realizará la transmisión de las señales de datos, voz y video.

- Un inyector o equipo adaptador de alimentación vía Cable UTP (también llamado **PoE**, donde este es un acrónimo de las palabras en ingles Power over Ethernet), este inyector permite la conexión entre el equipo suscriptor (radio y antena direccional) y la red Ethernet; así también permite la conexión a la fuente de alimentación de 120 Voltios para energizar el sistema. La conexión del suscriptor al inyector se logra mediante la interfaz Ethernet RJ45.

A continuación veremos una serie de figuras, en la cuales distinguiremos características de estos equipos:

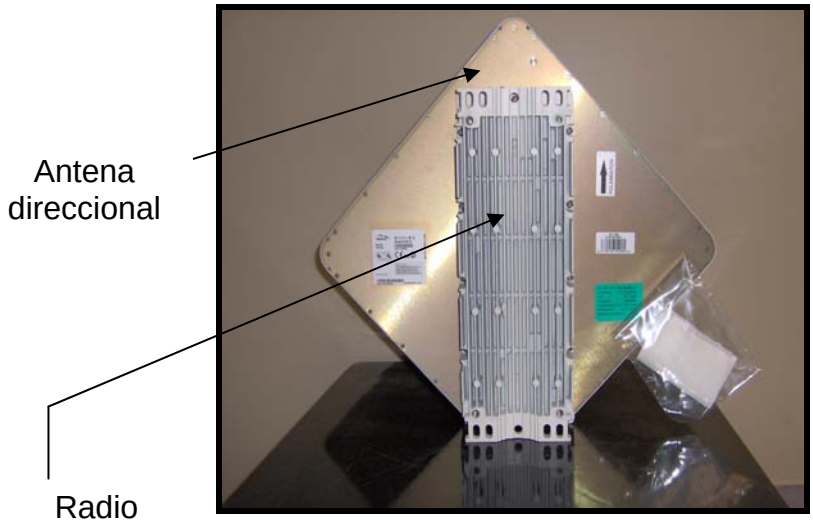


FIG. 4 22 Vista posterior del equipo suscriptor

En la figura 4.22 se puede observar la vista posterior del equipo suscriptor, aquí podemos distinguir la radio base incorporada a la antena direccional de 21 dBi 10.5^{o} horizontales y 10.5^{o} vertical, esta radio se conectará al resto de elementos de la red Ethernet vía interfaz RJ45 la misma que se podrá ver en la siguiente figura:

FIG.4.23 Vista inferior del equipo suscriptor

FIG. 4.24 Indicadores y conexión del equipo suscriptor

En las figuras 4.23 y 4.24 , podemos observar el puerto RJ45 mediante el cual de conecta el equipo a la red Ethernet, además el equipo cuenta con un display mediante el cual el equipo nos indica en nivel de captación de la señal entre el suscriptor y la estación base, permitiéndonos obtener una excelente orientación de la antena direccional, así como también podemos observar tres LEDs indicadores: el primero nos indica el encendido o apagado del equipo, el segundo nos indica la conectividad con la red Ethernet y el tercero nos indica si existe la conectividad con el equipo estación base.

FIG. 4.25 El Adaptador de alimentación vía Cable UTP (PoE).

En la figura 4.25 se puede observar el adaptador de alimentación vía cable UTP (PoE), equipo que permite la conexión tanto del equipo suscriptor y del equipo de la estación base a sus respectivas redes Ethernet, así como también es el equipo mediante el cual ellos se conectan a la fuente de 120 V.

FIG. 4.26 Conector a Ethernet del adaptador de alimentación vía cable UTP (PoE).

FIG. 4.27 Conector a radio del adaptador de alimentación vía Cable UTP (PoE).

En la figura 4.27 se puede observar el puerto RJ45 del adaptador de alimentación vía cable UTP (PoE), mediante el cual se conecta a la radio del equipo suscriptor y de la radio base a la red Ethernet

4.2.2. COMPONENTES DEL SISTEMA DE SEGURIDAD PARA EL CENTRO DE GESTIÓN.

A continuación describiremos los diferentes equipos a utilizarse en este bloque, así como sus características y ubicación en el área del centro de gestión.

4.2.2.1. ESTACIÓN BASE: EL BREEZE ACCESS VL.

Antes de la descripción del equipo, mostraremos un cuadro comparativo, el cual expondrá el motivo del por qué escogimos la marca Alvarion.

Para esto nos basaremos de los siguientes parámetros: radio de cobertura, número de suscriptores, seguridades, gestión y costos, concluyendo que el más acorde a nuestras necesidades es el Breeze Access V_L.

MARCA	RC	# SUS	SEG	GEST	$$$
DLINK	bajo	Bajo	bajo	bajo	medio
3COM	Medio	alto	medio	medio	Alto
ALVARION	alto	medio	alto	alto	Bajo

Tabla 4.11 Cuadro comparativo del equipo Estación Base

Con ésta introducción procedemos a la explicación de este equipo.

Las estaciones bases vienen en modelos modulares o independientes todas ellas con una capacidad de recibir hasta 512 suscriptores, así como también el rango máximo de cobertura de dicha celda se puede configurar entre 0 y 54 Km. Los equipos locales del cliente o suscriptor (**CPE** - customer premise equipment) vienen en varios modelos para diferentes anchos de bandas y con una o diferentes configuraciones de usuarios.

Estas unidades van a instalarse en el área donde estará situado el centro de gestión.

La función de este equipo es la de recibir la señalización de los equipos de seguridad de las viviendas y enviarla al equipo VisorALARM que es el que registrará los eventos, dichos eventos serán presentados en los servidores de alarmas.

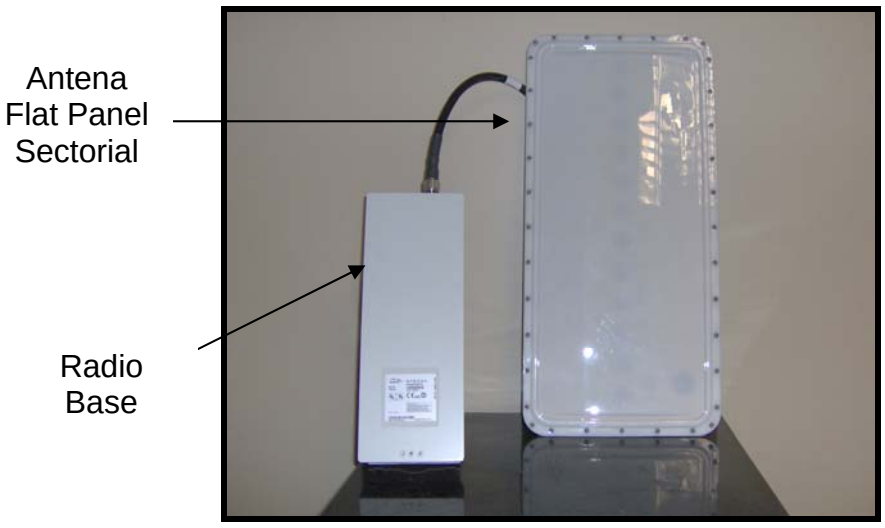


FIG. 4.28 Equipo estación base (Breeze Access VL)

En la figura 4.28, podemos observar un equipo estación base BreezeAccess VL conformado, por la radio base y una antena sectorial de 15dBi, 120^{o} horizontal x 10.5^{o} vertical ambas unidades se conectan mutuamente a través de un cable coaxial categoría RG 8, cabe recalcar de que para nuestra aplicación la antena sería reemplazada por una antena omnidireccional de 10dBi de ganancia como la que se muestra en la siguiente figura 4.31.

FIG. 4.29 Vista posterior del equipo estación base Breeze Access VL

En esta figura 4.29 podemos observar la parte posterior del equipo estación base, el cual puede ser instalado en la estación de control, este equipo se conecta mediante un adaptador de alimentación vía cable UTP (PoE), a la red Ethernet del centro de gestión.

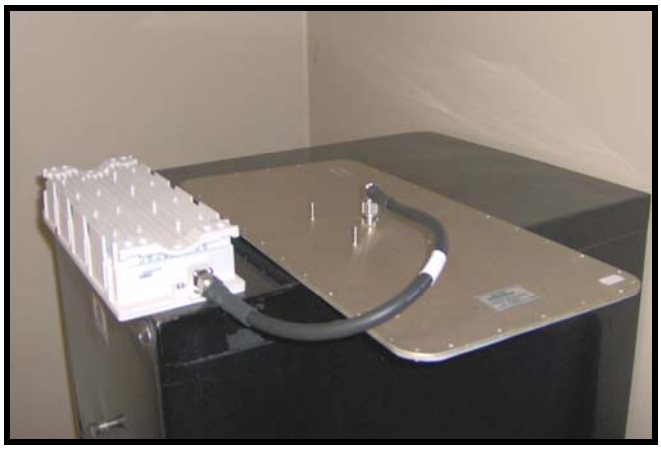


FIG. 4.30 Conexión entre la radio y la antena direccional de la estación base

Esta figura nos muestra la conexión entre la radio base y la antena la cual se logra mediante un cable coaxial categoría RG 8.

FIG. 4.31 Antena Omnidireccional, a 5GHz y 10 dB de ganancia.

La figura 4.31 nos muestra el modelo de antena, necesaria para nuestra aplicación, la cual es una antena omnidireccional modelo AN-1134 fabricada por Alvarion Company, es decir, el mismo proveedor del equipo Breeze Access VL. Esta antena cuenta con las siguientes características:

La ganancia es de 10 dBi, es apta para trabajar en frecuencias de 5 GHz, con un consumo de potencia de 50 Watts, un azimut de 360^{o} y 9^{o} verticales y con una impedancia de 50 Ohms. Además tiene un peso de 0.5 lb. y una longitud de 15.7 pulgadas.

A continuación veremos los gráficos que reflejan los patrones de radiación de la misma, para lo cual tenemos el patrón del azimut y el de elevación:

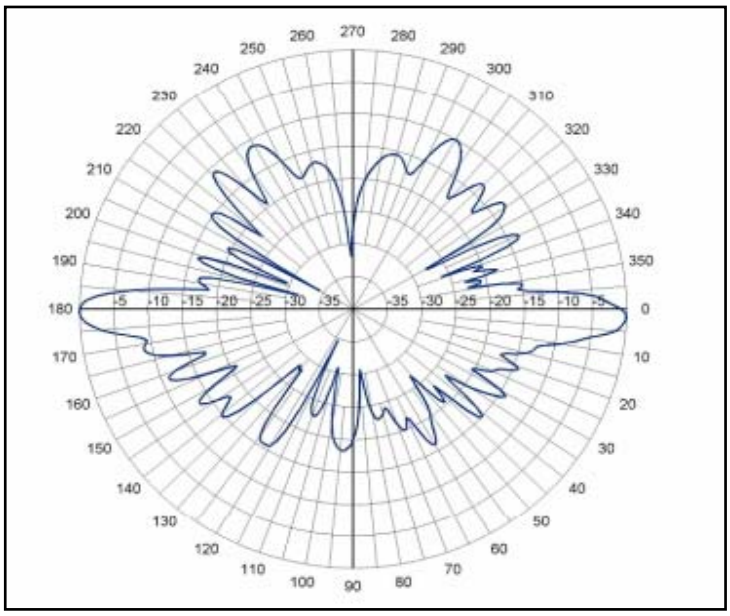


FIG. 4.32 Patrón de elevación

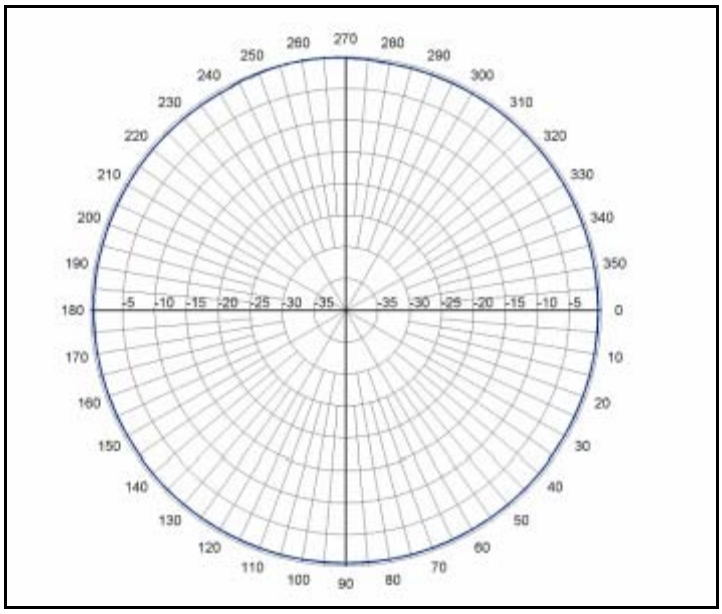


FIG. 4.33 Patrón de Azimut

Configuración y gestión de la estación base como de los equipos.

Gestión	A través de Programa Monitor sustentado mediante el protocolo SNMP (Protocolo de gestión simple de red)
Acceso de gestión remota	Desde red alámbrica, o enlaces inalámbricos
Protección de acceso de gestión	Mediante password de multinivel
Configuración de parámetros IP	Configurable manualmente o por DHCP

TABLA 4.12 Modo de Control y gestión

Cabe recalcar que el equipo inalámbrico del centro de gestión cuenta también con un inyector o adaptador de alimentación vía cable UTP (PoE) y a partir de este dispositivo se realizará la conexión hacia la red

LAN a través del switch no gestionable mencionado en el ítem relacionado a la descripción de los equipos instalados en el interior de las viviendas.

4.2.2.2. EQUIPO RECEPTOR DE ALARMAS: VISORALARM.

Para el caso de este equipo sólo tuvimos dos opciones, en donde, por costo y por ciertas especificaciones técnicas se escogió la marca Telsec.

La segunda opción era la marca LPL Development con un costo de $ 3.800 +IVA, además de que sus características también van enfocadas a redes GSM/SMS/GPRS, la cual no es nuestro caso.

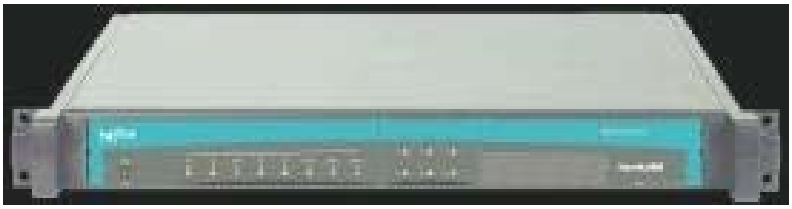


FIG. 4.34 La receptora VisorALARM marca Telsec

El equipo receptor de alarmas o también conocido como Visor ALARM, es la receptora de alarmas IP para Centrales de Alarmas. Cada VisorALARM nos permitirá gestionar hasta 3.000 MIP (Módulos de Protocolos Internet), remotos. Las receptoras VisorALARM son capaces de apilarse para soportar un mayor número de equipos remotos. Diseñada con la idea de minimizar los tiempos de puesta en marcha del sistema, la receptora puede ser programada para emular

los principales protocolos de las receptoras del mercado de la seguridad lo que repercute en la facilidad de integración de este dispositivo con su software de gestión de alarmas actual.

La receptora VisorALARM es una receptora IP diseñada para recibir alarmas desde cualquiera de los módulos MIP instalados dentro de los paneles de alarmas convencionales. Desde el punto de vista de una Central Receptora de Alarmas, el VisorALARM funciona exactamente igual que cualquiera de las receptoras convencionales actualmente existentes en cualquier Centro de Recepción de Alarmas o CRA, de hecho la receptora VisorALARM es capaz de emular la mayoría de los protocolos actuales utilizados por las receptoras lo que permite una inmediata instalación e integración de la misma dentro de la CRA.

Conexiones FISICAS de la receptora de Alarmas: VisorALARM.

FIG. 4.35 Conexiones físicas en el VisorALARM

1. *Conexión a una red de área local.*

Para la conexión a la red IP, el equipo dispone de una interfaz LAN Ethernet 10/100base T. Dicha interfaz LAN presenta un conector RJ45 para la conexión a redes Ethernet 10baseT/100baseT mediante

cables de par trenzado apantallados (SPT) o sin apantallar (UTP). Por lo que la conexión será entre el conector etiquetado como LAN y el switch o hub de la red.

2. *Conexión al servidor de alarmas.*

La conexión de datos con el servidor de automatización de alarmas se realiza mediante una de las tres interfaces serie disponibles en el equipo. Dichas interfaces serie están etiquetados como WAN1, WAN2 y WAN3 y disponen de conectores DB25 hembra. Para esto se usará un cable serie DB25 macho a DB9 hembra, para la conexión entre el conector WAN1 y el otro terminal en la PC con el software de automatización

Es importante resaltar que sólo uno de los tres interfaces serie puede ser utilizado para su conexión al servidor de alarmas. Los otros dos están reservados para su uso futuro.

3. *Conexión para la configuración.*

La receptora IP VisorALARM presenta un conector tipo DB-9 hembra en el panel posterior del equipo referenciado como AUX, que proporciona acceso a la consola local del equipo para tareas de configuración y monitorización del mismo. Para su uso es necesario conectar el puerto AUX a un terminal asíncrono (o a un PC con emulación de terminal).

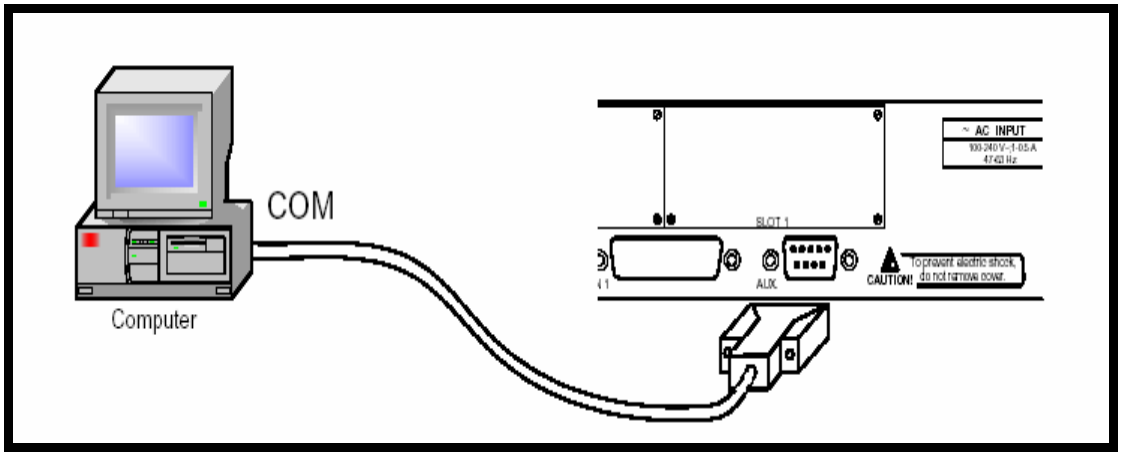


FIG. 4.36 Conexión para configuración/monitorización por consola

La configuración del terminal debe ser:

Velocidad: 9600 bps

Ocho bits de datos

Ningún bit de paridad

Un bit de parada

Ningún tipo de control de flujo

La conexión al puerto de configuración puede realizarse con un cable DB-9 hembra a DB-9 macho, suministrado con el equipo. En el caso de que el terminal asíncrono disponga de conectores DB25, deberá utilizar un adaptador adicional DB9H-DB25H (incluido en el equipo).

Configuración del Equipo.

1. *Encendido de equipo.*

Una vez instalado el equipo se ha de proceder a encender el mismo, inmediatamente después tiene lugar un proceso de autotest e inicialización que a continuación se describe.

En primer lugar el equipo realiza un breve autotest en el que se comprueba que el programa de arranque es correcto y una breve detección e inicialización de la memoria de acceso aleatorio dinámico sincrónica (**SDRAM** - Synchronous dynamic random access memory), presente en el equipo que nos permite la entrega de ráfagas de información a altas velocidades utilizando una interfaz sincrónica).

En cada paso del proceso de autotest se enciende un LED en amarillo, en el panel frontal del equipo.

Si se detecta algún problema el proceso termina y el LED parpadea en rojo. Una vez terminado el proceso la consola esta disponible y empieza a mostrar datos.

Una vez terminado el proceso de arranque se realiza un autotest y auto detección del hardware de la placa. En primer lugar se encienden todos los LEDs del equipo en amarillo, luego en rojo y finalmente en verde, con ello se facilita la comprobación visual de su funcionamiento. Después por cada elemento interno comprobado se va encendiendo un LED del equipo en amarillo, prueba es satisfactoria el LED se queda en verde. Si se detecta un fallo el LED correspondiente se queda en rojo y una vez terminado el auto test, según el problema del equipo este se resetea y vuelve a repetir el proceso o permite operar por consola para la resolución del mismo.

