ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA, AUTOMATIZACIÓN Y CONTROL

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA, AUTOMATIZACIÓN Y CONTROL

AUTOR: AYALA SANDOVAL, RONALD FERNANDO

TEMA: DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD ELECTRÓNICA MULTIMARCA CON TECNOLOGÍA ESTÁNDAR PARA LA EMPRESA SRT HARDCOM S.A.

DIECTOR: ING. ESCOBAR, MARCELO

CODIRECTOR: ING. TIPÁN, EDGAR

SANGOLQUÍ, FEBRERO 2014

Certificado de tutoría

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
INGENIERÍA EN ELECTRÓNICA, AUTOMATIZACIÓN Y CONTROL

CERTIFICADO

Ing. Marcelo Escobar
Ing. Edgar Tipán

CERTIFICAN

Que el trabajo titulado "Diseño e implementación de un sistema de seguridad electrónica multimarca con tecnología estándar para la empresa SRT HARDCOM S.A.", realizado por Ronald Fernando Ayala Sandoval, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la Universidad de las Fuerzas Armadas - ESPE, en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas - ESPE.

Debido a que se trata de un trabajo de investigación recomiendan su publicación.

El mencionado trabajo consta de un documento empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan a Ronald Fernando Ayala Sandoval que lo entregue al Ingeniero Luis Orozco, en su calidad de Coordinador de la Carrera.

Sangolquí, 17 de Febrero de 2014

Ing. Marcelo Escobar	Ing. Edgar Tipán
DIRECTOR	CODIRECTOR

Declaración de Responsabilidad

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

INGENIERÍA EN ELECTRÓNICA, AUTOMATIZACIÓN Y CONTROL

DECLARACIÓN DE RESPONSABILIDAD

RONALD FERNANDO AYALA SANDOVAL

DECLARO QUE:

El proyecto de grado denominado "Diseño e implementación de un sistema de seguridad electrónica multimarca con tecnología estándar para la empresa SRT HARDCOM S.A.", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan al pie, de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 17 de Febrero de 2013

Ronald Fernando Ayala Sandoval

Autorización de publicación

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

INGENIERÍA EN ELECTRÓNICA, AUTOMATIZACIÓN Y CONTROL

AUTORIZACIÓN

Yo, Ronald Fernando Ayala Sandoval

Autorizo a la Universidad de las Fuerzas Armadas - ESPE la publicación, en la biblioteca virtual de la Institución del trabajo "Diseño e implementación de un sistema de seguridad electrónica multimarca con tecnología estándar para la empresa SRT HARDCOM S.A.", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría

Sangolquí, 17 de Febrero de 2013

Ronald Fernando Ayala Sandoval

DEDICATORIA

A mis padres, mi hermana y mis abuelos, que sin su apoyo incondicional y sus enseñanzas a lo largo de mi vida no hubiera podido superar este peldaño que marca el rumbo de lo que me resta por vivir.

Ronald Ayala S.

AGRADECIMIENTO

Agradecer a Dios primeramente por permitirme la vida, por mostrarme siempre el camino a seguir y ponerme en el camino a personas valiosas de las cuales he aprendido los valores y principios que marcan mi vida. A mis padres y a mi familia por su comprensión, apoyo y aliento en los momentos difíciles de esta larga etapa. Al Ingeniero Marcelo Escobar por la ayuda brindada para llevar a cabo este proyecto y al Ingeniero Edgar Tipán por los consejos para concluir de la mejor manera este propósito.

Ronald Ayala S.

INDICE GENERAL

INDICE DE FIGURAS

ÍNDICE DE TABLAS

INDICE DE ANEXOS

RESUMEN

El presente proyecto ha sido desarrollado para cumplir con las exigencias de la empresa SRT HARDCOM en cuanto se refiere a un sistema de seguridad integral y robusto. Estas exigencias solicitaban que el sistema sea realizado con tecnología estándar haciendo uso de dispositivos adquiridos con anterioridad por la empresa pero que no se les estaba dando uso. Con el objetivo de potenciar la funcionalidad de estos dispositivos se adquirieron nuevos elementos bajo la misma marca que es de la empresa española ISDE-ING que maneja el estándar LONWorks, debido a la flexibilidad que el estándar y los dispositivos presentan se pudo integrar los sistemas de control de accesos, detección de incendios, sistema anti – intrusión y un circuito cerrado de televisión, este último permitirá el monitoreo local o remoto en tiempo real de las instalaciones. Además mediante una HMI podrá verificarse el estado de cada uno de los sensores, detectores o actuadores que se encuentran integrados en el sistema así como también realizar la apertura de las puertas, donde se ha implementado el control de accesos, desde la misma interfaz.

PALABRAS CLAVE

- Inmótica
- Tecnología LONWorks
- Sistema de control
- Automatización y control

ABSTRACT

This project has been developed to meet the requirements of the company SRT HARDCOM refers to a integral and robust security system. These requirements make the system be realized with standard technology using devices previously acquired by the company but not were giving use. In order to enhance the functionality of these devices were purchased new devices under the same brand that is the Spanish ISDE -ING company that handles LONWorks standard , due to the flexibility that the standard and the devices presented could be integrate systems like access control, fire detection, anti - intrusion system and CCTV , the latter allow local or remote real-time monitoring of the offices. Also through HMI can check the status of each of the sensors, actuators or detectors who are integrated in the system as well the opening of the doors , which has implemented the access control from the same interface.

CAPÍTULO I.

INTRODUCCIÓN.

El propósito de los avances tecnológicos han sido en su gran mayoría para solucionar o simplificar las labores cotidianas del ser humano, además sean capaces de brindarles seguridad y a un costo muy accesible con respecto a todos los beneficios que se obtienen a mediano y largo plazo.

En torno a estos avances se han desarrollado soluciones tecnológicas también con lo que tiene que ver con problemas sobre todo de supervisión en domicilios u oficinas lo cual se denomina domótica e inmótica respectivamente.

Sin duda estos avances tecnológicos son mucho más difundidos en países como Estados Unidos o países de Europa, pero desde hace algunos años todas estas bondades tecnológicas las requieren países como el nuestro que no puede quedarse atrás en cuanto a todos estos avances se refiere.

La integración de un sistema de seguridad electrónica tiene que ver con la interacción de los dispositivos de distintos sistemas, alarmas, anti-intrusión, CCTV o incendios, formando uno solo con un mismo fin que es el de salvaguardar la integridad de las personas y de los bienes materiales de quienes han decidido implementar éste sistema de seguridad electrónica.

Ésta tecnología es mucho más difundida en las empresas u oficinas que en domicilios ya que es donde más interesa tener sus bienes seguros y controlar el trabajo y la asistencia de sus empleados.

En concordancia con el proyecto a llevarse a cabo se han seleccionado los equipos y dispositivos que más se ajustan con los requerimientos tanto técnicos como económicos del mismo.

1.1. SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN.

1.1.1. GENERALIDADES.

Más conocido como CCTV, éste sistema de video vigilancia se encuentra compuesto por cámaras de video conectadas a monitores o televisores.

Es denominado como circuito cerrado ya que a diferencia de lo que pasa con la difusión, todos sus componentes se encuentran enlazados y solamente tienen acceso a ellos un número limitado de personas.

En un principio estos dispositivos se usaban únicamente para detectar o evitar robos, actualmente pueden existir varias aplicaciones de un CCTV como en la medicina, en la educación o como parte de la lucha contra eventos antisociales.

1.1.2. SISTEMA DE CCTV PARA VIDEO-VIGILANCIA.

En esta aplicación del circuito cerrado de televisión, éste circuito estará compuesto además de las cámaras y monitores por un grabador digital de video o DVR por sus siglas en inglés (Digital Video Recorder) o NVR por sus siglas en inglés (Network video Recorder), la diferencia entre estos dos dispositivos de almacenamiento digital radica en que el DVR se lo utiliza en

un circuito analógico mientras que un NVR se lo usa en estructuras basadas en redes IP.