Inicializado el equipo, se apagan todos los LEDs y se descomprime el código de la aplicación, proceso durante el cual el LED B2 parpadea en verde y por consola se muestran tantos puntos como bloques del código descomprimido.

Terminado el proceso de descompresión se ejecuta la aplicación; se lee la configuración y se muestra el prompt del equipo o un login de acceso. En esta situación si todo ha sido correcto el LED S estará en color verde.

Si se dispone de un terminal o un PC con emulador de terminal conectado a la consola del equipo, se puede ver una información de arranque similar a la que se muestra a continuación:

```
****************** Router Teldat ***************
BOOT CODE VERSION: 01.08.09 May 18 2004 15:40:57
gzip May 18 2004 15:32:30
P.C.B.: 43 MASK:0502 Microcode:0000
START FROM FLASH
BIOS CODE DUMP.
BIOS DATA DUMP.
End of BIOS dump
====================
BIOS TELDAT (c) Teldat
====================
BIOS CODE VERSION: 01.08.09
CLK=49152 KHz BUSCLK=49152 KHz L0
Date: 06/01/04, Tuesday Time: 11:28:50
SDRAM size: 64 Megabytes
BANK 0: 64 Megabytes (detected)
Caches: ON Write-Back
FLASH: 8 Mb.
NVRAM: 128 Kb.
EEPROM: 2048 Bytes.
DPRAM: 7168 Bytes.
WAN1: DCE
WAN2: DCE
WAN3: DCE
ISAC
RDSI_B

RDSI_B
FAST ETHERNET
PCI BRIDGE
Current production date: 03 15
Current software license: 2 16
Current serial number: 403/02684
TRYING APP CODE DUMP
(CONFIGURED) ATLAS.BIN.
APP DATA DUMP
```

```
Running application
Flash configuration read
Initializing
Teldat (c)2001-2004
Router model VisorALARM 2 16 CPU MPC860 S/N: 403/02684
1 LAN, 3 WAN Lines, 1 ISDN Line
```

Ahora, ya encendido el equipo y realizado el autotest, procederemos a la configuración del equipo VisorALARM, para su correcto funcionamiento.

La funcionalidad básica del VisorALARM es recibir alarmas de los equipos MIP por una red IP, y su envío a un software de automatización mediante un interfaz serie emulando una de las tres receptoras soportadas. Por lo tanto, la configuración del VisorALARM consta de tres partes básicas:

- Configuración inicial: nombre del equipo, usuario y password para acceder a consola, etc.

- Configuración IP: parámetros necesarios para obtener conectividad IP con los equipos MIP (dirección IP, máscara y Gateway).

- Configuración propia: para la recepción de alarmas.

La configuración del VisorALARM se puede realizar, como se ha citado anteriormente, con una conexión serie con el Interfaz AUX del equipo y un software de emulación de terminal en un PC. Además, si se dispone de conectividad IP con el equipo, se puede obtener la misma funcionalidad mediante una conexión telnet a la dirección IP del VisorALARM.

2. *Configuración inicial.*

El primer paso para la configuración es acceder al menú de configuración del equipo. Para ello se utiliza el comando “process 4” desde la consola del VisorALARM.

```
Teldat (c)2001-2004
Router model VisorALARM 2 16 CPU MPC860 S/N: 403/02684
1 LAN, 3 WAN Lines, 1 ISDN Line
*process 4
Config>
```

El segundo paso es asegurar de que se parte de una configuración vacía.

```
Config>no configuration
Config>
```

A continuación se establece un nombre de usuario y una clave para el acceso a la consola, para evitar accesos no deseados a la configuración del equipo. Este paso es opcional, pero es recomendable por motivos de seguridad. Elegir un nombre de usuario y una clave de acceso. El siguiente ejemplo muestra como configurar estos parámetros, utilizando **admin** como nombre de usuario y **vsrnet** como password.

```
Config>user admin password vsrnet
Config>
```

Un posible siguiente paso es configurar un nombre para el equipo. El propósito principal de dicho nombre es que aparezca en la consola del equipo para así poder distinguir entre diversos equipos en caso de que se disponga de varios equipos. Este parámetro es opcional.

El siguiente ejemplo muestra como configurarlo, utilizando RECEPTORA como nombre de equipo.

```
Config>set hostname RECEPTORA
RECEPTORA Config>
```

Por ultimo se ha de configurar el interfaz serie que va a utilizarse para el envío de las alarmas al software de automatización, para que funcione como “receptora”. Se recomienda usar el interfaz WAN 1, aunque no es obligatorio. El siguiente ejemplo muestra como realizar esta configuración.

```
RECEPTORA Config>set data-link arly serial0/0
RECEPTORA Config>
```

En el ejemplo se ha utilizado la interfaz serial 10/0, que corresponde con el interfaz WAN1. Si se quisiera utilizar otro interfaz, se debe sustituir por el serial10/1 para el interfaz WAN2 o serial 10/2 para el WAN 3.

Es necesario recalcar que sólo se puede configurar un interfaz para funcionar como receptora de Alarmas.

Por ultimo, se muestra la configuración para comprobar el estado de dicha configuración hasta el momento.

```
RECEPTORA Config>show config
; Showing System Configuration
; Router VisorALARM 2 16 Version 10.1.19
no configuration
set data-link arly serial0/0
set data-link x25 serial0/1
set data-link x25 serial0/2
set hostname RECEPTORA
user ADMIN hash-password F02B539270D0695387FB26F3B41185B8
;
;
;
;
;
; --- end ---
RECEPTORA Config>
```

3. *Configuración del Protocolo IP*

En este apartado se describen los pasos necesarios para configurar el protocolo IP en el VisorALARM. Aquí es necesario configurar lo siguiente:

- Dirección IP y mascara del interfaz Ethernet
- Dirección IP del Gateway o puerta de enlace predeterminada del VisorALARM.

Para acceder el entorno de configuración IP, se deberá introducir el siguiente comando.

```
RECEPTORA Config> PROTOCOL IP
RECEPTORA IP config>
```

A continuación se asigna la dirección IP junto con su mascara al interfaz Ethernet. En el siguiente ejemplo se le asigna la dirección 128.185.123.22 con la mascara 255.255.255.0.

```
RECEPTORA IP config>address ethernet0/0 128.185.123.22 255.255.255.0
```

El siguiente paso es configurar la dirección IP del Gateway. La dirección IP del Gateway debe pertenecer a la misma subred que la dirección IP del interfaz Ethernet. En el siguiente ejemplo se configura este parámetro tomando como valor 128.185.123.1

```
RECEPTORA IP config>route 0.0.0.0 0.0.0.0 128.185.123.1 1
RECEPTORA IP config>
```

Finalmente, se muestran la configuración de este menú y se vuelve al menú de configuración general.

```
RECEPTORA IP config>show config
; Showing Menu and Submenus Configuration
; Router VisorALARM 2 16 Version 10.1.19
;
```

```
address ethernet0/0 128.185.123.22 255.255.255.0
; ;
route 0.0.0.0 0.0.0.0 128.185.123.1 1
; ; ;
RECEPTORA IP config>exit
RECEPTORA Config>
```

4. *Configuración de Interfase de Emulación de receptora de alarmas (ARLY)*

El interfaz ARLY es un interfaz serie que dota al equipo de toda la funcionalidad de una receptora IP de alarmas, de manera que el equipo:

- Recibe las alarmas de los MIP registrados por red IP
- Emula una receptora convencional de alarmas enviando las alarmas por un puerto serie asíncrono para su procesado en un software de automatización de alarmas
- Supervisa los MIP registrados y genera la correspondiente alarma en caso de fallo de comunicación
- Soporta la instalación y mantenimiento de los MIP registrados.

A continuación se describe el proceso de configuración de los parámetros concernientes a la recepción de alarmas del VisorALARM. Para acceder a la configuración del interfaz ARLY se utiliza el comando NETWORK y la línea serie asociada al interfaz ARLY:

```
RECEPTORA Config>NETWORK SERIAL0/0
-- ARLY Interface Configuration --
RECEPTORA ARLY-1 Cfg>
```

5. *Patrón de configuración.*

Para facilitar la tarea de instalación de MIPs, el VisorALARM dispone de una funcionalidad que permite que un MIP se instale configurando un conjunto reducido de parámetros y mediante una operación de *registro*, reciba el resto de la configuración desde el VisorALARM.

El proceso completo se describe a continuación:

- El instalador configura, bien mediante consola serie o bien mediante consola telefónica, los siguientes parámetros en el MIP:

  Número de cuenta del cliente
  Dirección IP y mascara
  Dirección IP del Gateway o pasarela por defecto
  Dirección IP Pública del Visor Alarm
  Puerto UDP del VisorALARM

- Reinicia el MIP

- Ejecuta el comando de registro, introduciendo el password de instalador.

- El MIP envía un comando de registro a la dirección y puerto del VisorALARM configurados, cifrado con el password de instalador.

- El VisorALARM recibe el mensaje. Recorre la lista de patrones de configuración que tiene configurados y trata de descifrar el mensaje con la clave de cada patrón. Si el mensaje descifra bien, asume que ese patrón es el que debe utilizar y genera una

configuración para dicho MIP en base a los parámetros del patrón de confirmación.

- Envía la configuración al MIP, cifrada con el password de instalador.

- El MIP recibe la configuración. La activa y la guarda.

Por lo tanto, debe configurarse al menos un patrón de configuración si se desea utilizar este tipo de instalación. Tiene sentido añadir más de un patrón de configuración si se desean configurar MIPs con diferentes parámetros.

Mediante los patrones de configuración es posible establecer todos los parámetros del MIP, excepto el número de cuenta de cliente. Sin embargo, no es necesario especificar todos los parámetros configurables en un MIP, solo aquellos que se deseen cambiar en el MIP. Aquellos parámetros que no se especifiquen en el patrón, quedarán configurados en MIP con la configuración de fábrica.

Para crear un patrón de configuración, debe ejecutarse el siguiente comando. En el ejemplo se crea un patrón con identificador 5.

```
RECEPTORA ARLY-1 Cfg>cfg-pattern 5 default
RECEPTORA ARLY-1 Cfg>
```

Para configurar cada uno de los parámetros se utiliza la sintaxis:

```
RECEPTORA ARLY-1 Cfg>cfg-pattern 5 opcion valor
```

Las opciones disponibles son todos los parámetros de configuración del MIP, que se detallan a continuación:

- default: crea un patrón nuevo o pone valores por defecto a uno existente

- instalator-password: establece el password de instalador. Debe ir seguido de una cadena de hasta 16 dígitos hexadecimales
- receiver-ip: dirección pública o privada del VisorALARM. Debe ir seguido de una dirección IP

- receiver-udp-port: puerto UDP en el que el VisorALARM espera recibir los datos. Debe ir de un número del 1 al 65535

- usr-password: password de la consola del MIP. Debe ir seguido de una cadena de 16 caracteres formada por los dígitos hexadecimales o las letras UVWXYZ. El password que se envía MIP será una cadena de 16 dígitos hexadecimales que se obtiene de sustituir la letra U por el primer dígito del número de cuenta del MIP, la V por el segundo y así hasta la Z por el sexto. Es decir, si se confirma 0000UVWXYZ, cuando se instale el MIP cuyo número de cuenta sea 123456, se le enviará 0000123456 como password de usuario. De este modo se permite configurar diferentes password para cada MIP, usando el mismo patrón de configuración.

- mip-password: password con el que el MIP cifra los mensajes que envía. Debe ir seguido de una contraseña con el mismo formato que el parámetro usr-password

- receiver-password: password con el que el VisorALARM cifra los mensajes que envia. Debe ir seguido de una contraseña con el mismo formato que el parámetro usr-password

- keep-alive-timer: tiempo entre Keepalives en segundos. El valor debe estar entre 1 y 65535 segundos

- keep-alive-retries: número de intentos de keepalives en caso de fallo. El valor debe ser entre 1 y 9 segundos

- Keep-alive-retries-timer: tiempo entre los reintentos keepalives en segundos. El valor debe estar 1 y 9 segundos

- Phone-length: número de dígitos que componen el número de teléfono al que llama el panel para enviar alarmas

- Alarm-tx-retries: número de reintentos de envío de alarmas en caso de fallo

- Callback-phone: número de teléfono al que llama el MIP para tareas de bidireccionalidad en caso de que hubiese la línea telefónica

A continuación se muestran los comandos para configurar un patrón de configuración, cuyo identificador es el 1. En dicho patrón los parámetros dirección IP y puerto UDP del VisorALARM, no se han configurado, ya que ya están configurados en el MIP (son necesarios para la instalación) y no desea que se cambien.

```
RECEPTORA ARLY-1 Cfg>cfg-pattern 1 default
RECEPTORA ARLY-1 Cfg>cfg-pattern 1 instalator-password 1234
RECEPTORA ARLY-1 Cfg>cfg-pattern 1 usr-password 654321
RECEPTORA ARLY-1 Cfg>cfg-pattern 1 mip-password 1234WXYZ90
RECEPTORA ARLY-1 Cfg>cfg-pattern 1 receiver-password 0W8X6Y4Z2FEBA
RECEPTORA ARLY-1 Cfg>cfg-pattern 1 keep-alive-timer 60
RECEPTORA ARLY-1 Cfg>cfg-pattern 1 keep-alive-retries 2
RECEPTORA ARLY-1 Cfg>cfg-pattern 1 keep-alive-retries-timer 3
RECEPTORA ARLY-1 Cfg>cfg-pattern 1 phone-length 9
RECEPTORA ARLY-1 Cfg>cfg-pattern 1 alarm-tx-retries 2
RECEPTORA ARLY-1 Cfg>cfg-pattern 1 callback-phone 918076565
RECEPTORA ARLY-1 Cfg>
```

Si se desea cambiar una de la opciones basta con introducir el comando que la configura con un nuevo valor. Por ejemplo:

```
RECEPTORA ARLY-1 Cfg>cfg-pattern 1 keep-alive-retries-timer 2
RECEPTORA ARLY-1 Cfg>
```

Si se puede dejar una de las opciones con su valor por defecto, se debe teclear *no* seguido del comando que se utilizó para configurarlo. Por ejemplo:

```
RECEPTORA ARLY-1 Cfg>no cfg-pattern 1 keep-alive-retries-timer 2
RECEPTORA ARLY-1 Cfg>
```

Por ultimo, para borrar todo un patrón, debe teclearse el comando:

```
RECEPTORA ARLY-1 Cfg>no cfg-pattern 5 default
RECEPTORA ARLY-1 Cfg>
```

Una vez que un MIP se ha registrado se guarda su configuración en la configuración del interfaz ARLY, de modo que permanezca entre reinicios del VisorALARM.

4.2.2.3. SERVIDOR DE ALARMAS Y MONITOREO.

El software para el sistema de alarmas (visorALARM) se instalará en un computador Pentium IV el mismo que generará una pantalla con cada evento que sucediese, como alarma de incendio, robo, etc.

En el caso del sistema de monitoreo con las cámaras IP, estas tienen un software propietario el cual será instalado en un computador de similares características que los del software visorAlarm. Estos dos computadores forman parte fundamental del centro de gestión.

Las características del computador las indicamos a continuación:

MARCA: XTRATECH

Características del PC

- Modelo del procesador: Pentium IV
- Velocidad: 3.2 GHz
- Memoria RAM: 512 Mbytes
- Espacio en disco: 120 Gbytes
- Monitor: 21”
- Este PC estará conformado por: teclado, mouse, parlantes y un DVDWriter.

4.2.3. COMPONENTES DEL SISTEMA DE SEGURIDAD PARA EL ÁREA PERIMETRAL.

En este último bloque se detalla sólo un componente, que son las cámaras IP, las cuales que con sus características técnicas nos permitirán un sistema confiable en todo momento, quedando el cerco eléctrico como un complemento a la seguridad del área perimetral.

Las cámaras a utilizarse en el desarrollo de nuestro proyecto son las cámaras de la marca Mobotix modelo M1D-Night-R64. Estas cámaras poseen un alto grado de resolución y precisión en lo que a captación de imágenes se refiere, equipadas con los avances mas destacados de la tecnología alemana.

FIG. 4.37 Cámara MOBOTIX modelo M1D-Night-R64

A continuación se dará una breve descripción de las generalidades del producto, así como sus características, componentes y conexiones.

4.2.3.1. CÁMARA IP: MOBOTIX.

Para la selección de las cámaras IP, nos basamos del análisis de las diferentes características que poseen, pero nos basamos de ciertos parámetros básicos como: zoom, infrarrojo, para exterior y resolución.

Con lo que se elaboró la siguiente tabla para detallar nuestro análisis y poder concluir con la elección de una marca.

MARCA	ZOOM	INFRARROJO	EXTERIOR	RESOLUCION
VEO	bajo	bajo	bajo	Medio
LINK SYS	bajo	bajo	bajo	Medio
DLINK	medio	bajo	bajo	Medio
AXIS	alto	medio	alto	Alto
MOBOTIX	alto	alto	alto	alto

Tabla 4.13 Cuadro comparativo de las Cámaras IP

Como se puede observar la marca Axis puede ser también la más opcionada pero algunas de sus características son optativas, lo cual hiciera que su costo se incremente. Concluyéndose con la marca Mobotix.

Con ésta introducción seguimos con la descripción de este equipo.

Este modelo de cámaras dispone de la óptica avanzada para conseguir las mejores imágenes en cualquier condición de

iluminación. Son cámaras capaces de conmutar entre dos lentes, la visión diurna y la infrarroja (IR), sin renunciar a la existencia de otro tipo de teleobjetivo. Cuando la iluminación es deficiente conmuta a la lente de tipo infrarrojo consiguiendo un incremento de la luminosidad en una factor de 20. Con esta mejora en la luminosidad, el tiempo de exposición disminuye drásticamente, permitiendo grabar nítidamente escenas con movimiento en condiciones de luz pobre.

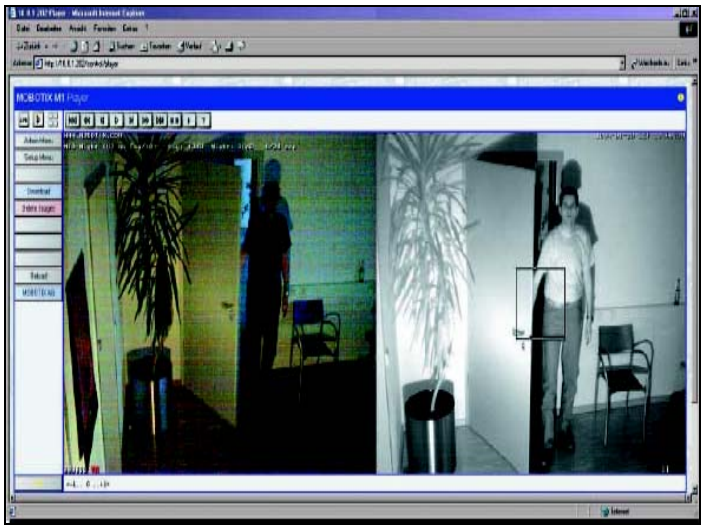


FIG. 4.38 Imagen original en la noche y en modo Infrarrojo

Las cámaras de este modelo, para redes IP ofrecen todas sus funcionalidades sin necesidad de instalar ningún software adicional. Tanto la administración y configuración de la cámara como la visión de las imágenes, puede ser efectuada desde cualquier navegador Web estándar. Su simplicidad, total compatibilidad y estructura cliente/servidor permite una fácil instalación en cualquier entorno de red ya existente.

Características

Las cámaras Mobotix modelo M1D-Night-R64 cuentan con las siguientes características:

- Cámara preparada para trabajar directamente con conexiones de red Ethernet y RDSI (Red Digital de Servicios Integrados).
- Cámaras con microprocesador Intel-Strongarm 128 Mb incorporado, con 235 MIPS (Millones de Instrucciones por segundo).
- Servidor de Web integrado con interfaz de red y Web.
- Sistema totalmente actualizable por software.
- La instalación no requiere software adicional.
- Óptica basada en sensores digitales CMOS (Complementary metallic oxide Semiconductor, semiconductor de oxido metálico complementario).
- Indexación y búsqueda real de cualquier imagen o vídeo capturado.
- Detección de movimiento en áreas definidas y seguimiento de objetos.
- Programación en la detección de eventos.

- Grabación de imágenes preliminares y posteriores a eventos.
- Generación de alarmas vía e-mail o FTP.
- Compresión de las imágenes en JPEG y MXPEG (sistema de compresión propietario basado en la compresión MPEG).
- Resoluciones de vídeo de alta calidad de hasta 640x480x12fps.
- Control de exposición.
- Compensación de luz de fondo.
- Balance automático de blancos.
- Mejoras de auto contraste y brillo.
- Capacidad para la definición de zonas de exposición para mejorar la compensación de luz de fondo.
- Exposición automática de 0,1ms a 1s.
- Control de ganancia automático de 12Hz.
- Memoria interna con capacidad para grabar hasta 50.000 imágenes.
- Gestión de passwords de hasta tres niveles (administración, usuario, invitado).
- Gestión de sonido integrada a través de RDSI.

- Conector RDSI integrado (dial-in, dial-out).

- Interfaz RS232 apto para módem/GSM/conexión serie.
- Posibilidad de integrar la conexión eléctrica en cable de red o RDSI.
- Diseño para exteriores de acuerdo con la norma IP65.

- Las cámaras proveen 3 modos digitales de zoom (ampliación de imágenes) y panning (panorámica). Simplemente se debe hacer clic para seleccionar la sección en la imagen que en vivo se quiera examinar más de cerca. Las tres imágenes en vivo de esta página demuestran la calidad del zoom digital; y sólo la configuración más alta de zoom requiere interpolación de píxeles.

FIG. 4.39 Ampliación de una imagen hasta 4 veces su tamaño (4x zoom)

4.2.3.2. ELEMENTOS Y CONEXIONES DE LAS CAMARAS MOBOTIX.

Las siguientes figuras denotan las vistas anterior y posterior de las cámaras Mobotix y de los componentes de las mismas:

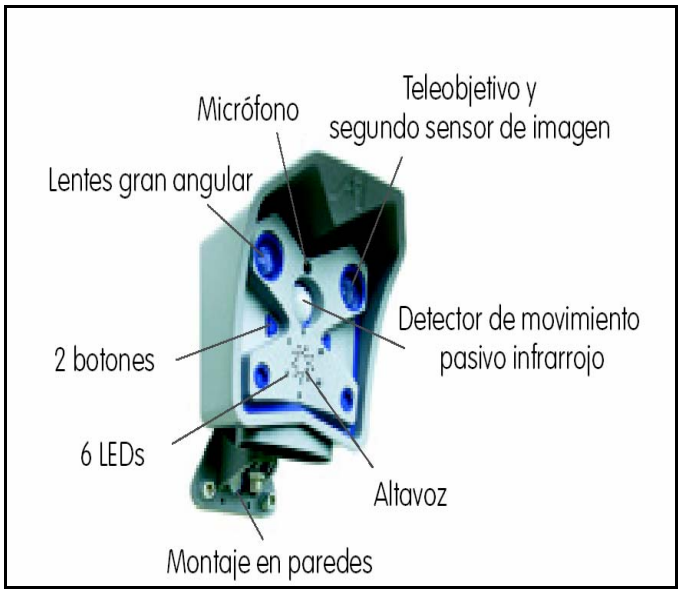


FIG. 4.40 Vista anterior de las cámaras Mobotix

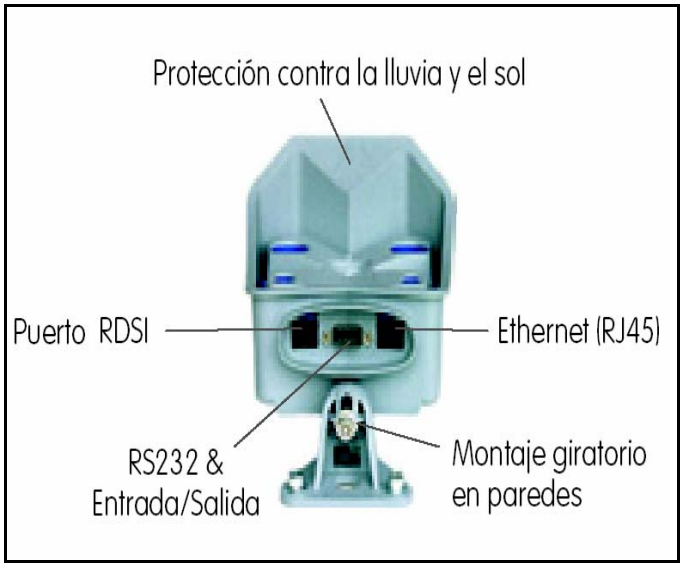


FIG. 4.41 Vista posterior de las cámaras Mobotix

Suministro de energía en las cámaras Mobotix

La cámara de MOBOTIX consume sólo 2.5 vatios a 30 V. Hay tres maneras de suministrar energía a la cámara:

1. **Mediante la conexión RDSI**

La energía viene directamente del cable conector hacia la red RDSI.

2. **Mediante una unidad de poder externa**

Conexión desde el suministro estándar de energía MOBOTIX (MX-SNT-E01-30-RJ) a uno de los conectores RJ45 de la cámara.

3. **Mediante el suministro de energía remota**

Usando el adaptador de poder de red (MX-NPA-3-RJ) y la unidad de energía externa MOBOTIX, la energía puede proporcionarse a través del cable de datos al RDSI o al puerto de Ethernet.

La conexión física de las cámaras MOBOTIX

Hay dos posibilidades de conectar la cámara de MOBOTIX físicamente, en donde ambas conexiones pueden usarse simultáneamente:

1. **Conexión a la red RDSI**

Esta conexión se la logra mediante la conexión directa al puerto de la red RDSI.

2. Conexión a la red ETHERNET

Conectando al switch o hub de la red local (LAN) usando el cable de conexión proporcionado.

La comunicación de las cámaras se realiza mediante el protocolo TCP/IP el cual incluye el protocolo PPP (Point to Point Protocol, Protocolo Punto a Punto) el mismo que nos permite la comunicación en las redes Ethernet como para redes RDSI. El acceso a la cámara vía RDSI es similar al acceso a internet mediante un proveedor RDSI. Todo lo que necesita es el número del teléfono de la cámara, el nombre del usuario, y las contraseñas respectivas de seguridad.

El número de IP de la cámara también sirve como el número de serie de cada una de ellas en la conexión a las redes RDSI. La dirección IP puede ser modificada cuando se lo requiera, después de que usted haya accedido a ella mediante cualquier navegador del Internet o del software propietario de la cámara. Actualmente, la conexión de DSL sólo puede establecerse para la conexión a las redes LAN mediante un módem con interfaz DSL.

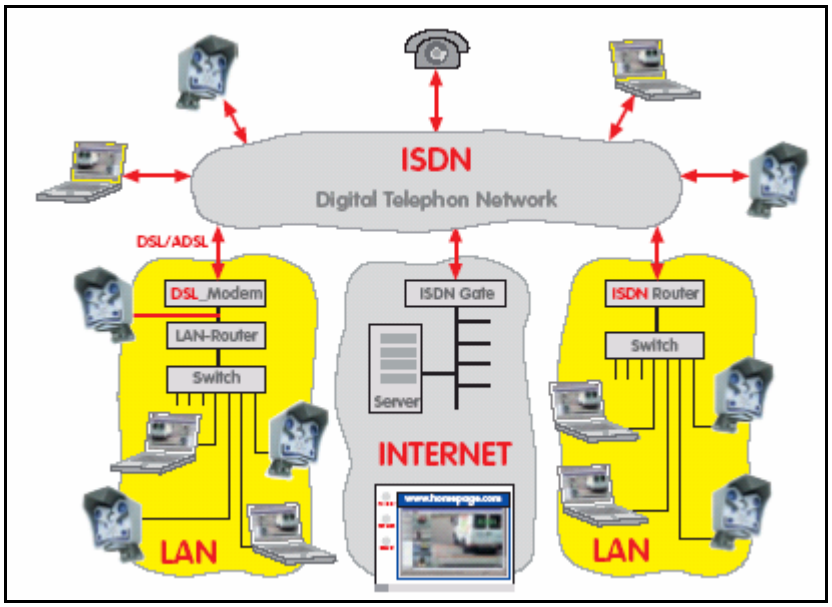


FIG. 4.42 Conexiones físicas de las cámaras Mobotix

Tanto en entornos pequeños como en grandes sistemas descentralizados, es una ventaja cuando usuarios esporádicos pueden acceder al sistema de vídeo simplemente a través del navegador. Esta plataforma de aproximación independiente requiere menos trabajo de instalación. MOBOTIX incluso ha implementado el acceso al sistema personal digital (**PDA** - Personal Digital Assistant), utilizando el navegador de un PC estándar, para poder lograr las siguientes destrezas:

- Búsqueda de eventos
- Reproducción de eventos
- Señales de alarma
- Pantalla con una lista de alarmas

- Administración de múltiples cámaras (hasta 16 cámaras), como se muestra en la siguiente figura:

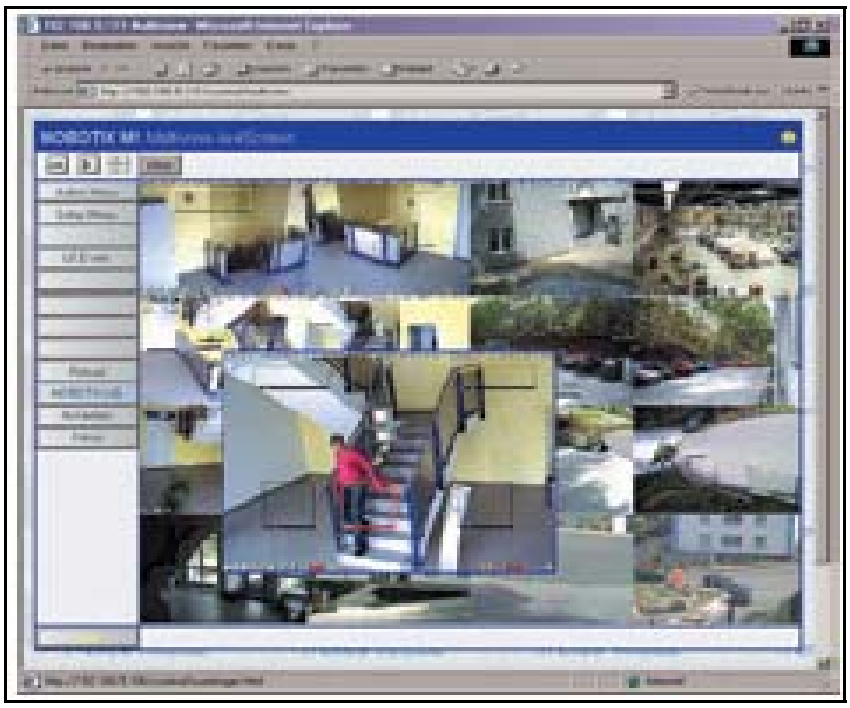


FIG. 4.43 Multi Vista con 16 cámaras en la ventana del navegador y zoom al pasar el ratón por encima

4.3. DISTRIBUCION DE LOS COMPONENTES EN EL SISTEMA DE SEGURIDAD.

Luego de la descripción de cómo funciona el sistema y de la descripción de cada componente utilizado en el mismo, sólo faltaría por describir la distribución de dichos componentes, tanto en los diferentes modelos de viviendas como en el área perimetral. En el caso del centro de gestión no es necesario un análisis de cómo tienen que ser distribuidos los equipos debido a que es un área adecuada para el monitoreo de las señales emitidas por los equipos.

4.3.1. DISTRIBUCIÓN DE LOS DISPOSITIVOS Y EQUIPOS DE SEGURIDAD EN LOS TRES MODELOS DE LAS VIVIENDAS.

La urbanización Punta Panorama cuenta con tres modelos de viviendas:

Un tipo de viviendas que es de una planta con dos dormitorios (CARLA), un segundo tipo que es de una planta con tres dormitorios (CAMILA) y un tercer modelo que son las viviendas de dos plantas con tres dormitorios (KARINA).

La distribución de los dispositivos será en función del modelo de vivienda, como se había dicho anteriormente, la urbanización posee tres modelos de viviendas, por ello la distribución de los dispositivos será de la siguiente manera:

En el primer modelo de viviendas (Modelo Carla), se ha dispuesto colocar en cada puerta y ventana un contacto magnético; en la sala y comedor se colocará detectores de movimientos cercanos a posibles accesos, después se colocarán detectores de humo en los dormitorios y en la sala de la vivienda así como también un detector térmico en la cocina para precautelar algún conato de incendio.

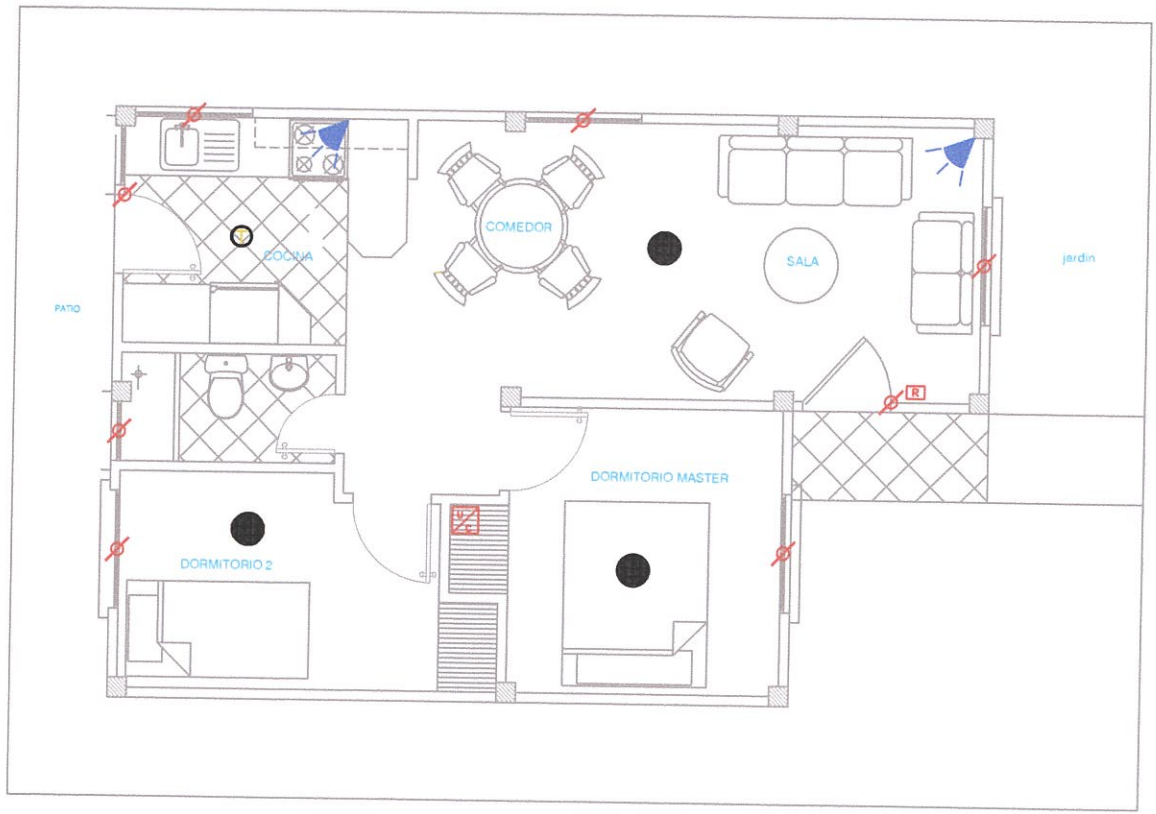
El PA va a estar ubicado en el área del closet de los dormitorios Master de las viviendas.

La ubicación del panel de control de alarmas debe de ser en un lugar donde el acceso no sea muy fácil para evitar manipulaciones maliciosas que boicoteen el funcionamiento del mismo, en cambio el teclado de

mandos debe ir de ser posible en un lugar cercano al ingreso principal de la vivienda para su fácil manipulación y programación del sistema de alarmas.

La misma técnica de ubicación de los sensores y demás dispositivos de seguridad se debe aplicar al resto de modelo de viviendas.

A continuación se verá los planos de la distribución de estos dispositivos en dichas viviendas (ver figuras 4.44, 4.45, 4.46 y 4.47).

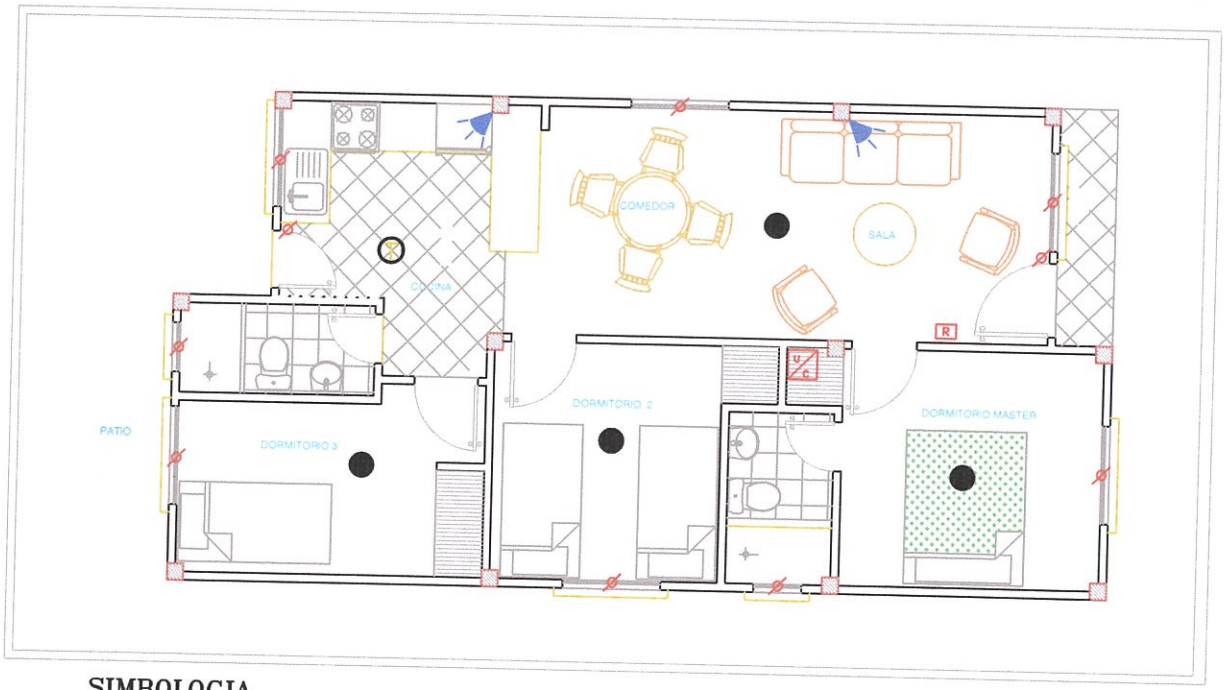


SIMBOLOGIA

- CONTACTO MAGNETICO TUBO TERMINAL EN PERFIL DE PUERTAS Y VENTANAS
- DETECTOR DE MOVIMIENTO
- TECLADO DE MANDO
- DETECTOR DE HUMO CAJA OCTOGONAL GRANDE EN TUMBADO
- PANEL DE CONTROL
- DETECTOR TERMICO CAJA OCTOGONAL GRANDE EN TUMBADO

FACULTAD DE INGENIERIA EN ELECTRICIDAD Y COMPUTACION

	FECHA	NOMBRE:	DENOMINACION:	ESCALA:
Dib.		VAMS	DISEÑO DEL SISTEMA DE SEGURIDAD MODELO CARLA	1:50
Rev.		DI		
Aprov.		AC		
ESPOL			FIGURA No. 4.44	