Estos sistemas pueden incluir operaciones asistidas por un computador, visión nocturna o activación por detección de movimiento, además de la interacción que las cámaras pueden tener con todo un sistema de seguridad electrónica al integrar este circuito cerrado de televisión con otros sistemas.

En el presente proyecto se utilizará un Digital Video Recorder debido esencialmente al costo y a las funciones muy similares que tienen un DVR y un NVR.

1.1.2.1. DIGITAL VIDEO RECORDER O DVR.

La función esencial de un DVR es el grabar las señales de video análogas de las cámaras y convertirlas a un formato digital, esto permite la monitorización remota del espacio vigilado.

Generalmente estos equipos tienen una gran capacidad de almacenamiento debido a toda la información que conlleva el grabar un video continuamente.

Anteriormente las grabadoras de video-vigilancia lo hacían sobre cintas magnéticas de cassette ahora conocemos que independientemente de qué tipo de cámaras de vigilancia se usen, la grabación de ésta información en cassette no es muy eficaz ya que éstos ocupan espacio físico, no almacenan mucha información y la dificultad para encontrar o identificar un suceso en específico es elevada.

El DVR es un equipo que contiene, software y un disco duro para el almacenamiento de video. Acepta las señales de video de cámaras analógicas y las convierte en digitales y se ha constituido en una solución muy efectiva en un mundo digitalizado con los mismos beneficios que un NVR pero mucho más económico.

Los sistemas convencionales de CCTV solo pueden transmitir las señales de sus cámaras a una sola estación de monitoreo, pero ese ya no es el caso con el uso de un DVR. Actualmente la gran mayoría de los DVR son capaces de permitir acceder a la información de sus cámaras de forma remota mediante un computador o teléfono móvil que cuente con acceso a Internet. Los DVR pueden proteger la información bajo contraseña para que solo los usuarios autorizados puedan monitorear el sistema.

Para aprovechar al máximo la capacidad de almacenamiento que dispone el disco duro, los DVR pueden ofrecer una serie de formatos para la compresión del video, el fin de ésta compresión ese el reducir el tamaño de los archivos lo máximo que sea posible sin comprometer la calidad de las imágenes. Los formatos de compresión más comunes son MPEG-4 o Motion JPEG.

1.2. SISTEMA DE CONTROL DE ACCESOS.

1.2.1. GENERALIDADES.

Los sistemas de control de accesos son indispensables en un sistema de seguridad electrónica ya que son usados generalmente para el control de puertas tanto internas como externas, su uso va desde viviendas, oficinas o edificios con alta tecnología, este sistema impide que las personas accedan sin autorización a áreas de interés para la oficina o empresa.

Otro de los beneficios que puede tener éste sistema es controlar los horarios de entrada y de salida de los empleados a sus oficinas teniendo así una manera efectiva de conocer los horarios que el personal está cumpliendo dentro de las oficinas.

Este tipo de sistemas cumplen con su cometido mediante el uso de dispositivos de entrada tales como lectores de proximidad, lectores

magnéticos o lectores biométricos, el uso de uno de estos dispositivos dependerá de la aplicación prevista para éste o el área donde se lo vaya a instalar.

Los sistemas de control de accesos son de dos tipos, Autónomos y Con conexión a computador, y su precio varía de acuerdo a las puertas sobres las cuales tendrá control.

Sistemas Autónomos.

Los sistemas autónomos no necesitan estar conectados constantemente a un computador, solamente basa su funcionamiento en los códigos almacenados en su memoria.

Uno de estos sistemas puede ser el utilizado para el acceso vehicular a edificios.

Con Conexión al Computador.