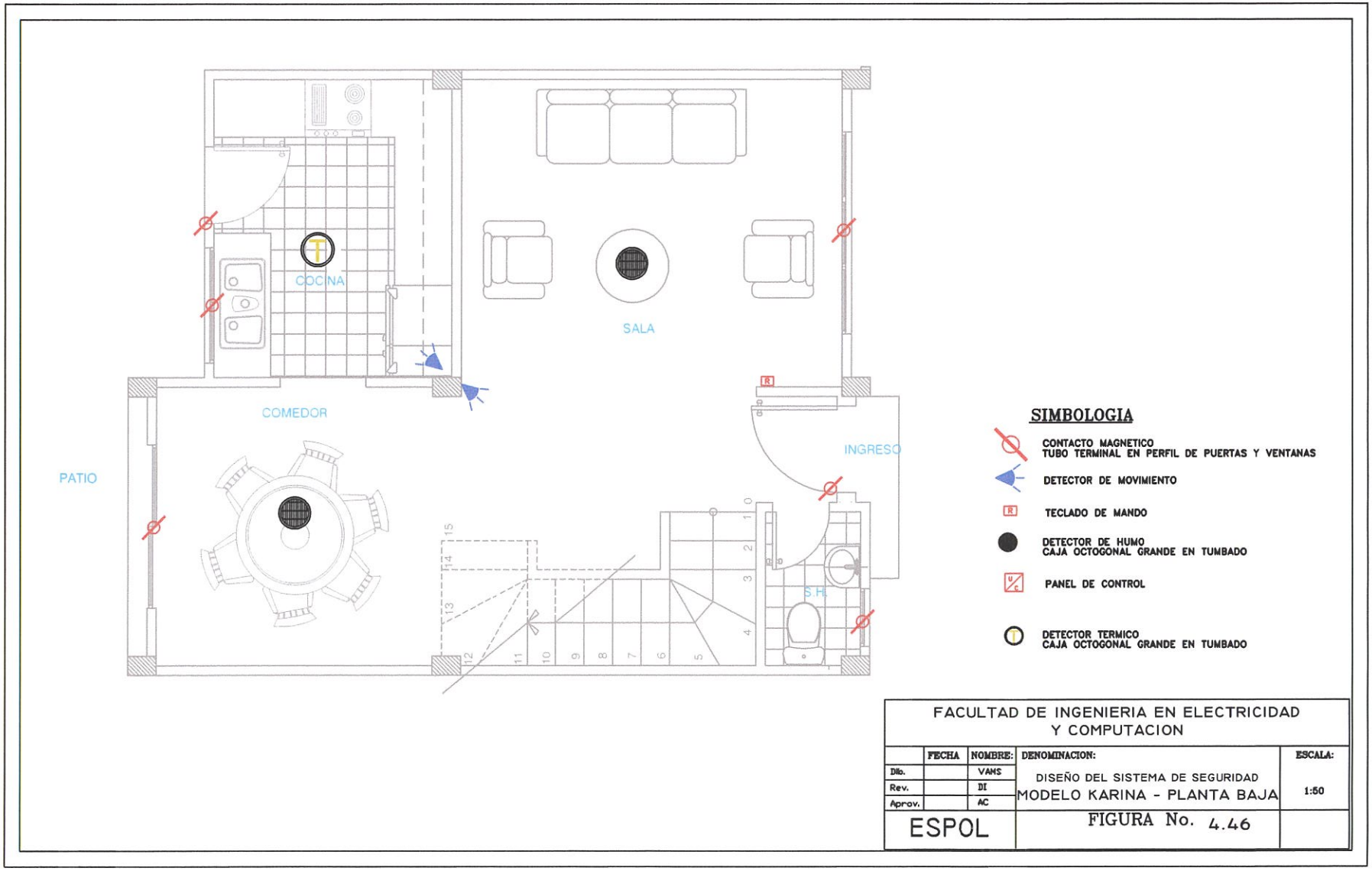


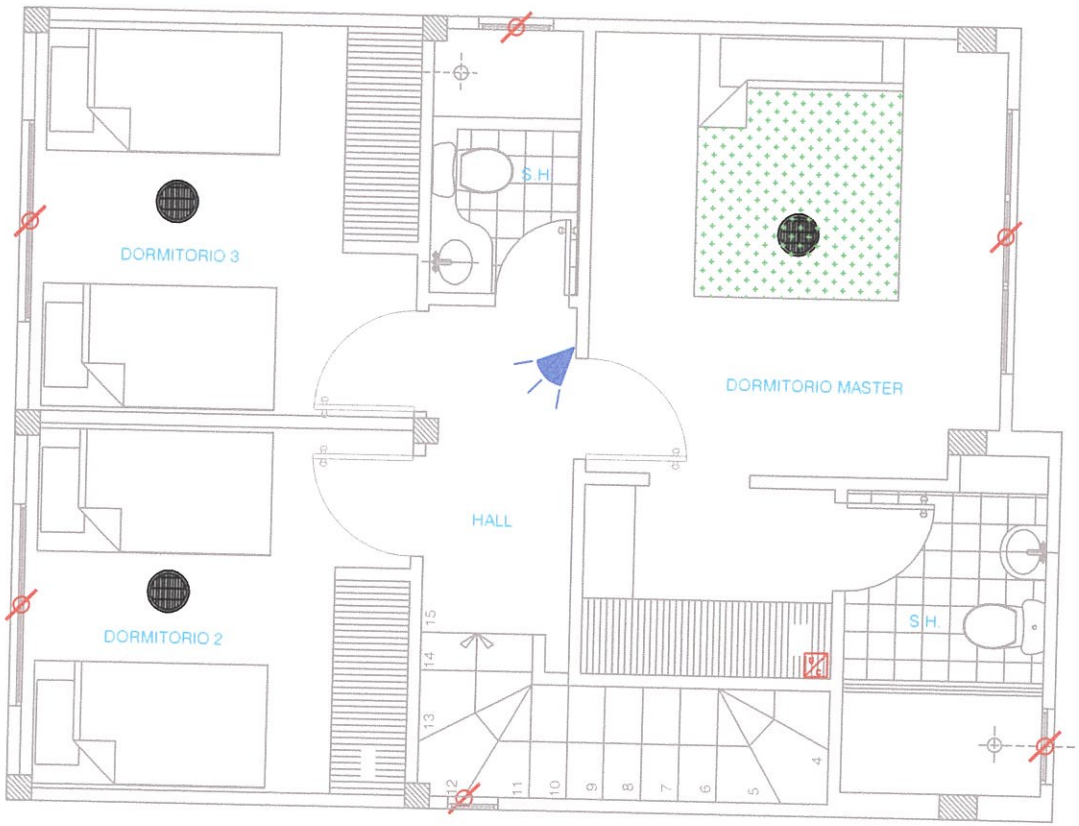
SIMBOLOGIA

- CONTACTO MAGNETICO
  TUBO TERMINAL EN PERFIL DE PUERTAS Y VENTANAS
- DETECTOR DE MOVIMIENTO
- TECLADO DE MANDO
- DETECTOR DE HUMO
  CAJA OCTOGONAL GRANDE EN TUMBADO
- PANEL DE CONTROL
- DETECTOR TERMICO
  CAJA OCTOGONAL GRANDE EN TUMBADO

FACULTAD DE INGENIERIA EN ELECTRICIDAD Y COMPUTACION

	FECHA	NOMBRE:	DENOMINACION:	ESCALA:
Dib.		VAMS	DISEÑO DEL SISTEMA DE SEGURIDAD MODELO CAMILA	1:50
Rev.		DI		
Aprov.		AC		
ESPOL			FIGURA No. 4.45	


COCINA
SALA
COMEDOR
PATIO
INGRESO
S.H.
SIMBOLOGIA
CONTACTO MAGNETICO
TUBO TERMINAL EN PERFIL DE PUERTAS Y VENTANAS
DETECTOR DE MOVIMIENTO
TECLADO DE MANDO
DETECTOR DE HUMO
CAJA OCTOGONAL GRANDE EN TUMBADO
PANEL DE CONTROL
DETECTOR TERMICO
CAJA OCTOGONAL GRANDE EN TUMBADO
FACULTAD DE INGENIERIA EN ELECTRICIDAD
Y COMPUTACION
FECHA
NOMBRE:
Dib.
VANS
Rev.
DI
Aprov.
AC
DENOMINACION:
DISEÑO DEL SISTEMA DE SEGURIDAD
MODELO KARINA - PLANTA BAJA
ESCALA:
1:50
ESPOL
FIGURA No. 4.46



SIMBOLOGIA

- CONTACTO MAGNETICO TUBO TERMINAL EN PERFIL DE PUERTAS Y VENTANAS
- DETECTOR DE MOVIMIENTO
- TECLADO DE MANDO
- DETECTOR DE HUMO CAJA OCTOGONAL GRANDE EN TUMBADO
- PANEL DE CONTROL

PLANTA ALTA

ESCALA: 1:50

FACULTAD DE INGENIERIA EN ELECTRICIDAD Y COMPUTACION				
	FECHA	NOMBRE:	DENOMINACION:	ESCALA:
Dib.		VAMS	DISEÑO DEL SISTEMA DE SEGURIDAD MODELO KARINA - PLANTA ALTA	1:50
Rev.		DI		
Aprov.		AC		
ESPOL			FIGURA No. 4.47	

4.3.2. DISTRIBUCIÓN DE LAS CÁMARAS IP EN EL ÁREA PERIMETRAL.

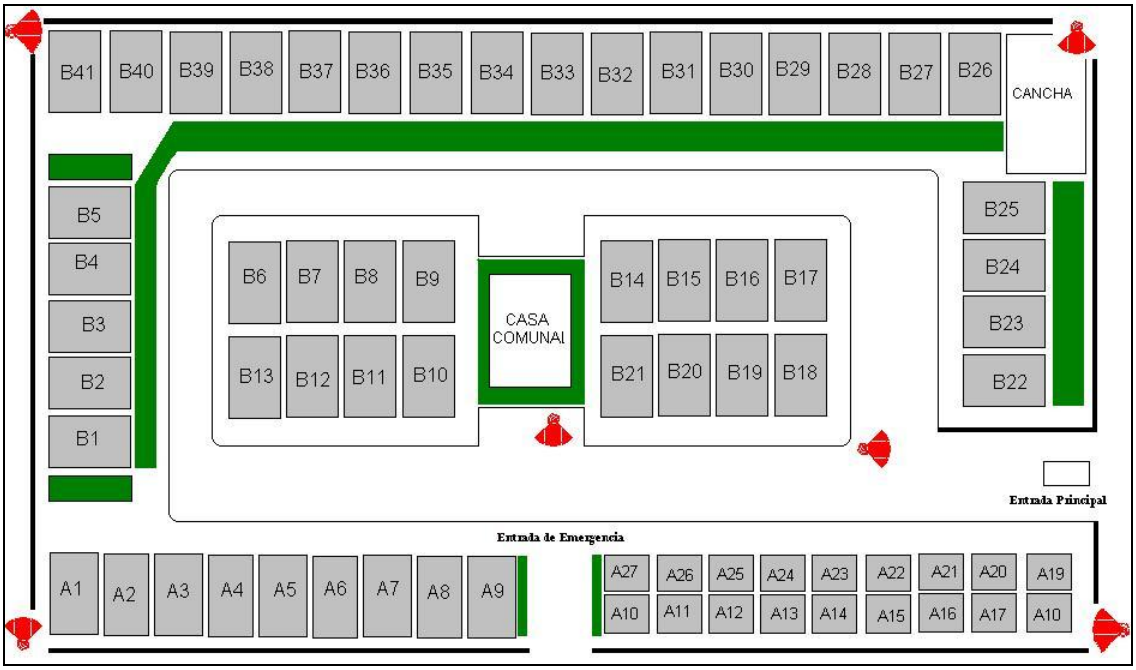


FIG. 4.48 Ubicación de las cámaras IP en la urbanización

La primera cámara supervisará la entrada principal a la urbanización cubriendo su extensión.

La segunda cámara estará ubicada en la salida de emergencia cubriendo el lado lateral izquierdo.

La tercera será ubicada en la esquina posterior izquierda que hace lindero con la ciudadela, cubriendo la calle posterior última y la lateral.

La cuarta cámara será instalada en la esquina posterior derecha que lindera la ciudadela y cubrirá la calle lateral derecha y se complementara con la tercera cámara en la supervisión de la calle última de la ciudadela.

La quinta estaría ubicada en la esquina izquierda frontal y ofrecerá el servicio de seguridad a las 9 viviendas que tienen su entrada principal hacia la ciudadela Panorama.

La sexta y última cámara será ubicada en la esquina derecha frontal para reforzar el trabajo de la cuarta cámara.

Cada cámara será conectada a las viviendas más cercanas a cada swich no gestionable, tal como indica mas en la descripción del mismo en la sección de equipos conectados a la vivienda.

4.4. DEDUCCIÓN DE PARÁMETROS PARA EL SISTEMA DE SEGURIDAD.

Finalmente, queda por dimensionar dos parámetros importantes en el desarrollo del diseño de este sistema, los cuales son: el ancho de banda a usar en la red y desarrollar la asignación de las direcciones IP para cada elemento de dicha red.

4.4.1. CÁLCULO DEL ANCHO DE BANDA DEL SISTEMA DE SEGURIDAD.

Para la transmisión de la información desde las viviendas hasta la consola de seguridad, como ya se ha dicho con anterioridad, contamos con el sistema inalámbrico BreezeAccess VL el cual nos proporciona un ancho de banda de hasta 54Mbps.

De aquí tenemos que contar el requerimiento tanto del servicio de voz, datos y video:

- La interfaz BreezeAccess RG es un equipo que hace uso de los codecs de voz G.723.1 lo que nos permite trabajar a velocidades tan bajas como los 5.3 Kbps.

- Los equipos MIPs y el VisorALARM en el proceso de sondeo y emisión de alarmas hacen uso de aproximadamente unos 10Kbps.

- Las cámaras para el proceso de compresión y transmisión de las imágenes hacen uso de aproximadamente 3Mbps.

Para realizar el cálculo del ancho de banda de nuestro sistema de seguridad, tomaremos el caso crítico para el cual todas las cámaras están transmitiendo, así también todas las viviendas se están comunicando por telefonía IP y el equipo MIP con el VisorALARM están en plena operación de sondeo y transmisión de alarmas:

Al instalar 6 cámaras en la urbanización y como cada una requiere de 3Mbps para transmitir las imágenes, entonces se necesitarán 18Mbps; una vivienda consume unos 15.3 Kbps en la transmisión de voz y datos, pero como son sesenta y ocho viviendas tenemos entonces 1.04Mbps. Por la tanto en este caso el sistema requiere de unos 19.04 Mbps lo cual representa aproximadamente el 35.26% del ancho de banda total teniendo un 64.74% del ancho de banda disponible para futuras expansiones. Este porcentaje nos garantiza que el sistema tendrá una aceptable tasa de

transmisión de voz, datos y video. Por supuesto de que este cálculo es en una situación extrema pero que nos da a conocer la demanda en una situación así, pero lo real esta muy distante a esta situación.

4.4.2. ASIGNACIÓN DE DIRECCIONES IP.

La asignación de las direcciones IP de la red, es decir, las direcciones que se le asignarán a cada equipo BreezeAccess suscriptor, así como de los equipos instalados en cada vivienda y en la consola de seguridad se la hará tomando direcciones IP privadas todas pertenecientes al mismo segmento de direcciones, todas de la clase C, la misma que nos permitirá la instalación de hasta 255 equipos en la red.

Para el direccionamiento se ha determinado tomar como el gateway del sistema al equipo estación base del centro de gestión, al cual se le ha designado la dirección IP: 192.168.100.1.

A continuación se detallará mediante un cuadro, el direccionamiento IP, el Netmask, el Gateway y la descripción del equipo al cual se le atribuye dicho direccionamiento, esto se la ha desarrollado para la consola de seguridad, las sesenta y ocho viviendas y las cámaras.

LOCALIDAD	IP	NETMASK	GATEWAY	EQUIPO
Consola de seguridad	192.168.100.1	255.255.255.0		Estación Base
	192.168.100.2	255.255.255.0	192.168.100.1	Servidor de Alarmas
	192.168.100.3	255.255.255.0	192.168.100.1	Servidor de Imágene
	192.168.100.4	255.255.255.0	192.168.100.1	Interfaz de telefonía
	192.168.100.5	255.255.255.0	192.168.100.1	Receptora de Alarma
	192.168.100.6	255.255.255.0	192.168.100.1	MIP
Vivienda # 1	192.168.100.7	255.255.255.0	192.168.100.1	Bridge inalámbrico
	192.168.100.8	255.255.255.0	192.168.100.1	Interfaz de telefonía
	192.168.100.9	255.255.255.0	192.168.100.1	MIP
Vivienda # 2	192.168.100.10	255.255.255.0	192.168.100.1	Bridge inalámbrico
	192.168.100.11	255.255.255.0	192.168.100.1	Interfaz de telefonía
	192.168.100.12	255.255.255.0	192.168.100.1	MIP
Vivienda # 3	192.168.100.13	255.255.255.0	192.168.100.1	Bridge inalámbrico
	192.168.100.14	255.255.255.0	192.168.100.1	Interfaz de telefonía
	192.168.100.15	255.255.255.0	192.168.100.1	MIP
Vivienda # 4	192.168.100.16	255.255.255.0	192.168.100.1	Bridge inalámbrico
	192.168.100.17	255.255.255.0	192.168.100.1	Interfaz de telefonía
	192.168.100.18	255.255.255.0	192.168.100.1	MIP
Vivienda # 5	192.168.100.19	255.255.255.0	192.168.100.1	Bridge inalámbrico
	192.168.100.20	255.255.255.0	192.168.100.1	Interfaz de telefonía

La configuración del resto de equipos, se debe realizar como se ha detallado anteriormente:

LOCALIDAD	IP	NETMASK	GATEWAY	EQUIPO
	192.168.100.198	255.255.255.0	192.168.100.1	MIP
Vivienda # 66	192.168.100.199	255.255.255.0	192.168.100.1	Bridge inalámbrico
	192.168.100.200	255.255.255.0	192.168.100.1	Interfaz de telefonía
	192.168.100.201	255.255.255.0	192.168.100.1	MIP
Vivienda # 67	192.168.100.202	255.255.255.0	192.168.100.1	Bridge inalámbrico
	192.168.100.203	255.255.255.0	192.168.100.1	Interfaz de telefonía
	192.168.100.204	255.255.255.0	192.168.100.1	MIP
Vivienda # 68	192.168.100.205	255.255.255.0	192.168.100.1	Bridge inalámbrico
	192.168.100.206	255.255.255.0	192.168.100.1	Interfaz de telefonía
Cámaras	192.168.100.207	255.255.255.0	192.168.100.1	Cámara 1
	192.168.100.208	255.255.255.0	192.168.100.1	Cámara 2
	192.168.100.209	255.255.255.0	192.168.100.1	Cámara 3
	192.168.100.210	255.255.255.0	192.168.100.1	Cámara 4
	192.168.100.211	255.255.255.0	192.168.100.1	Cámara 5
	192.168.100.212	255.255.255.0	192.168.100.1	Cámara 6

Tabla 4.14 Direccionamiento IP de los equipos de las viviendas y del centro de gestión

CAPITULO 5

ANÁLISIS DE LOS COSTOS Y FINANCIAMIENTO DEL PROYECTO.

5.1. ANÁLISIS DE LA INVERSIÓN TOTAL DEL PROYECTO.

Para el cálculo de la inversión inicial del proyecto debemos tener en cuenta la cantidad de dispositivos necesarios para implementar el sistema de alarmas en los tres diferentes modelos de viviendas existentes en la urbanización, por lo cual se realiza la siguiente deducción de los costos para la adquisición de los dispositivos para cada modelo.

5.1.1. DEDUCCIÓN DEL COSTO DE LOS SISTEMAS DE ALARMAS POR MODELO DE VIVIENDAS.

Tal y como se dijo en el ítem anterior en la urbanización existen tres modelos de viviendas, por lo cual el cálculo de los costos para los sistemas de alarmas debe hacerse en función de ello, a continuación se desarrolla los análisis específicos para cada caso:

5.1.1.1. MODELO CARLA.

Este modelo está constituido por las 18 viviendas de una planta con dos dormitorios. Para la implementación del sistema de alarmas se necesitará el siguiente número de dispositivos:

DESCRIPCION	UNID	P.U. ($)	P.TOTAL ($)
Contactos magnéticos	8	1,50	12,00
Detector de humo	3	49,00	147,00
Detector térmico	1	38,00	38,00
Detector de movimiento	2	13,00	26,00
Panel de control con teclado	1	121,00	121,00
MIP	1	180,00	180,00
Interfaz telefónica	1	300,00	300,00
Switch	1	45,00	45,00
Equipo suscriptor	1	600,00	600,00
		Sub-total	1.469,00
		IVA 12%	176,28
		TOTAL	**1.645,28**

TABLA 5.1 Costos de los dispositivos para el modelo Carla

Este es el valor para instalar el sistema de alarmas en una vivienda de este tipo, por lo que el costo total para la implementación del sistema en las 18 viviendas es de:

$$CT_D = 18 * 1.645{,}28 = \$29.615{,}04$$

5.1.1.2. MODELO CAMILA.

El modelo Camila está constituido por las 41 viviendas de una planta con tres dormitorios, para la implementación del sistema de alarmas para este modelo se necesitará el siguiente número de dispositivos:

DESCRIPCION	UNID	P.U. ($)	P.TOTAL ($)
Contactos magnéticos	10	1,50	15,00
Detector de humo	4	49,00	196,00
Detector térmico	1	38,00	38,00
Detector de movimiento	2	13,00	26,00
Panel de control con teclado	1	121,00	121,00
MIP	1	180,00	180,00
Interfaz telefónica	1	300,00	300,00
Switch	1	45,00	45,00
Equipo suscriptor	1	600,00	600,00
		Sub-total	1.521,00
		IVA 12%	182,52
		TOTAL	1.703,52

TABLA 5.2 Costos de los dispositivos para el modelo Camila

Este es el valor para poder instalar el sistema de alarmas en una vivienda de este modelo, en donde se tiene 41 casas, por lo tanto el costo total para la implementación de los sistemas de alarmas será:

$$CT_D = 41 * 1.703{,}52 = \$69.844{,}32$$

5.1.1.3. MODELO KARINA.

Este modelo está constituido por las 9 viviendas de dos plantas con tres dormitorios, para la implementación del sistema de alarmas para este modelo de viviendas se necesitará el siguiente número de dispositivos:

DESCRIPCION	UNID	P.U. ($)	P.TOTAL ($)
Contactos magnéticos	12	1,50	18,00
Detector de humo	5	49,00	245,00
Detector térmico	1	38,00	38,00
Detector de movimiento	3	13,00	39,00
Panel de control con teclado	1	121,00	121,00
MIP	1	180,00	180,00
Interfaz telefónica	1	300,00	300,00
Switch	1	45,00	45,00
Equipo suscriptor	1	600,00	600,00
		Sub-total	1.586,00
		IVA 12%	190,32
		TOTAL	1.776,32

TABLA 5.3 Costos de los dispositivos para el modelo Karina

Este es el valor para poder implementar el sistema de alarmas en una vivienda de este modelo y a esto se lo multiplica por 9 se obtiene el costo total para la implementación de los sistemas de alarmas, siendo:

$$CT_D = 9 * 1.776{,}32 = \$15.986{,}88$$

La suma de estos tres valores nos dará el monto necesario que se necesitará para la instalación de los sistemas de alarmas en todas las viviendas de la urbanización:

Por lo tanto tenemos:

$$CT_S = 29.615{,}04 + 69.844{,}32 + 15.986{,}88 = \$115.446{,}24$$

Una vez de que se ha hecho el análisis del requerimiento de los dispositivos y del costo para lograr la implementación de los sistemas de alarmas en todas la viviendas de la urbanización, vamos ahora a realizar un estudio del costo total de la inversión inicial para la automatización del sistema de seguridad, así en el siguiente cuadro se muestra un resumen de los equipos necesarios, sus respectivos costos para poner en funcionamiento el proyecto:

DESCRIPCION	UNID	P.U. ($)	P.TOTAL ($)
Switchts de 8 puertos	1	45,00	45,00
Cámaras IP	6	1.200,00	7.200,00
Radio base + unidad de acceso + antena omnidireccional	1	5.000,00	5.000,00
Interfaces para telefonía IP	1	300,00	300,00
Computadores para monitoreo	2	839,44	1.678,88
Equipo receptor de alarmas VisorALARM	1	2.500,00	2.500,00
Teléfonos digitales convencionales	1	15,00	15,00
Sistemas de Alarmas en las viviendas (CT_S)			115.446,24
Costo total para la adquisición de equipos			**132.185,12**

TABLA 5.4 Costo total del sistema de seguridad

5.2. INVERSION TOTAL DEL PROYECTO.

A la inversión inicial para la adquisición de los equipos, es decir, los **132.185,12 dólares**, se le adicionará el costo del mantenimiento incluido en la garantía de 1 año que se le otorgará al contratista por el sistema de seguridad, el mismo que tendrá un valor de **15000 dólares**.

Así también se debe de tomar en cuenta la mano de obra necesaria para la instalación y configuración del sistema, para este hecho se ha determinado la contratación de tres técnicos, para la instalación, configuración y puesta en marcha del sistema, la contratación se hará por un lapso de dos meses, tiempo estimado para la culminación del proyecto, los mismos que recibirán un sueldo de **500 dólares** mensuales.

Entonces:

$$M_{obra} = 3 * 500 * 2_{meses} = \$3.000$$

La suma de todos estos gastos nos da el total de Inversión de: **150.185,12 dólares.**

$$T_E = CT_S + Mant + M_{obra} = 132.185{,}12 + 15.000 + 3.000 = \$150.185{,}12$$

5.3. FINANCIAMIENTO DEL COSTO DEL PROYECTO.

El valor de **$ 150.185,12** calculado como total de la inversión, que involucra la adquisición de equipos, el pago de mano de obra y garantía, será financiado por el Banco de Guayaquil.

A continuación se calculará la mensualidad que deberán cancelar los copropietarios de la urbanización al Banco, considerando el análisis del sistema actual de seguridad, el sistema actual pero correcto y el sistema propuesto. Este análisis se debe realizar para obtener valores reales que nos indiquen si justifican la inversión propuesta.

Como primera premisa tenemos el sistema actual, el cual cuenta con 4 guardias divididos en dos turnos de 12 horas cada uno. Con este servicio los copropietarios pagan una mensualidad de $ 30, el cual se lo desglosa de las siguientes referencias:

$$Costo\_guardia = sueldo + movilización + a\lim entación = 230 + 30 + 50 = \$310/guardia$$
$$Costo\_operativo = \$800/turno\_de\_dos\_guardias$$
$$Costo\_total = (4*310) + 800 = 1240 + 800 = \$2040$$
$$Valor\_por\_vivienda = 2040/68 = \$30$$

Ahora nos basaremos del mismo sistema pero corregido. Para esto se considera el área de la urbanización (15.000 m^2) y el número de viviendas construidas (68) para calcular cuántos guardias deberían cuidar dicha urbanización; concluyendo que lo óptimo es 12 guardias por turno de 8 horas cada uno, por lo que:

$$Costo\_operativo = 12 * 400 = \$4.800 / turno\_de\_doce\_guardias$$
$$Costo\_total = (36 * 310) + 4.800 = 11.160 + 4800 = \$15.960$$
$$Valor\_por\_vivienda = 15.960 / 68 = \$235$$

Con este cálculo los copropietarios deberán pagar por este nuevo servicio una mensualidad de $235. Este valor es el que nos va a servir de base para el siguiente análisis.

Teniendo como referencia estos dos valores, solo faltaría calcular en que tiempo se va a pagar el valor financiado y cuál va hacer la mensualidad con el sistema propuesto.

Para el primer punto, nos basamos en la comparación del sistema actual corregido con el nuevo sistema, ya que ambos garantizan la seguridad de la urbanización. Es decir, los copropietarios deben cancelar mensualmente $ 235 de los cuales hay que desglosarlos para pago de financiamiento y pago de los guardias, quedando $ 205 sólo para lo primero.

Cálculo del periodo del valor a financiar

Hay dos formas para deducir el tiempo en que los copropietarios van a terminar de cancelar el financiamiento, por medio de un cálculo en Excel o por medio de unas fórmulas.

Datos:

Valor a financiar: $ 150.185,12

Ingreso mensual: $ 205 * 68 = $ 13.940

Interés anual: 8 %

1. Cálculo en Excel:

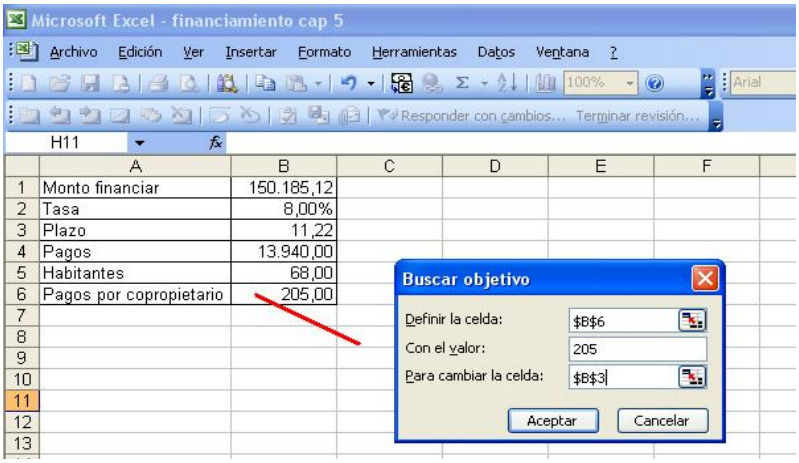


FIG. 6.1 Visualización del cálculo con Excel.

Para calcular el tiempo en que se debe de pagar el financiamiento se lo realiza por medio de la función herramientas y se escoge buscar objetivo, en el primer campo colocamos el pago por copropietario (la cual debe haber una fórmula), en el campo valor colocamos los $ 205 que es lo que se esta destinando para el pago y en el último campo colocamos el plazo, por lo que nos arroja un plazo de 11.22 meses lo cual se lo redondea a 12 o 1 año.

2. Cálculo con fórmula:

Para esto nos guiaremos de las tablas de interés compuesto, pero para ello necesitamos calcular dos parámetros: el factor de recuperación del capital (FRC) o factor A/P, y el interés efectivo.

$$A/P = \frac{13.940}{150.185{,}12} = 0{,}0928187$$

$$i = (1+i_a)^{1/m} - 1 = (1+0{,}08)^{1/12} - 1 = 0{,}006434 = 0{,}64\%$$

Con estos dos datos se va a las tablas para revisar cual sería el periodo. Las tablas se las encuentra adjuntas en el apéndice.

- Para el interés del 0,5 %, el factor A/P se encuentra entre 0,09366 y 0,08607, por lo que el periodo está entre 11 y 12 meses.

- Ahora en el caso del 0,75 %, el factor A/P esta entre 0,09505 y 0,08745, coincidiendo también en un periodo de 11 a 12 meses.

Con lo que se concluye que el tiempo que los copropietarios deben pagar dicho financiamiento es de 12 meses.

Cálculo de la mensualidad por el nuevo sistema

Luego de haber cancelado la deuda los copropietarios al Banco, la mensualidad que se va a calcular se basará en: mantenimiento de los equipos y para seguir pagando a los cuatro guardias. Entonces, el costo por el mantenimiento semestral de los equipos es de $ 600 (dos al año) y los $ 30 mensuales por los guardias.

$$Mc = \frac{1200}{68*12} = \$1{,}47 mensualidad / copropietario$$

Entonces el valor que deben cancelar mensualmente los copropietarios es de:

$$M_T = 30 + 1{,}47 = 31{,}47 \equiv \$31{,}5$$

Con esto nos podemos dar cuenta que el ahorro que el copropietario va hacer mensualmente es significativo, entre el sistema convencional de seguridad y el sistema propuesto, ya que:

$$Ahorro = 235 - 31{,}5 = \$203{,}5$$

Además, se considera el ahorro de la vida útil de los equipos por copropietario y por el conjunto, los cuales serían:

$$Ahorro\_anual\_vida\_útil_{copropietario} = 9años(no\_deuda) * 203{,}5 * 12(meses) = \$21.978$$
$$Ahorro\_anual\_vida\_útil_{conjunto} = 21.978 * 68 = \$1´494.504$$

CONCLUSIONES

El presente proyecto tuvo como principio el ofrecer una alternativa tecnológicamente viable en lo que a sistemas de seguridad electrónica se refiere, para lo que se ha realizó la investigación de diversos productos y sistemas los que en conjunto permitieron convertir en realidad el mencionado principio.

Para el desarrollo del diseño de este proyecto se escogieron dispositivos de gran aceptación en mercados muy exigentes como el mercado norteamericano y europeo, desde los detectores en los sistemas de alarmas en las viviendas hasta el equipo para establecer nuestra red de acceso inalámbrico. Dicha determinación se la realizo con el propósito de cumplir con una importante finalidad de nuestro proyecto el cual es el desarrollo de un sistema rápido, confiable y que otorgue las garantías a los usuarios en el momento de optar por nuestra propuesta.

La cantidad de suscriptores a los que se les dará el servicio del presente proyecto será de sesenta y ocho viviendas, específicamente en este proyecto, los cuales están distribuidos alrededor de la estación base o centro de gestión. Esta cantidad puede ser expandida, en el caso de un aumento de la población, hasta un máximo de 512 suscriptores, capacidad máxima estimada por los equipos utilizados.

En función del radio de cobertura de los mismos, el cual puede alcanzar hasta un máximo de cincuenta y cuatro kilómetros, queda la disponibilidad de enlazar otros suscriptores que no necesariamente estén dentro de esta urbanización.

El diseño de la red prevé que sea escalable, es decir, que se adapte con facilidad a nuevas tecnologías en lo que a sistemas de alarmas se refiere, con la única condición de que la misma se debe gestionar mediante el protocolo Contac ID.

En lo referente a la telefonía IP que el proyecto ofrece para la comunicación entre los equipos suscriptores no tiene tarifación, ya que es una red de telefonía privada propia de nuestro sistema de seguridad que no tiene interconexión con la red de telefonía publica.

La operación de los equipos de radio se encuentra en una frecuencia radioeléctrica de los 5 GHz, banda que se encuentra prácticamente libre sin necesidad de uso de licencia, la cual nos garantiza la fiabilidad e inviolabilidad en la comunicación inalámbrica, mediante las mejoradas técnicas de seguridad que estos equipos nos otorgan sobre los equipos operan en la banda de 2.4 GHz o Wi-Fi que aunque son mas comercializados en nuestro medio no son capaces de otorgarnos las cualidades anteriormente denotadas.

La aplicación de la tecnología IP se la ha realizado basándose en los protocolos y normas de comunicación, interactuando con el lenguaje de los sistemas de seguridad, creando una plataforma capaz de recibir y poner en funcionamiento tecnologías y aplicaciones a futuro tales como sistemas de

Internet por el cual se verán muy beneficiados todos los usuarios.

En el momento de la aplicación del proyecto se darán los beneficios de seguridad a cada vivienda con dispositivos y paneles de control que emitirán las señales de alarma al centro de gestión, además de una red privada de telefonía IP basado en la red inalámbrica,

Los equipos utilizados son de marcas reconocidas, que se acogen a protocolos y normas bajo las cuales se ha desarrollado el proyecto.

La capacidad de crecimiento de este sistema de seguridad basado en tecnología IP sobre una plataforma inalámbrica tiene un crecimiento modular, permitiendo el crecimiento de la ciudadela con el mismo servicio de seguridad a las viviendas.

Si bien los costos se ven elevados, esto se debe a que la tecnología utilizada para el proyecto es una tecnología de última generación, que nos otorga capacidades que otras no nos las pueden otorgar, por otro lado creemos de que ningún precio es alto siempre y cuando nos de la garantía de que nuestro bienes y nuestras vidas sobre todo estén bajo una total y absoluta “seguridad”, sobre todo, en estos días, en los que la inseguridad, es el común denominador de todo titular de prensa.

Los cálculos nos demostraron que el proyecto es viable, ya que se tiene un ahorro del 87 % con respecto a un sistema convencional óptimo, es decir, en vez de pagar $ 235 mensuales con ese sistema se pagaría $ 31.5, claro esta luego del año de haber pagado los equipos.

Además se concluyó que el ahorro en el tiempo de la vida útil de los equipos por copropietario es de $21.978 y por el conjunto en general es de $1´494.504, esto es en base a los 9 años restantes de vida útil, ya que el primer año es para el financiamiento.

Por lo tanto, se hace necesario de que se den las facilidades para que proyectos innovadores con tecnología aplicada a la seguridad del bien publico y personal, se exijan en las empresas que en estos momentos otorgan servicios de seguridad física, los que en muchas ocasiones no cumplen con los mínimos principios para lo que fueron creadas, dando como resultado una ciudadanía totalmente desprotegida y victima del hampa organizada.

APENDICE

ESPECIFICACIONES TÉCNICAS

A. PANEL DE CONTROL

Particionamiento Avanzado:

- ☞ Hasta 3 particiones independientes
- ☞ Partición No. 3 puede ser área común
- ☞ Usuarios pueden ser asignados a cualquier combinación de particiones

Memoria de Eventos:

- ☞ 250 eventos de memoria visualizables a través del COMPASS Downloader o po teclado alfanuméricos

Código de Instalador Separado:

- ☞ VISTA-48 tiene código de instalador separado para fácil servicio

Monitor Incorporado de Falla en Línea Telefónica:

- ☞ El monitor de falla de VISTA-48 puede advertir sobre problemas con la línea de comunicaciones del sistema de seguridad

Agendas:

- ☞ Hasta 32 agendas, 8 definidas por el instalador y 24 definidas por el usuario
- ☞ Códigos de usuario pueden ser asignados a de uno a ocho grupos, cada grupo posee su propia ventana de tiempo y días de la semana dentro de los cuales los códigos de usuario son funcionales
- ☞ La agenda de operación puede controlar el horario y días de los reportes de prueba

- La agenda de transmisión puede controlar el horario y días de los reportes de pruebas
- Cada partición tiene su propia agenda para autoarmado/desarmado pueden tener la opción de ser repetitivas o no repetitivas (agendas temporales)
- Todas las agendas, de usuario, salidas y autoarmado/desarmado pueden tener la opción de ser repetitivas o no repetitivas (agendas temporales)

Facilidad para Usuario Final:

El VISTA-48 soporta dispositivos inalámbricos particulares que simplifican la vida al cliente. Disponible en 315MHz (Serie AP), 345 MHz (Serie EU) y 868 MHz (Serie H).

Estas emocionantes interfaces para usuarios final eliminan la complejidad en el armado y desarmado, así como la necesidad de retardos de entrada / salida [Excepto 5804]

Conveniencia y controles:

El VISTA-48 puede controlar hasta 16 diferentes dispositivos dentro de un hogar o sitio de negocios.

Estos dispositivos pueden ser activados por:

- Dispositivos inalámbricos
- Teclados inalámbricos
- Eventos del sistema (Modo armado, desarmado, alarmas, etc.)
- Agendas de tiempo

Los Mejores Inalámbricos:

La serie 5800 tiene un rango en exteriores de hasta 1 Km. La serie 5800 H tiene un rango en exteriores de hasta 0.5Km. Los sistemas híbridos de Ademco (combinación de alámbricos/inalámbricos) han sido reconocidos como una herramienta eficaz.

Eléctrico:

- La serie 5Potencia Auxiliar 12VDC, 600 mA máx.
- Soporta batería de hasta 7AH
- Transformador 16.5 VAC / 40 VA
- Salida de Alarma 12 VDC, 2.0 A máx.

Salida de Control:

- 16 salidas programables soportadas
- Soporta 2 salidas programables incorporadas de voltaje
- Soporta hasta 4 tarjetas de relevos (parte n. 4204) con 4 relevos por tarjeta o menos si los relevos del teclado 6164 son usados
- Transformador/Interfase Opcional X-10 (n. de parte 4300 para 60 Hz/110VAC o XM10E/XF-10 para 50Hz/230VAC) puede ser usada para controlar hasta 15 dispositivos de recepción X-10

Zonas (8 zonas alámbricas):

- Método seleccionable de cableado: NC. NA, RFL supervisada, doble balanceada, zona doblada
- Respuesta seleccionable: 10 mseg., 400msec., 700msec., 1.2 sec.
- Asignable a cualquier partición
- 23 tipos de zona para escoger, 4 de los cuales son personalizados y configurables por el instalador
- Supresión programable de sensor Intermitente

Dispositivos Soportados:

1. Receptores Inalámbricos:

Serie 5800

- 5882AP, 5881ENx, 5883, 5882EU & 5882EUH hasta 40 zonas
- 60mA
- 6128RF-SP, 6128RF-ESP hasta 16 zonas & 6128RFH-ESP hasta 40 zonas (Español) 85mA

- 6128RF-IT hasta 16 zonas y 6128RFH-IT hasta 40 zonas (Italiano) - 85mA
- 6128RF, 6150RF hasta 16 zonas & 6128RFH-UK hasta 40 zonas (Inglés)-85 mA

Dispositivos Inalámbricos Soportados

- 5839, 5839EU & 5839H Teclados alfanuméricos inalámbricos de 2 vías
- Llaveros inalámbricos 5804AP, 5804, 5804BD, 5804BDV, 5804EU y 5804H
- Diversidad de recepción con dos antenas
- Montaje remoto para mejor recepción (o local dentro del control)
- Supervisión individual, detección de interferencia en RF e indicación de batería baja

Dispositivos de Expansión Alámbricos

- 4219 - 8 zonas alámbricas - 16mA
- 4204 hasta 4 relevos - 15mA (Cada relevo activo consume 40mA)
- 4229 - 8 zonas alámbricas y 2 relevos - 36mA

Soporte dispositivos portadores de línea

- 4300 Transformador/interfase: 60hZ, 110VAC
- XF-10 transformador/interfase: 50Hz, 230VAC
- XM10E interfase: 50Hz, 230VAC

Teclados

- 6164 lenguaje personalizado (requerido para programación) - 100mA
- Serie 6148, LCD de palabras fijas - 25mA

Soporta detectores de humo de dos hilos

- Hasta 16 detectores de zona en uno

Dispositivos de Interruptor de llave

- 4146 interruptor de llave, uno por partición

2. Transmisores

Familia 5800

- Baterías de 3 voltios Duracell Litio
- 5800/5800AP-1 Km. rango, serie EU hasta 300 mts, serie H hasta 0.5km

- Modo de Aprendizaje
- Tamper de protección contra retiro de cubierta o de muro Standard en serie EU/H

3. Comunicaciones:

Discado multifrecuencia

Formatos soportados

- ADEMCO Contact ID
- ADEMCO 4 + 2 Express
- Robofon Contact ID
- Robofon 6 + 2
- Formato de seguimiento de indicación audible

Capacidades de reporte

- Dividido
- Doble
- Dividido / Doble

Reporte Expandido

Reporte Hexadecimal soportado

Códigos de hasta 6 dígitos PABX soportados y hasta 20 dígitos en números de telecomunicación

Toma de línea de doble polo

Reportes de batería Baja 11.2-11.6 VDC

Soporte de reporte por pérdida y restauración de AC

Verificación de Audio de Alarma (Voz en dos vías)

- Soporta Ademco UVS y AVS-EU

Consejos Importantes de Instalación:

• Este sistema utiliza consolas direccionables y /o Módulos Expansores de Zonas (ver tabla de direcciones en la sección Información General de Programación).