Éste tipo de sistemas generalmente incluyen un software para su configuración y almacenamiento de los códigos de acceso, y se diferencian por el número de puertas que controla. Estos sistemas disponen de una memoria que mantiene un respaldo de los códigos de acceso en caso de la pérdida de energía.

El sistema de accesos estará constituido por los siguientes componentes:

- Lectora de proximidad
- Tarjetas de proximidad
- Módulo de control
- Cerradura electromagnética
- Botón de salida
- Control desde una interfaz

Existen varios protocolos con los que se pueden enlazar los controladores de accesos con sus respectivos sensores o lectores de proximidad que son soportados por ambos, pero se utilizará el protocolo Wiegand 26.

1.2.2. PROTOCOLO WIEGAND.

1.2.2.1. GENERALIDADES.

Este protocolo es el más utilizado por los fabricantes de lectores de proximidad ya que permite la transmisión de la información y la alimentación para el dispositivo a través de un par de cobre sin comprometer la calidad de los datos.

“El término del interface Wiegand es una marca de la sociedad “Sensor Engineering Company” y fue diseñado para conseguir una tecnología que permitiera transmitir datos de un identificador (tarjeta) entre dos dispositivos alejados entre sí, como, por ejemplo, un lector y la central de control de accesos. El protocolo Wiegand es ampliamente utilizado por la mayor parte de los fabricantes porque permite la transmisión de información a través de un par de cobre que se acompaña de la alimentación para el dispositivo de lectura si afectar por ello a los datos.” (Control-Accesos, 2008)

1.2.2.2. PROTOCOLO WIEGAND 26.

Al igual que cualquier protocolo de comunicaciones, Wiegand 26, consta de dos partes fundamentales, una de ellas describe el modo en que se transmite la información obtenida análoga o digitalmente y otra parte que indica la manera de interpretar numéricamente esta información.

SISTEMA DE TRANSMISIÓN

Se trata de una transmisión que usa tres hilos. El primero que es denominado DATA1 que maneja los unos lógicos, el segundo que maneja los ceros lógicos o DATA0 y la línea de referencia para ambos hilos llamado GND. Las señales trasmitidas van entre 0V y 5,5V como máximo. Los valores de uno lógico y cero lógico son impulsos de entre 20 µs a 100 µs de duración.

Mientras se encuentra sin transmitir GND se encuentra en nivel bajo y las líneas DATA1 y DATA0 se encuentran en nivel alto de 5V o VCC. Para transmitir un uno lógico se envía por DATA1 un pulso a Bajo, generalmente de 50 µs, mientras que DATA0 permanece Alto. Para transmitir un cero lógico se envía por DATA0 un pulso a Bajo de la misma duración, mientras que ahora DATA1 se mantiene en Alto.

Representación de la transmisión de la secuencia 1101001. Figura 1.

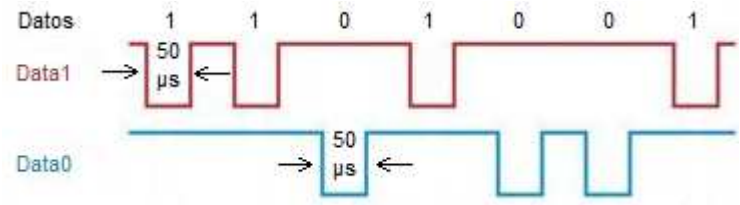


Figura 1. Diagrama de estados del protocolo Wiegand 26.

El protocolo Wiegand 26 está compuesto por 26 Bits que se los interpreta de la siguiente manera:

- El primer Bit, B0, corresponde a la Paridad Par de los primeros 12 bits transmitidos de B1 a B12.
- Los bites del B1 al B8 forman un Byte que es denominando como Facility Code del código de la tarjeta.

- Los 16 bits siguientes del B9 al B24 son dos Bytes a los que en conjunto se los llama User Code.
- Finalmente el bit B25, es la paridad impar de los bits del B13 al B24.