• Las consolas deben configurarse para direcciones entre 16-23 (la primera consola tendrá la dirección 16, lo que es diferente de otros paneles de control mas antiguos) y programarse en los campos de datos *190-*196.
• Los Módulos Expansores de Zona deben configurarse para direcciones específicas (07-11), basándose en los números zonas utilizados (ver tabla de direcciones en la sección Zonas de Expansión 4219/4229).
• Los Módulos de Relés 4204 deben configurarse para direcciones específicas (12-15; ver sección Conexión de Módulos de Relés).
• Las Consolas 6164 deben configurarse para dos direcciones: una dirección de teclado y una dirección de módulo expansor de zonas (si quiere utilizar las zonas de expansión de la consola).
• Esta unidad de control no se encenderá si no tiene la alimentación C.A. conectada (no se encenderá sólo con la batería). Sin embargo, una vez se ha encendido el sistema, funcionará con la alimentación de la batería en caso de pérdida de red C.A.
• Los relés tienen dos modos de menús de programación: Utilice el Modo Menú *79 para trazar las direcciones de los módulos y los números de los dispositivos (salidas). Use el Modo Menú *80 para definir las funciones de las salidas (ver sección Programación de Equipos de Salida).
• Este sistema soporta teclas de función programables. Use el Modo Menú *57 para definir las teclas de función (ver sección de Programación de Teclas de Función).
• Este sistema proporciona varias prestaciones de localización. Ver sección de Información General de Programación para un resumen de la programación del Localizador (Busca).

Códigos de Informe para Estado del Sistema:

Los códigos de informe de zona se programan utilizando los modos interactivos 56 o 58 de Programación de Zonas, mientras que los códigos de estado del sistema (no alarma) y los códigos de restablecimiento se introducen en los siguientes campos de datos. Los dígitos de códigos de informes actuales que introduzca dependen de la

instalación en particular, y deberían estar de acuerdo con la Central Receptora que recibe las señales.

Para inhabilitar un código de informe, introduzca “0” en el primer dígito.

Formato 3+1, 4+1 Standard o Robofon 8: Introduzca un código para el primer dígito: 1–9, A, B, C, D, E, o F.

Introduzca #+10 para A (esto transmite un “0” en algunos receptores), #+11 para B, #+12 para C, #+13 para D, #+14 para E, #+15 para F.

Si introduce 0 en la segunda casilla el sistema avanzará hasta el siguiente campo.

Formato Expandido o 4+2: Introduzca códigos para ambos dígitos (primer y segundo dígitos) para 1–9 o A–F, como se describe en el paso anterior. Si introduce “0” como Segundo dígito se elimina el mensaje expandido para ese informe.

Informes ADEMCO o Robofon Contact ID®: Introduzca un dígito en la primera casilla para habilitar que la zona transmita informes. Utilice un dígito diferente para cada zona hasta que haya utilizado todos los dígitos disponibles. Si el número de zonas excede el número de dígitos disponibles, empiece con el dígito 1 otra vez. Este es solo un dato para “habilitar” códigos y no es el código enviado a la Central Receptora. Los datos introducidos en la segunda casilla son ignorados. Si introduce 0 en la primera casilla se inhabilita el informe.

CAMPO	TITULO y DATOS A INTRODUCIR	EXPLICACIÓN
*59	**Código Informe Error Salida** 0 = ningún informe 1-F = código informe; ver descripción anterior	Después de conectar el sistema, las zonas que permanecen abiertas una vez terminado el tiempo de salida generan un sonido de alarma en la consola y sirena auxiliar (en la consola también se mostrará el mensaje "ALARMA SALIDA", y comenzará el tiempo de entrada. Si desconecta el sistema antes de que termine el tiempo de entrada silenciará la alarma y no se enviará ningún mensaje a la CRA. La consola mostrará "CA" (consola numérica) o "ALARMA CANCELADA" (alfanumérica). Si no se desconecta el sistema antes de que termine el tiempo de entrada, se enviará un mensaje "ALARMA SALIDA" a la Central Receptora si la opción de Código Informe Error Salida está habilitada. La consola mostrará el mensaje "EA" (numérica) "ALARMA SALIDA" (alfanumérica), y el sonido de alarma continuará hasta que se desconecte el sistema (o hasta el final del tiempo sirena). Una condición de Alarma Salida también resultará si tiene lugar un fallo en una zona de salida o interior dentro de los 2 minutos siguientes al final del tiempo de salida, y se enviará un mensaje "ALARMA SALIDA" a la Central Receptora. Con el formato Contact ID, el mensaje incluirá el número de zona y el código de error 374 ("ERROR ALARMA–SALIDA").
*60	**Código Informe Avería** 0 = No; 1-F = ver descripción antes de *59	Enviado si una zona está en condición de avería.
*61	**Código Informe Anulación** 0 = No; 1-F = ver descripción antes de *59	Enviado cuando se anula una zona manualmente o se anula automáticamente al final del tiempo salida.
*62	**Código Informe Pérdida C.A.** 0 = No; 1-F = ver descripción antes de *59	El envío de este informe es aleatorio con un retardo de hasta 1 hora. Si la red C. A. se restablece antes de que se envíe el informe, no se enviará ningún informe de "RESTABL. C.A.".
*63	**Código Informe Baja Batería** 0 = No; 1-F = ver descripción antes de *59	Enviado cuando existe una condición de baja batería del sistema.
*64	**Código Informe Prueba (Test)** 0 = No; 1-F = ver descripción antes de *59	Enviado periódicamente para comprobar que el comunicador y las líneas telefónicas están funcionando. La frecuencia del informe se programa en el modo Calendarios (evento 11).
*65	**Código Informe Desconexión** 0 = No; 1-F = ver descripción antes de *59	Enviado cuando se desconecta el sistema en las particiones seleccionadas.
*66	**Código Informe Conexión Total/Parcial** 0 = No; 1-F = ver descripción antes de *59	Esta opción permite una programación independiente para los informes Total y parcial de cada partición. NOTA: Los informes de "DESCONEXIÓN" (APERTURA) no se envían si el informe de CONEXIÓN (CIERRE) asociado no está habilitado.
*67	**Cód. Informe B.Batería Transmisores RF** 0 = No; 1-F = ver descripción antes de *59	Enviado cuando existe una condición de baja batería de un transmisor vía radio.
*68	**Código Informe de Cancelación** 0 = No; 1-F = ver descripción antes de *59	Enviado al desconectar el sistema después de que se haya reportado una condición de alarma.

CAMPO	TITULO y DATOS A INTRODUCIR	EXPLICACIÓN
*59	**Código Informe Error Salida** 0 = ningún informe 1-F = código informe; ver descripción anterior	Después de conectar el sistema, las zonas que permanecen abiertas una vez terminado el tiempo de salida generan un sonido de alarma en la consola y sirena auxiliar (en la consola también se mostrará el mensaje "ALARMA SALIDA", y comenzará el tiempo de entrada. Si desconecta el sistema antes de que termine el tiempo de entrada silenciará la alarma y no se enviará ningún mensaje a la CRA. La consola mostrará "CA" (consola numérica) o "ALARMA CANCELADA" (alfanumérica). Si no se desconecta el sistema antes de que termine el tiempo de entrada, se enviará un mensaje "ALARMA SALIDA" a la Central Receptora si la opción de Código Informe Error Salida está habilitada. La consola mostrará el mensaje "EA" (numérica) "ALARMA SALIDA" (alfanumérica), y el sonido de alarma continuará hasta que se desconecte el sistema (o hasta el final del tiempo sirena). Una condición de Alarma Salida también resultará si tiene lugar un fallo en una zona de salida o interior dentro de los 2 minutos siguientes al final del tiempo de salida, y se enviará un mensaje "ALARMA SALIDA" a la Central Receptora. Con el formato Contact ID, el mensaje incluirá el número de zona y el código de error 374 ("ERROR ALARMA–SALIDA").
*60	**Código Informe Avería** 0 = No; 1-F = ver descripción antes de *59	Enviado si una zona está en condición de avería.
*61	**Código Informe Anulación** 0 = No; 1-F = ver descripción antes de *59	Enviado cuando se anula una zona manualmente o se anula automáticamente al final del tiempo salida.
*62	**Código Informe Pérdida C.A.** 0 = No; 1-F = ver descripción antes de *59	El envío de este informe es aleatorio con un retardo de hasta 1 hora. Si la red C. A. se restablece antes de que se envíe el informe, no se enviará ningún informe de "RESTABL. C.A.".
*63	**Código Informe Baja Batería** 0 = No; 1-F = ver descripción antes de *59	Enviado cuando existe una condición de baja batería del sistema.
*64	**Código Informe Prueba (Test)** 0 = No; 1-F = ver descripción antes de *59	Enviado periódicamente para comprobar que el comunicador y las líneas telefónicas están funcionando. La frecuencia del informe se programa en el modo Calendarios (evento 11).
*65	**Código Informe Desconexión** 0 = No; 1-F = ver descripción antes de *59	Enviado cuando se desconecta el sistema en las particiones seleccionadas.
*66	**Código Informe Conexión Total/Parcial** 0 = No; 1-F = ver descripción antes de *59	Esta opción permite una programación independiente para los informes Total y parcial de cada partición. NOTA: Los informes de "DESCONEXIÓN" (APERTURA) no se envían si el informe de CONEXIÓN (CIERRE) asociado no está habilitado.
*67	**Cód. Informe B.Batería Transmisores RF** 0 = No; 1-F = ver descripción antes de *59	Enviado cuando existe una condición de baja batería de un transmisor vía radio.
*68	**Código Informe de Cancelación** 0 = No; 1-F = ver descripción antes de *59	Enviado al desconectar el sistema después de que se haya reportado una condición de alarma.

***69**	**Códigos Restablecimiento** Enviar código restablecimiento (si se borra fallo): 0 = al final tiempo sirena (si restablecido) o al desconectar (tanto si restablecido como si no) 1 = dinámicamente según se borrén fallos 2 = solo después de desconectar	Se enviará un mensaje de restablecimiento de alarma con la condición seleccionada.
***70**	**Cód. Informe Restablec. Alarma** 0 = no; 1-F = ver descripción antes de *59	Enviado cuando se restablece una zona de alarma a su condición sin fallos o a la hora seleccionada en el campo *69.
***71**	**Cód. Informe Restablec. Avería** 0 = no; 1-F = ver descripción antes de *59	Enviado cuando se restablece la avería de una zona.
***72**	**Cód. Informe Restabl. Anulación** 0 = no; 1-F = ver descripción antes de *59	Enviado cuando una zona anulada se valida o vuelve a incluir en el sistema ya sea manualmente o al desconectar la partición/sistema.
***73**	**Cód. Informe Restablec. C.A.** 0 = no; 1-F = ver descripción antes de *59	Enviado cuando se restablece la alimentación C.A. después de un corte de corriente.
***74**	**Cód. Informe Rest. Baja Batería** 0 = no; 1-F = ver descripción antes de *59	Enviado cuando se restablece a normal una condición de baja batería del sistema.
***75**	**Cod. Informe Rest. Baja Batería RF** 0 = no; 1-F = ver descripción antes de *59	Enviado cuando la condición de baja batería de un transmisor se restablece (es decir., se coloca una nueva pila).
***76**	**Cód. Informe Rest. Prueba (Test)** 0 = no; 1-F = ver descripción antes de *59	Enviado al salir del modo Prueba (Test).

Campos Varios del Sistema

CAMPO	TITULO y DATOS A INTRODUCIR	EXPLICACIÓN
***77**	**Mes de Cambio a Horario Verano** 0 = Inhabilitar 1 = Enero 2 = Febrero 3 = Marzo 4 = Abril # + 10 = Octubre # + 11 = Noviembre # + 12 = Diciembre	Introduzca el mes de inicio y de fin del horario de verano, si aplica a su región.
***78**	**Fin de Semana de Cambio a Horario Verano** 0 = Inhabilitar 1 = primero 2 = segundo 3 = tercero 4 = cuarto 5 = último 6 = penúltimo 7 = antepenúltimo	Introducir el fin de semana de inicio y de fin del horario de verano, si aplica a su región.
***84**	**Conexión Parcial Automática** 0 = no 1 = solo partición 1 2 = solo partición 2 4 = solo partición 3 Añadir valores para múltiples particiones (Ej.:. para particiones 1 y 2, introducir 3).	Si se habilita, el sistema cambiará automáticamente los modos TOTAL o MAXIMO a PARCIAL e INSTANT respectivamente si la puerta de entrada/salida no se abre y cierra dentro del tiempo de salida después de que un usuario conecte en modo TOTAL desde una consola cableada (no un dispositivo RF). Se envía un informe de Desconexión (Apertura) seguido por uno de Conexión Parcial a la CRA. Si se abre y cierra la puerta dentro del periodo de tiempo de salida, el sistema permanece en modo TOTAL o MAXIMO. Cualquier dispositivo RF que conecte el sistema en modo TOTAL anula esta opción y el sistema permanece conectado en el modo TOTAL. NOTA: No debe usar esta opción si está utilizando el TeleCommand. No aplica si: • Opción salida Conexión Contacto final (campo *88, opción 3) habilitada. • Si está utilizando Blockschloss.
***85**	**Temporizador Verificación Zona Cruce** 0 = 15 sg. 1 = 30 sg. 2 = 45 sg. 3 = 60 sg. 4 = 90 sg. 5 = 2 min 6 = 2-1/2 min 7 = 3 min 8 = 4 min 9 = 5 min #+10 = 6 min #+11 = 7 min #+12 = 8 min #+13 = 10 min #+14 = 12 min #+15 = 15 min	Establece el periodo máximo de tiempo en el cual dos zonas cruzadas deben activarse en un sistema conectado para enviar un mensaje de alarma a la Central Receptora. Si solo se activa una zona cruzada durante este tiempo, se envía a la Central Receptora un mensaje de avería (código CID 380) para esa zona. Asignar los pares de zonas cruzadas en la lista de zonas 4.

CAMPO	TITULO y DATOS A INTRODUCIR	EXPLICACIÓN
*86	**Mensaje Cancelación en Pantalla** 0 = no 1 = si	Si está habilitado (1 = si), esta opción genera un mensaje "**ALARMA CANCELADA**" en la pantalla LCD de la consola en las siguientes condiciones: • Después de la señal de despedida del mensaje de cancelación a la Central Receptora, indicando una transmisión correcta. • Si se cancela con éxito una alarma antes de que la Central Receptora reciba el mensaje de alarma. Ej.:, si se activa una alarma por error y el usuario pulsa código + PARO antes de que termine el retardo de comunicación, el mensaje nunca será enviado a la CRA. • Si el informe de cancelación no está habilitado y sistema está desconectado: a. **antes** de que termine el retardo de comunicación (informe de alarma no enviado) se mostrará el mensaje "Alarma Cancelada". b. **después** de que termine el retardo de comunicación no se mostrará el mensaje "Alarma Cancelada".
*87	**Tiempo Retardo Fallo Misceláneo** 0 = 15 sg. 6 = 2-1/2 min #+12 = 8 min 1 = 30 sg. 7 = 3 min #+13 = 10 min 2 = 45 sg. 8 = 4 min #+14 = 12 min 3 = 60 sg. 9 = 5 min #+15 = 15 min 4 = 90 sg. #+10 = 6 min 5 = 2 min #+11 = 7 min	Usado con zonas a las que se les ha asignado un tipo de zona configurable con retardo fallo activado (seleccionado en la pantalla proceso alarma/avería), y establece un tiempo de respuesta de zona de 15 sg. a 15 min. Puede asignarse a zonas con detectores que faciliten una indicación de avería si un tanque de aceite o gas está bajo, o aplicaciones similares para supervisión de condiciones críticas donde se desea una respuesta de no alarma y donde el tiempo de respuesta de zona debería ser muy largo para evitar reaccionar a fallos transitorios normales.
*88	**Opciones Salida** 0 = Todas las zonas de intrusión deben estar intactas antes de conectar el sistema 1 = Todas las zonas intrusión excepto de la ruta de salida (lista zonas12) deben estar intactas antes de conectar el sistema. Entrarán en estado de alarma si no se restablecen al final del tiempo de salida 2 = Todas las zonas de intrusión excepto las de la ruta de salida (lista zonas 12) deben estar intactas antes de conectar el sistema. Se anularán si no se restablecen para el final del tiempo salida 3 = Conexión contacto final: Todas las zonas de intrusión excepto las de ruta de salida (lista zn 12) deben estar intactas antes de conectar el sistema. Una vez conectado, el tiempo de salida continua activo indefinidamente hasta que última zona, según lo definido en la lista zn 8, se restablezca; luego comenzará un tiempo de salida de 5 segundos antes de que el estado de conexión esté activo	Seleccionar la opción deseada. **NOTA:** Debe ser "0" si el sistema utiliza tipo de zona 82 - blockschloss.
*89	**C. Informe Registro Eventos Lleno** 0 = no; 1-F = ver descripción antes de *59	Si se habilita el registro de eventos en el campo *90, se puede enviar un mensaje a la C.R.A. cuando el registro esté lleno al 80%. Una vez lleno el registro, los nuevos mensajes sobrescriben los mas antiguos.
*90	**Habilitar Registro de Eventos** 0 = no 1 = registrar Alarmas/Restabl. Alarmas 2 = registrar Averías/Restabl. Averías 4 = registrar Anulaciones/Rest. Anulación 8 = registrar Desconexión/Conexión x = registrar combinación de eventos (sumar valores de opción)	Este sistema puede registrar hasta 250 eventos en un histórico. El operador del programa bidireccional podrá descargar el registro y verlo o imprimirlo todo o categorías seleccionadas. El operario también podrá borrar el registro. El registro de eventos también se puede visualizar en una consola alfanumérica (ver Manual de Usuario para mas detalles). La visualización/impresión en la central receptora mostrará la fecha, hora, evento, y descripción de lo ocurrido. Ej.: Para seleccionar Alarmas/Rest. Alarmas" y "Desconexión/Conexión", introduzca 9 (1+8); para seleccionar todos los eventos, introduzca #15.
*91	**Opciones Varias** 0 = ninguna 4 = uso de módulo Verificación Audible Alarmas (AAV) 8 = Habilitar reinicio tiempo salida/reset †† Ejemplo múltiples opciones: para poner tanto AAV como reinicio tiempo salida, introducir # + 12 (4 + 8).	Seleccionar las opciones deseadas sumando los valores de cada opción. ††La opción "Reinicio Tiempo Salida/reset" permite el uso de la tecla [*] para reiniciar el tiempo salida en cualquier momento cuando se conecta el sistema PARCIAL o INSTANT. Esta opción también permite restablecer el tiempo salida automáticamente, lo que reinicia el tiempo salida si se vuelve a abrir y cerrar la puerta de entrada/salida antes de que expire el tiempo salida después de una conexión TOTAL o MAXIMA. **IMPORTANTE:** No debería usar el AAV si se envían Informes de Alarma a un busca o a un número secundario a no ser que se utilice la opción de zona supervisada (que pausa las llamadas). En caso contrario, la llamada del comunicador al número secundario después del informe de alarma impedirá que el AAV tome control de la línea telefónica, y la sesión de "Escucha" del AAV no podrá tener lugar.

CAMPO	TITULO y DATOS A INTRODUCIR	EXPLICACIÓN
*92	**Supervisión Línea Telefónica** Dígito 1–Tiempo: 0 = inhabilitado 1-15 = 1 minuto a 15 minutos respectivamente (2 = 2 min, 3 = 3 min, etc.; # + 10 =10 min, # + 11 = 11 min, # + 12 = 12 min, # + 13 = 13 min, # + 14 = 14 min, # + 15 = 15 min) Dígito 2–Pantalla/Opciones acústicas: 0 = mensaje en pantalla consola solo cuando línea tenga fallos. 1 = mensaje en pantalla más sonido avería en consola cuando línea en fallo. Cada partición silencia su propio sonido de avería. Sin límite tiempo automático. 2 = Igual que "1" mas equipo salida programado se ACTIVA. Si cualquiera de las particiones está conectada, se activará la sirena auxiliar. La sirena auxiliar se silenciará al final del tiempo sirena o introduciendo el código de seguridad mas la tecla PARO desde cualquier partición (no tiene por que ser la partición que estaba conectada).	Dígito 1: Establece el periodo de tiempo que debe permanecer el fallo de línea telefónica una vez detectado antes de que la opción del segundo dígito se active. Dígito 2: Selecciona la respuesta deseada al fallo de línea telefónica. La opción 2 puede utilizarse aunque no tenga conectado un modulo de relés o un dispositivo de Portadora de Línea al panel de control. El equipo de salidas programado debe programarse para PARARSE en el campo *80 o PARARSE al introducir [código de seguridad] + [#] + 8 + número equipo. La partición en el campo *80 debe programarse como "0," para PARO.
*93	**Contador de Alarmas** 0 = número de informes ilimitado 1 = 1 par de informes por zona por periodo conexión 2 = 2 pares de informes por zona por periodo de conexión	Esta opción puede utilizarse para limitar el número de mensajes de alarma/restablecimientos de alarma por zona enviados a la central receptora en un periodo de conexión.
*94	**Número de Teléfono del Módem del PC** Introduzca hasta 20 dígitos como sigue: 0–9, # +11 para "*", # + 12 para "#", # + 13 para una pausa.	Introduzca el número de teléfono del módem del PC para la comunicación bidireccional. No rellene espacios no utilizados. Para terminar pulse *. Para borrar los datos introducidos en el campo, pulse *94*.
*95	**Contador de Rings para Bidireccional** 0 = Desactivar bidireccional iniciado desde Central Receptora 1–14 = número de rings antes de que el panel de control conteste la llamada entrante #+15 = uso con contestador automático	Ver siguiente tabla para programar este campo.

Módulo Teléfono	contest. automático	Bidirec-cional	Programar campo *95 como...
si	no	no	1-14 (no 0)
si	si	no	mas alto que el número de rings programado en contestador/fax (Ej.:, si el contestador/fax está a 4 rings, programar este campo a 5). Esto permite acceso a través del modulo de teléfono si el equipo contestador/fax está apagado.
si	no	si	1-14 (no 0)
si	si	si	15 (para superar el contestador automático/fax†)
no	no	no	0
no	si	no	0
no	no	si	1-14
no	si	si	15

† NOTA: Si introduce "15" para superar un contestador automático y está utilizando un Módulo TeleCommand en el sistema, por favor observe lo siguiente:

Al llamar desde un teléfono fuera del local protegido, el usuario debería realizar la llamada inicial, permita sólo 1 o 2 rings, y a continuación cuelgue, y vuelva a realizar la llamada otra vez. El modulo telefónico capturará ahora la línea, y sonarán dos tonos largos 2, seguidos por el mensaje de voz usual para el código de acceso. Si no sigue este procedimiento, la operación del módulo telefónico no será posible.

Campos de Programación del Busca (Pager)

CAMPO	TITULO y DATOS A INTRODUCIR	EXPLICACIÓN
*160	**Número Teléfono Busca 1(Pager)** Introduzca hasta 20 dígitos	Si introduce menos de 20 dígitos, salir pulsando [*] y el siguiente número de campo. Para borrar los datos de este campo, pulsar *160*.
*161	**Caracteres Busca 1 (Pager)** Introduzca hasta 16 caracteres	Pueden enviarse hasta 16 caracteres opcionales como prefijo del código de estado del sistema de 7 dígitos enviados al busca 1 (si se utiliza). El número de teléfono en el campo *160 debe estar programado. Si introduce menos de 16 caracteres, salir pulsando [*] y el siguiente número de campo. Para borrar los datos de este campo, pulsar *161*. Por ejemplo, use estos 16 caracteres opcionales para lo siguiente: • Número PIN (para identificar el busca específico con la compañía del servicio de busca) • Número de abonado • * (introducir # + 11 para enviar *) • # (introducir # + 12 para enviar #) • Pausa (introducir # + 13 para una pausa de 2 segundos)* • Cualquier carácter(es) que el usuario final decida transmitir * Algunos sistemas de localización (busca) requieren una pausa(s) antes del prefijo. El formato para el código de estado del sistema de 7 dígitos se define como sigue: Formato Busca: XXX-YYYY donde: XXX = código evento 3 dígitos: 911 = Alarma 811 = Avería 101 = Apertura (desconexión) 102 = Cierre (conexión) YYYY= usuario o nº zona de 4 dígitos (dependiendo del tipo de evento). El primer dígito indica la partición, seguido por 0, y el usuario o zona de 2 dígitos. *Ejemplo 1.* El busca muestra: 9 1 1 – 1 0 0 4 Esto indica que el sistema está reportando una alarma (911) causada por un fallo en la zona 4 en la partición 1. *Ejemplo 2.* El busca muestra: 1 0 2 – 2 0 0 5 Esto indica que el sistema está reportando un cierre–conexión del sistema (102) por el usuario 5 en la partición 2.
*162	**Opciones Informe Busca 1** 0 = No enviar informes 1 = D/C todos los usuarios con opción busca 4 = Todas las alarmas y averías 5 = Todas las alarmas, averías, Desconex. /Conexión todos los usuarios con busca 12 = Alarmas y averías para zonas de la lista de zonas 9 13 = Alarmas y averías para las zonas en lista de zonas 9 y D/C para todos los usuarios con opción busca	Introducir los tipos de informe a ser enviados al busca 1 por cada partición. † Transmite informe a busca solo cuando la conexión(cierre)/ desconexión (apertura) se realiza desde una consola utilizando un código de seguridad; las conexiones/desconexiones automáticas, conexiones con pulsador RF asignado, y conexión mediante llave no envían mensajes al busca.
*163	**Número Teléfono Busca 2 (Pager)** Introduzca hasta 20 dígitos	Si introduce menos de 20 dígitos, salir pulsando [*] y el siguiente número de campo. Para borrar los datos de este campo, pulsar *163*.
*164	**Caracteres Busca 2 (Pager)** Introduzca hasta 16 caracteres	Ver campo *161. Si introduce menos de 16 caracteres, salir pulsando [*] y el siguiente número de campo. Para borrar datos introducidos, pulsar *164*.
*165	**Opciones Informe Busca 2** Ver informes busca 1, campo *162 para valores, excepto usar lista zonas 10.	Introducir los tipos de informe a ser enviados al busca 2 por cada partición.
*166	**Número Teléfono Busca 3 (Pager)** Introduzca hasta 20 dígitos	Si introduce menos de 20 dígitos, salir pulsando [*] y el siguiente número de campo. Para borrar los datos de este campo, pulsar *166*.
*167	**Caracteres Busca 3** Introduzca hasta 16 caracteres	Ver campo *161. Si introduce menos de 16 caracteres, salir pulsando [*] y el siguiente número de campo. Para borrar datos introducidos, pulsar *167*.
*168	**Opciones Informe Busca 3** Ver informes busca 1, campo *162 para valores, excepto usar lista zonas 11.	Introducir los tipos de informe a ser enviados al busca 3 por cada partición.
*169	**Retardo del Busca para Alarmas** 0 = ninguno 2 = 2 minutos 1 = 1 minuto 3 = 3 minutos	Este campo determina el retardo de los informes de alarma enviados al busca. Esto le da tiempo suficiente a la Central Receptora para verificar el informe de alarma que ha recibido, antes de que el comunicador intente llamar al busca. NOTA: El retardo no se reinicia para nuevas alarmas que ocurran durante retardo de una alarma en curso de un busca. Este retardo es para TODOS los buscas del sistema.

Campos Varios del Sistema

*173 OPCIONES INFORMES RF

0 = ninguno
1 = Informes Tamper RF durante desconexión
2 = Llaves RF transmiten baja batería
3 = Informes Tamper RF durante desconexión y Llaves RF transmiten baja batería

Seleccionar opción deseada.

*175 Opciones Antisabotaje (Tamper)

Dígito 1: 0 = protección tamper estándar
1 = detectar tamper de zonas anuladas
2 = detectar tamper en modo Prueba (Test)
3 = detectar tamper en modo Test y de zonas anuladas
Dígito 2: 0 = todos los usuarios pueden borrar un tamper**
1 = solo el instalador puede borrar un tamper

Seleccionar opciones deseadas.

Detección Antisabotaje (Tamper) Estándar (dígito 1 opción0): El sistema normalmente detecta los fallos de tamper de dispositivos equipados con interruptores tamper (para retirada de tapa y/o de pared) mientras el sistema está conectado o desconectado. Los fallos Tamper se ignoran cuando se anula una zona o cuando el sistema está en modo Prueba a no ser que estén seleccionadas en el dígito 1 las opciones 1, 2, o 3. El mensaje de tamper es el siguiente:

Desconectado: TAMPER 1xx (o zz)
donde 1xx = dirección equipo ECP
zz = número zona o equipo en fallo.
Conectado: ALRM_TMPR

** Debe ser "0" si campo *25 dígito 2 programado como 1 o 2, sino, solo el instalador podrá desconectar el sistema y borrar los mensajes tamper.

*176 Opciones Sirena

Dígito 1: 0 = sirena externa
1 = sirena externa invertida
2 = sirena interior
3 = sirena interior invertida
Dígito 2: 0 = inhabilitar
1 = habilitar retardo 30 sg. de sirena y comunicador durante tiempo entrada

Seleccionar las opciones deseadas.

Dígito 1: si el dígito 1 no está programado para una sirena externa (opción 0 ó 1), entonces el segundo dígito será ignorado.

Dígito 2, si está habilitado: Si el tiempo de entrada está activo y se activa una zona instantánea, se retarda la sirena 30 segundos y también el informe se retarda 30 sg, siempre que en el campo *50 no se haya programado un retardo mayor (el retardo de comunicación de 30 segundos sustituye cualquier valor inferior a 30 segundos que esté programado ene el campo *50).

*177 Duración Dispositivos 1, 2

0 = 15 sg	6 = 2-1/2 min	#+12 = 8 min
1 = 30 sg	7 = 3 min	#+13 = 10 min
2 = 45 sg	8 = 4 min	#+14 = 12 min
3 = 60 sg	9 = 5 min	#+15 = 15 min
4 = 90 sg	#+10 = 6 min	
5 = 2 min	#+11 = 7 min	

Estos valores establecen la duración de las acciones de salida opciones 5 (duración 1) y 6 (duración 2) programados en *80 Programación de Funciones Salida.

*178 Supervisión RF / Jam RF

0 = Informes Supervisión RF y Jam RF
1 = Transmitir fallos supervisión RF como alarmas tamper si sistema conectado
2 = Transmitir Jam RF como alarma tamper si sistema conectado
3 = Transmitir Jam RF y Fallo Supervisión RF como alarma tamper si sistema conectado**

Seleccionar la opción deseada. Ver campo *22 para opciones relacionadas.

Dígito 0: Las condiciones de Jam RF se transmiten como Avería zona 90 (Contact ID código 344, Detección Jam Receptor RF) mas un informe de avería zona por cada zona RF en el sistema (código CID 383, Sabotaje en Sensor) cuando el sistema está conectado o desconectado. Las consolas muestran Tamper zz (zz = zonas) y Tamper 90 (numéricas) o JAM RECEPTOR (alfanuméricas).
Los fallos de supervisión RF se transmiten como averías de zona (código CID 381, RF Pérdida Superv.) cuando el sistema está conectado o desconectado. Las consolas muestran COMPROBAR zz (zz = zona).

Dígito 1: Igual que Dígito 0 excepto que los fallos supervisión RF se transmiten como alarmas zona (código CID 144, Sabotaje en Sensor) si sistema conectado; consolas muestran ALARMA zz

Dígito 2: Igual que Dígito 0 excepto que las condiciones Jam RF se transmiten como alarmas zona (código CID 144, Sabotaje en Sensor) si el sistema está conectado; consolas muestran ALARM zz.

Dígito 3: Igual que Dígito 0 si desconectado, pero si el sistema está conectado, tanto condición Jam RF como fallos supervisión RF se transmiten como alarmas zona (Código Contact ID 144, Sabotaje en Sensor)

NOTAS: Debe habilitar la detección Jam RF en el campo *22 para poder habilitar la transmisión de cualquier informe RF en este campo. Debe habilitar los informes de restablecimiento de alarma (campo *70) para que se transmitan los restablecimientos de alarma de Supervisión RF/ Jam RF. Debe habilitar los informes de avería y restablecimiento avería (campos *60, *71) para que se transmitan las condiciones de avería de Supervisión RF/Jam RF y los restablecimientos.

** Debe ser "3" para cumplir Norma prEN50131-5-3 Clase 2

CAMPO	TITULO y DATOS A INTRODUCIR	EXPLICACION
*180	**Limitar Anulación de Zonas** 0 = número de anulaciones de zona ilimitado en cada partición 1-7 = número de anulaciones de zona permitido en cada partición	Seleccionar el número máximo de zonas que pueden ser anuladas. Cada partición utiliza este dato individualmente.
*181	**Frecuencia C.A. 50/60 Hercios** 0 = 60Hz, usar cristal como respaldo 1 = 50Hz, usar cristal como respaldo 2 = Sincronización por cristal, proporcionar 60Hz para X10 3 = Sincronización por cristal, proporcionar 50Hz para X10	Seleccionar el método de sincronización del reloj de cristal interno utilizado por el panel de control.
*182	**Día Cambio Horario Verano** 0 = activar el Domingo por la mañana 1= activar el Sábado por la mañana 2 = activar el Viernes por la mañana	Seleccionar el día de cambio apropiado a horario de verano.
*183	**Formato Fecha/Hora** 0 = 12 horas/MMDDAA 1 = 12 horas/DDMMAA 2 = 24 horas/MMDDAA 3 = 24 horas/DDMMAA	Seleccionar el formato de fecha y hora deseado.
*185	**Opciones de Permisos Bidireccional** 0 = todo permitido 1 = no permitir visualizar códigos de usuario 2 = no permitir comandos ni descarga programa si sistema conectado 3 = no permitir visualización de códigos usuario, ni comandos, ni descarga programa si sistema conectado*	Seleccionar las opciones deseadas. *Debe ser "3" para cumplir norma EN50131-1/prEN50131-3
*186	**Opciones de Pantalla** Dígito 1: Bloquear primera alarma en pantalla 0 = no; 1 = si Dígito 2: Pantalla en blanco (excepto Pérdida C.A) excepto durante tiempo salida, o 30 sg después de desconexión 0 = no; 1 = si	Seleccionar la opción deseada para los mensajes en la pantalla de la consola. Dígito 1: Si se habilita, solo se mostrará la primera zona que entra en alarma. Pulsar tecla LISTO para avanzar una posición por el resto de las zonas que han entrado en alarma, a continuación se volverá a mostrar la primera zona en alarma. NOTA: Debe ser "11" para cumplir la norma EN50131-1/prEN50131-3
*187	**Repetir Zumbador en Salida Aux. 1 (Trigger)** 0 = no; 1 = si	Habilitar esta opción si quiere que un dispositivo externo conectado a la salida de voltaje 1 (trigger) repita los sonidos del zumbador de la consola NOTA: Si utiliza esta opción, el trigger 1 deberá estar dedicado sólo a esta función; no asigne ninguna otra función a la salida de voltaje 1.
*188	**Opciones Antisabotaje Consola** Dígito 1: Bloqueo consola: 0 = no; 1 = si, bloqueo de 15 minutos Dígito 2: Supervisión y Detección Fallo Tamper Consola: 0 = no, 1 = si	Dígito 1. Si se habilita, el sistema bloqueará la consola durante 15 minutos si se pulsan 30 teclas (6 intentos de código + comando) sin que se detecte un código de usuario válido. Mientras el teclado está bloqueado, se mostrará un mensaje "Sabotaje Código" en las pantallas de las consolas ubicadas en la partición que está bloqueada. Se transmitirá un mensaje a la Central Receptora (461 Código Incorrecto), y además se incluirá en el registro de eventos. Dígito 2. Habilita o inhabilita la supervisión de consola (direcciones ECP 16-23) en el panel de control. Si se habilita, la conexión y tamper de las consolas será supervisado por el sistema. Estas condiciones generarán una avería si el sistema está desconectado, y una alarma si está conectado. NOTA: Debe ser "11" para cumplir la normativa EN50131-1/prEN50131-3

Campos de Programación de Consolas

NOTA: Debe asignar a cada consola una dirección única. Los resultados serán imprevisibles si dos o mas consolas tienen la misma dirección.

CAMPO	TITULO y DATOS A INTRODUCIR	EXPLICACIÓN
*190	Consola 2 Dirección 17 Dígito 1 – Asignación de Partición: 0 = consola inhabilitada 2 = partición 2 1 = partición 1 3 = partición 3 Dígito 2 – Opciones Acústicas: 0 = sin supresión 1 = suprimir pitidos conex./desconex. y E/S 2 = suprimir solo pitidos modo aviso 3 = suprimir pitidos conexión/desconexión, E/S y modo aviso	Consola 2 Dígito 1: introducir la partición en la que está ubicada la consola Dígito 2: Introducir las opciones acústicas deseadas para esta consola. NOTA: La dirección 16 está reservada para la consola 1, que está programada de fábrica en la partición 1 con todos los sonidos habilitados.
*191	Consola 3 Dirección 18 Ver campo *190 para opciones.	Consola 3 Ver explicación en campo *190.
*192	Consola 4 Dirección 19 Ver campo *190 para opciones.	Consola 4 Ver explicación en campo *190.
*193	Consola 5 Dirección 20 Ver campo *190 para opciones.	Consola 5 Ver explicación en campo *190.
*194	Consola 6 Dirección 21 Ver campo *190 para opciones.	Consola 6 Ver explicación en campo *190.
*195	Consola 7 Dirección 22 Ver campo *190 para opciones.	Consola 7 Ver explicación en campo *190.
*196	Consola 8 Dirección 23 Ver campo *190 para opciones.	Consola 8 Ver explicación en campo *190.
*197	Intervalo Mensaje Tiempo Salida 0 = sin mensaje en pantalla 1-5 = segundos entre refrescos pantalla	Si se habilita, las consolas mostrarán el tiempo de salida restante después de conectar el sistema, refrescando el mensaje en el intervalo seleccionado (es decir, si el tiempo de salida es de 30 segundos y selecciona "2" en este campo, la pantalla de la consola se refrescará cada 2 segundos, mostrando 30, 28, 26, 24, etc.). Para consolas mas antiguas puede ser necesario introducir un intervalo superior a "1" para que los usuarios tengan tiempo de pulsar las teclas entre los refrescos de pantalla.
*198	Mostrar Número de Partición 0 = no 1 = si	Si habilita esta opción, se mostrará el número de partición en la esquina superior izquierda de la pantalla. Esta opción es útil si va a utilizar la opción IR A (GOTO).
*199	Mensaje Fallo ECP 0 = Mensaje 3 dígitos ("1"+dirección equipo) 1 = Mensaje prefijado de 2 dígitos como "91"	Seleccione "0" si va a utilizar consolas alfanuméricas y/o consolas numéricas de mensajes prefijados de 3 dígitos (6148, 6150, 6160, 6164). Los fallos ECP de las consolas y/u otros equipos ECP periféricos se mostrarán como "1" más la dirección del equipo (00-30) del dispositivo causando el fallo (Ej., los fallos en el equipo 07 se mostrarán como "107"). Seleccione "1" si va a utilizar consolas numéricas de mensajes prefijados de 2 dígitos (Ej., algunas consolas de la serie 6128RF). Si se habilita, los fallos ECP de las consolas y/u otros equipos ECP periféricos se mostrarán como "91" en las consolas de 2 dígitos, y como "191" en las de 3 dígitos o Alfanuméricas.

TABLA A.1 Campos de programación de consolas

B. TECLADO DE MANDO

Físicas

- 10.8 cm. x 14.3 cm. x 2.5 cm.