1.3. SISTEMA DE ALARMA ANTI-INTRUSIÓN.

1.3.1. GENERALIDADES.

Hoy en día con la alta tasa de criminalidad que perjudica a la sociedad en general es fundamental contar con un sistema de alarma anti-intrusión o antirrobo, como su nombre lo indica es un sistema dedicado a detectar el ingreso de personas no deseadas a nuestro hogar, oficina o locales comerciales evitando así ser víctimas de daño a las personas o el hurto de los bienes materiales que en ese momento se encontrasen.

Un sistema anti intrusión está compuesto esencialmente por sensores de movimiento que pueden encontrarse en el interior o en el exterior de las instalaciones a supervisar, un teclado que permita la identificación del personal autorizado a ingresar y pueda desactivarse el nivel de alarma y finalmente una sirena que avise sobre la violación de seguridad. Adicional a estos dispositivos se implementarán sensores de ruptura de cristal, pulsador de pánico y contactos magnéticos para detectar la apertura de puertas o ventanas mientras la alarma se encuentre activa.

Como no puede ser de otra manera en este proyecto se lo va a integrar con otros sistemas de alarma para aprovechar todas las potencialidades que éste puede brindar.

1.3.2. DESCRIPCIÓN DE ELEMENTOS COMPONENTES.

TECLADO DE ACCESO.

Debido a que el sistema de seguridad electrónica se lo va a implementar sobre tecnología LonWorks®, se utilizará un teclado de accesos compatible con éste, bajo la marca Española ISDE-ING y es el modelo **INM-050-X/V3.** Figura 2.

Figura 2. Nodo INM-050.

Este teclado servirá principalmente para armar y desarmar a la alarma que estará implementada en las instalaciones de la empresa SRT HARDCOM S.A.

SENSORES DE MOVIMIENTO.

Se utilizarán sensores de movimiento los cuales son capaces de detectar la variación de luz del espacio hacia donde se encuentren orientados, informando de esta manera si un cuerpo se está moviendo en el área.

Figura 3. Detector de movimiento.

En la Figura 3., se observa la forma más común de un sensor de movimiento, el cual cuenta con un domo por el cual “sensa” el dispositivo las variaciones de luz y sobre éste se encuentra un diodo emisor de luz que indica que ha detectado movimiento.

DISCRIMINADOR DE AUDIO.

Este sensor está dedicado a detectar las ondas sonoras producidas en el ambiente pero especialmente comunica cuando ha detectado el sonido característico de la ruptura de un cristal el cual puede ser una ventana o puerta de cristal.

Éste sensor constantemente compara las frecuencias sonoras de su alrededor con una frecuencia pre-establecida en su memoria que corresponde a dicha ruptura de un cristal.

Figura 4. Discriminador de audio.

Este dispositivo cuenta con hendiduras como se ven en la Figura 4., que permiten el ingreso de las ondas sonoras hasta el sensor ubicado internamente en conjunto con toda su circuitería.

CONTACTO MAGNÉTICO.

Los contactos magnéticos se los instalará en las puertas y ventanas donde se consideren como puntos a los cuales personas podrían ingresar sin autorización. Éstos contactos magnéticos dan su señal de alerta cuando éste se ha separado quedando abierto o cerrado el circuito.

Figura 5. Contacto Magnético.

El contacto magnético está compuesto por dos partes (Figura 5.), las cuales van instaladas en la ventana o puerta y la otra parte en el marco de ésta.

PULSADOR DE PÁNICO.

El pulsador de pánico se lo ubica generalmente oculto a la vista del público en puntos estratégicos donde la persona que lo accione lo haga rápidamente al sentirse atacada o entrar en pánico por alguna situación.

Figura 6. Pulsador de pánico.

Como se muestra en la Figura 6., solamente se trata de un pulsador común y corriente con la identificación correspondiente, al pulsarlo activará inmediatamente la alarma sin ninguna restricción adicional.