Cableado

- **-** tierra
- **+** 12 V_{CC}
- DO salida de datos al panel de control
- DI entrada de datos desde el panel de control

Consumo

- En reposo -30 mA
- Activada -55 mA

C. DETECTOR DE MOVIMIENTO

- *Físicas*: carcaza blanca de alto impacto (87x62x40 mm).
- *Energía*: 20 mA – 12 V_{AC}
- *Voltaje de operación*: 10 – 14 V_{DC}
- *Relé de alarma*: tipo A 100 mA – 24 V_{DC}
- *Switch tamper*: 24 V, 100 mA
- *Temperatura de operación*: 14^{o}F – 120^{o}F (-10^{o}C a 49^{o}C).
- *Inmunidad a RF*: 20 V/m de 10 – 1000 MHz
- *Inmunidad a luz blanca*: 2.500 lux.
- *Sensibilidad PIR*: seleccionable por jumper alto (H) o bajo (L).
- *Habilitación de LED*: puede ser habilitado/deshabilitado por jumper, para verificar si el dispositivo esta funcionando.
- *Ducto del cableado*: 8x6.5 mm
- *Detección de rango*: 12x12 m, campo de vista PIR (dos campos de vista por apuntador PIR), rango lejano 44^{o}, intermedio 14^{o}, muy bajo 8^{o}, vista baja 4^{o}.

D. DETECTOR DE HUMO

- Tamaño: 8.1 cm. de altura y 13.9 cm. de diámetro
- Rango de temperatura de operación: Otros modelos de 0^o – 49^o C
- Humedad: 10 – 93% RH no condensado
- Velocidad del aire: 3000 pies/m
- Cable 12 – 18 AWG, se recomienda par trenzado
- Especificaciones de la prueba:

  Puerto de prueba

  Tarjeta de prueba

  Módulo de prueba

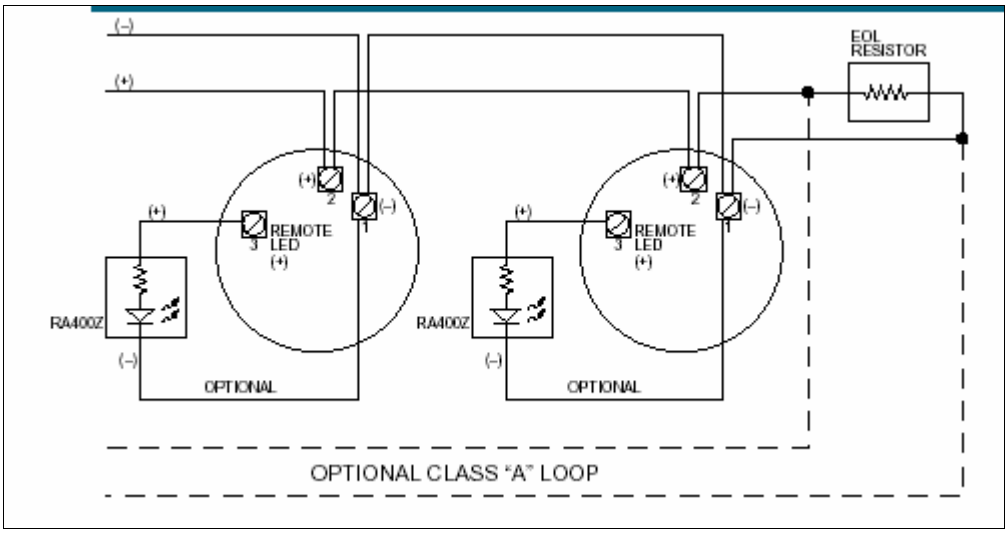


FIG. D.1 Diagrama del cableado del Detector de Humo

E. DETECTOR TÉRMICO

- Corriente típica en espera: 110 – 240 μA
- Corriente máxima de alerta: 50 mA (limitado por el panel de control)
- Humedad máxima: 95% RHN

F. MIP

Tamaño	120x92x30 mm
Potencia	12 Vdc /400 mA
Interfaces de comunicación	Ethernet 10 Mbps, Teléfono
Entradas / Salidas	1 Entrada / 1Salida
Configuración	*Local*: con un teléfono de tonos (DMTF). *Remota*: Carga de la configuración a partir de la receptora
Protocolo del Panel de alarmas	Contact – ID
Encriptación	Código RC4
Seguridad	Llave Protegida
Dirección IP	Pública y Privada (DHCP bajo construcción)
Puertos TCP	Programable
Sondeo de línea	Programable
Protocolo de comunicación	UDP

TABLA F.1 Especificaciones técnicas del MIP

G. SWITCH NO GESTIONABLE

- Método de conmutación: Store and Forward
- RAM buffer asignado dinámicamente para cada puerto
- Autoaprendizaje de la configuración de red
- Control de flujo IEEE 802.3x
- Porcentajes filtro/envío de los paquetes Ethernet: 14,880 pps por puerto
- Porcentajes filtro/envío de los paquetes Fast Ethernet: 148,800 pps por puerto
- Tabla de filtro para direcciones: 1K por dispositivo

- RAM buffer: 1MB por dispositivo

H. CARACTERISTICAS TÉCNICAS DEL EQUIPO DE TRANSMISION INALAMBRICA

Radio MODEM

Frecuencia	5.725 - 5.850 GHz 5.47 - 5.725 GHz
Tecnología para acceso de Radio	OFDM (Orthogonal Frequency Division Multiplexing, múltiplexación por división de frecuencia ortogonal), que es muy robusta frente a la interferencia entre símbolos
Modulación	BPSK, QPSK, 16QAM, 64QAM

TABLA H.1 Características del radio modem

Comunicación de Datos

Estándar	IEEE 802.3 CSMA/CD
VLAN	IEEE 802.1Q
SEGURIDAD	a.-ESSID b.-WEP 128 c.-VLAN acuerdo al estándar IEEE 802.1Q

TABLA H.2 Estándares para la comunicación de datos

Características Eléctricas:

- **Unidad suscriptora**

Potencia Consumida	25 Wmax
Voltaje	85-256 V_{AC}, 47-63 Hz
	$54V_{DC}$

TABLA H.3 Características eléctricas de la unidad suscriptora

- **Estación Base**

Potencia Consumida	**30Wmax**
Voltaje	85-256 V_{AC}, 47-63 Hz
	54 V_{DC}

TABLA H.4 Características eléctricas de la estación base

I. VISOR ALARM

- **Arquitectura Hardware**

PROCESADORES	Motorola MPC860, a 50, 66 u 80 MHz, según versiones
MEMORIA	32, 64 128 ó 256 Mbytes de SDRAM, según versiones
UNIDAD DE ALMACENAMIENTO	Memoria FLASH, 4 , 8 ó 16 Mbytes según versiones: EEPROM 2 Kbytes, NVRAM 128 Kbytes

TABLA I.1 Arquitectura del VisorALARM

- **Interfaz LAN**

PROTOCOLOS	Ethernet (802.3) / Ethernet blue book
VELOCIDAD	10 Mbps (10BaseT)/ 100 Mbps (100BaseT)
CONECTOR	RJ45 hembra

TABLA I.2 Interfaz LAN del VisorALARM

- **Interfaces WAN**

PROTOCOLOS	FRAME RELAY, X.25, PPP, SDLC, X.28
INTERFACES	Drivers insertables V.24 / V.35 / X.21 DTE/ DCE
Nº PUERTAS	3
VELOCIDAD	200 a 2048 Kbps
CONECTOR	DB-25 Hembra

TABLA I.3 Interfaces WAN del VisorALARM

- **Interfaces ISDN**

ACCESO	Básico 2B+D
VELOCIDAD	2 x 64 Kbps (Canales B)
CONECTOR	RJ45 hembra

TABLA I.4 Interfaces ISDN del VisorALARM

- **Interfaz de configuración**

TERMINAL LOCAL	V.24 9.600-8-N-1-sin control de flujo
CONECTOR	DB-9 hembra

TABLA I.5 Interfaz de configuración

- **Alimentación AC**

TENSION DE ENTRADA	100 – 240 V ~
CORRIENTE DE ENTRADA	1-0.5 A
FRECUENCIA DE ENTRADA	47-63 Hz

TABLA I.6 Alimentación AC del VisorALARM

- **Alimentación DC**

TENSION DE ENTRADA	-48 V
CORRIENTE DE ENTRADA	1 A

TABLA I.7 Alimentación DC del VisorALARM

- **Dimensiones y Peso**

TIPO	Caja sobremesa
LARGO x ANCHO x ALTO	310 x 415 x 43 mm
PESO	3,5Kg

TABLA I.8 Dimensiones y peso del VisorALARM

- **Especificaciones Ambientales**

TEMPERATURA AMBIENTE	Encendido: 5º a 55ºC Apagado: -20º a 60ºC
HUMEDAD RELATIVA	Encendido: 8% a 85% Apagado: 5% a 90%

TABLA I.9 Especificaciones ambientales del VisorALARM

J. TABLAS DE FACTORES DE INTERÉS COMPUESTO

0.5%	TABLA 2 Flujo de efectivo discreto: Factores de interés compuesto							0.5%
	Pagos únicos		Pagos de serie uniforme				Gradientes aritméticos	
n	Cantidad compuesta F/P	Valor presente P/F	Factor de amortización A/F	Cantidad compuesta F/A	Recuperación de capital A/P	Valor presente P/A	Gradiente de valor presente P/G	Gradiente de serie anual A/G
1	1.0050	0.9950	1.00000	1.0000	1.00500	0.9950		
2	1.0100	0.9901	0.49875	2.0050	0.50375	1.9851	0.9901	0.4988
3	1.0151	0.9851	0.33167	3.0150	0.33667	2.9702	2.9604	0.9967
4	1.0202	0.9802	0.24813	4.0301	0.25313	3.9505	5.9011	1.4938
5	1.0253	0.9754	0.19801	5.0503	0.20301	4.9259	9.8026	1.9900
6	1.0304	0.9705	0.16460	6.0755	0.16960	5.8964	14.6552	2.4855
7	1.0355	0.9657	0.14073	7.1059	0.14573	6.8621	20.4493	2.9801
8	1.0407	0.9609	0.12283	8.1414	0.12783	7.8230	27.1755	3.4738
9	1.0459	0.9561	0.10891	9.1821	0.11391	8.7791	34.8244	3.9668
10	1.0511	0.9513	0.09777	10.2280	0.10277	9.7304	43.3865	4.4589
11	1.0564	0.9466	0.08866	11.2792	0.09366	10.6770	52.8526	4.9501
12	1.0617	0.9419	0.08107	12.3356	0.08607	11.6189	63.2136	5.4406
13	1.0670	0.9372	0.07464	13.3972	0.07964	12.5562	74.4602	5.9302
14	1.0723	0.9326	0.06914	14.4642	0.07414	13.4887	86.5835	6.4190
15	1.0777	0.9279	0.06436	15.5365	0.06936	14.4166	99.5743	6.9069
16	1.0831	0.9233	0.06019	16.6142	0.06519	15.3399	113.4238	7.3940
17	1.0885	0.9187	0.05651	17.6973	0.06151	16.2586	128.1231	7.8803
18	1.0939	0.9141	0.05323	18.7858	0.05823	17.1728	143.6634	8.3658
19	1.0994	0.9096	0.05030	19.8797	0.05530	18.0824	160.0360	8.8504
20	1.1049	0.9051	0.04767	20.9791	0.05267	18.9874	177.2322	9.3342
21	1.1104	0.9006	0.04528	22.0840	0.05028	19.8880	195.2434	9.8172
22	1.1160	0.8961	0.04311	23.1944	0.04811	20.7841	214.0611	10.2993
23	1.1216	0.8916	0.04113	24.3104	0.04613	21.6757	233.6768	10.7806
24	1.1272	0.8872	0.03932	25.4320	0.04432	22.5629	254.0820	11.2611
25	1.1328	0.8828	0.03765	26.5591	0.04265	23.4456	275.2686	11.7407
26	1.1385	0.8784	0.03611	27.6919	0.04111	24.3240	297.2281	12.2195
27	1.1442	0.8740	0.03469	28.8304	0.03969	25.1980	319.9523	12.6975
28	1.1499	0.8697	0.03336	29.9745	0.03836	26.0677	343.4332	13.1747
29	1.1556	0.8653	0.03213	31.1244	0.03713	26.9330	367.6625	13.6510
30	1.1614	0.8610	0.03098	32.2800	0.03598	27.7941	392.6324	14.1265
36	1.1967	0.8356	0.02542	39.3361	0.03042	32.8710	557.5598	16.9621
40	1.2208	0.8191	0.02265	44.1588	0.02765	36.1722	681.3347	18.8359
48	1.2705	0.7871	0.01849	54.0978	0.02349	42.5803	959.9188	22.5437
50	1.2832	0.7793	0.01765	56.6452	0.02265	44.1428	1035.70	23.4624
52	1.2961	0.7716	0.01689	59.2180	0.02189	45.6897	1 113.82	24.3778
55	1.3156	0.7601	0.01584	63.1258	0.02084	47.9814	1 235.27	25.7447
60	1.3489	0.7414	0.01433	69.7700	0.01933	51.7256	1 448.65	28.0064
72	1.4320	0.6983	0.01157	86.4089	0.01657	60.3395	2 012.35	33.3504
75	1.4536	0.6879	0.01102	90.7265	0.01602	62.4136	2 163.75	34.6679
84	1.5204	0.6577	0.00961	104.0739	0.01461	68.4530	2 640.66	38.5763
90	1.5666	0.6383	0.00883	113.3109	0.01383	72.3313	2 976.08	41.1451
96	1.6141	0.6195	0.00814	122.8285	0.01314	76.0952	3 324.18	43.6845
100	1.6467	0.6073	0.00773	129.3337	0.01273	78.5426	3 562.79	45.3613
108	1.7137	0.5835	0.00701	142.7399	0.01201	83.2934	4 054.37	48.6758
120	1.8194	0.5496	0.00610	163.8793	0.01110	90.0735	4 823.51	53.5508
132	1.9316	0.5177	0.00537	186.3226	0.01037	96.4596	5 624.59	58.3103
144	2.0508	0.4876	0.00476	210.1502	0.00976	102.4747	6 451.31	62.9551
240	3.3102	0.3021	0.00216	462.0409	0.00716	139.5808	13 416	96.1131
360	6.0226	0.1660	0.00100	1 004.52	0.00600	166.7916	21 403	128.3236
480	10.9575	0.0913	0.00050	1 991.49	0.00550	181.7476	27 588	151.7949

TABLA J.1 Tabla al 0,5 %

0.75%	TABLA 3 Flujo de efectivo discreto: Factores de interés compuesto							0.75%
	Pagos únicos		Pagos de serie uniforme				Gradientes aritméticos	
n	Cantidad compuesta F/P	Valor presente P/F	Factor de amortización A/F	Cantidad compuesta F/A	Recuperación de capital A/P	Valor presente P/A	Gradiente de valor presente P/G	Gradiente de serie anual A/G
1	1.0075	0.9926	1.00000	1.0000	1.00750	0.9926		
2	1.0151	0.9852	0.49813	2.0075	0.50563	1.9777	0.9852	0.4981
3	1.0227	0.9778	0.33085	3.0226	0.33835	2.9556	2.9408	0.9950
4	1.0303	0.9706	0.24721	4.0452	0.25471	3.9261	5.8525	1.4907
5	1.0381	0.9633	0.19702	5.0756	0.20452	4.8894	9.7058	1.9851
6	1.0459	0.9562	0.16357	6.1136	0.17107	5.8456	14.4866	2.4782
7	1.0537	0.9490	0.13967	7.1595	0.14717	6.7946	20.1808	2.9701
8	1.0616	0.9420	0.12176	8.2132	0.12926	7.7366	26.7747	3.4608
9	1.0696	0.9350	0.10782	9.2748	0.11532	8.6716	34.2544	3.9502
10	1.0776	0.9280	0.09667	10.3443	0.10417	9.5996	42.6064	4.4384
11	1.0857	0.9211	0.08755	11.4219	0.09505	10.5207	51.8174	4.9253
12	1.0938	0.9142	0.07995	12.5076	0.08745	11.4349	61.8740	5.4110
13	1.1020	0.9074	0.07352	13.6014	0.08102	12.3423	72.7632	5.8954
14	1.1103	0.9007	0.06801	14.7034	0.07551	13.2430	84.4720	6.3786
15	1.1186	0.8940	0.06324	15.8137	0.07074	14.1370	96.9876	6.8606
16	1.1270	0.8873	0.05906	16.9323	0.06656	15.0243	110.2973	7.3413
17	1.1354	0.8807	0.05537	18.0593	0.06287	15.9050	124.3887	7.8207
18	1.1440	0.8742	0.05210	19.1947	0.05960	16.7792	139.2494	8.2989
19	1.1525	0.8676	0.04917	20.3387	0.05667	17.6468	154.8671	8.7759
20	1.1612	0.8612	0.04653	21.4912	0.05403	18.5080	171.2297	9.2516
21	1.1699	0.8548	0.04415	22.6524	0.05165	19.3628	188.3253	9.7261
22	1.1787	0.8484	0.04198	23.8223	0.04948	20.2112	206.1420	10.1994
23	1.1875	0.8421	0.04000	25.0010	0.04750	21.0533	224.6682	10.6714
24	1.1964	0.8358	0.03818	26.1885	0.04568	21.8891	243.8923	11.1422
25	1.2054	0.8296	0.03652	27.3849	0.04402	22.7188	263.8029	11.6117
26	1.2144	0.8234	0.03498	28.5903	0.04248	23.5422	284.3888	12.0800
27	1.2235	0.8173	0.03355	29.8047	0.04105	24.3595	305.6387	12.5470
28	1.2327	0.8112	0.03223	31.0282	0.03973	25.1707	327.5416	13.0128
29	1.2420	0.8052	0.03100	32.2609	0.03850	25.9759	350.0867	13.4774
30	1.2513	0.7992	0.02985	33.5029	0.03735	26.7751	373.2631	13.9407
36	1.3086	0.7641	0.02430	41.1527	0.03180	31.4468	524.9924	16.6946
40	1.3483	0.7416	0.02153	46.4465	0.02903	34.4469	637.4693	18.5058
48	1.4314	0.6986	0.01739	57.5207	0.02489	40.1848	886.8404	22.0691
50	1.4530	0.6883	0.01656	60.3943	0.02406	41.5664	953.8486	22.9476
52	1.4748	0.6780	0.01580	63.3111	0.02330	42.9276	1 022.59	23.8211
55	1.5083	0.6630	0.01476	67.7688	0.02226	44.9316	1 128.79	25.1223
60	1.5657	0.6387	0.01326	75.4241	0.02076	48.1734	1 313.52	27.2665
72	1.7126	0.5839	0.01053	95.0070	0.01803	55.4768	1 791.25	32.2882
75	1.7514	0.5710	0.00998	100.1833	0.01748	57.2027	1 917.22	33.5163
84	1.8732	0.5338	0.00859	116.4269	0.01609	62.1540	2 308.13	37.1357
90	1.9591	0.5104	0.00782	127.8790	0.01532	65.2746	2 578.00	39.4946
96	2.0489	0.4881	0.00715	139.8562	0.01465	68.2584	2 853.94	41.8107
100	2.1111	0.4737	0.00675	148.1445	0.01425	70.1746	3 040.75	43.3311
108	2.2411	0.4462	0.00604	165.4832	0.01354	73.8394	3 419.90	46.3154
120	2.4514	0.4079	0.00517	193.5143	0.01267	78.9417	3 998.56	50.6521
132	2.6813	0.3730	0.00446	224.1748	0.01196	83.6064	4 583.57	54.8232
144	2.9328	0.3410	0.00388	257.7116	0.01138	87.8711	5 169.58	58.8314
240	6.0092	0.1664	0.00150	667.8869	0.00900	111.1450	9 494.12	85.4210
360	14.7306	0.0679	0.00055	1 830.74	0.00805	124.2819	1 3312	107.1145
480	36.1099	0.0277	0.00021	4 681.32	0.00771	129.6409	1 5513	119.6620

TABLA J.2 Tabla al 0,75 %

BIBLIOGRAFIA

1.- Tutorial de Gestión de Redes y Servicios de Telecomunicaciones por el Ing. Edgar Leyton Q.

2.- Manual de los Principios de la seguridad universal por Baltasar Urguzin.

3.-http://www.alvarion.com

4.-http://www.teldat.com

5.-http://www.dlink.com

6.-http://www.ademaco.com

7.-http://www.monografías.com

8-Ingeniería Económica, Leland Blank y Anthony Tarquin, Mc Graw Hill - 5ta. Edición