1.4. SISTEMA DE ALARMA DE INCENDIOS.

1.4.1. GENERALIDADES.

Una alarma de incendios es un sistema que se activa cuando se detecta algún evento correspondiente a la existencia de humo, a la activación de una estación manual o a un cambio brusco de temperatura. El sistema advierte al personal de la existencia de un posible incendio para realizar la evacuación.

Éste sistema generalmente forma parte de un sistema de seguridad electrónica que incluye el sistema de alarma anti-intrusión, pero en este proyecto se avanzará más allá y se o integrará además con Sistemas de CCTV y Sistemas de Control de Accesos.

1.4.2. DESCRIPCIÓN DE ELEMENTOS COMPONENTES.

ESTACIÓN MANUAL.

En una alarma de incendios un elemento imprescindible es la estación manual ya que en caso de incendio lo pueden activar las personas mucho antes de que los sensores de humo o temperatura hayan detectado la existencia del fuego.

Figura 7. Estación Manual de Incendios.

Se trata de interruptores que cierran o abren su circuito e indican su alarma al momento de que se los acciona, según el modelo se tira de una lengüeta (Figura 7.), de una palanca o se pulsa un botón.

SENSOR DE HUMO.

Un sensor de humo es un dispositivo que detecta la presencia de humo en el aire y emite su señal de alarma. El detector de humo a utilizarse será del tipo foto-eléctrico.

Su funcionamiento se resume a que en una cámara interna que está en contacto con el aire se encuentra una fuente luminosa enfrentada a un detector luminoso, cuando la densidad del humo interrumpe el paso de la luz entre el emisor y el sensor fotosensible se activa un relé encendiendo la alarma.

Figura 8. Detector de Humo.

1.5. INTEGRACIÓN DE SISTEMAS DE SEGURIDAD.

1.5.1. GENERALIDADES.

El significado de la palabra Integración nos conduce a la interconexión o al entrar a formar parte de todo un conjunto de dispositivos, equipos o sistemas. Este significado llevado a la Integración de Sistemas de Seguridad hace que todos los subsistemas que lo componen compartan información, haciendo posibles relaciones óptimas entre el sistema, el espacio a ser vigilado y el operario o supervisor del sistema teniendo toda la información en una sola plataforma.

Un Sistema de Seguridad Integral debe cumplir la modularidad en sistemas más sencillos dedicados cada uno específicamente a sus funciones pero bajo una dirección centralizada. De esta manera se podrían encontrar los siguientes sistemas:

Figura 9. Concepto de Sistema de Seguridad Electrónica Integrada

Una plataforma que logre reunir a todos los componentes de un Sistema de Seguridad Electrónica debe ser capaz de recibir, controlar y generar señales para comunicarse con todos los dispositivos de cada uno de los sistemas.

Los beneficios de una Integración de un Sistema de Seguridad Electrónica son evidentes, como el poder relacionar todos los sistemas para optimizar los recursos disponibles en caso de alguna eventualidad.

El centralizar toda la información que nos brinda el sistema y el operar bajo una misma interfaz ayuda a mejorar la eficacia de la gestión de la seguridad ya que permite un menor tiempo de respuesta en las instalaciones donde se implemente el sistema.

En fin, un Sistema de Seguridad Electrónica Integrada cumple con varias necesidades, adicionales a las mencionadas, de las cuales se puede destacar las siguientes:

- Simplicidad de operación y mantenimiento.
- Alta inmunidad frente a pérdida de información.
- Flexibilidad y adaptabilidad en cuanto a ampliaciones o cambios.

1.5.2. EQUIPOS QUE COMPONEN LA INTEGRACIÓN.

Para la selección de los equipos que compondrán el Sistema de Seguridad Electrónica se ha tomado en cuenta sus conceptos de comunicación y funcionamiento.

Debido a que el Sistema de Seguridad Electrónica se basa en el protocolo LonWorks®, se lo implementará con nodos de la marca Española ISDE-ING, los cuales tendrán a su cargo dispositivos periféricos como sensores y actuadores.

FIGURA 10. Sistemas y dispositivos a ser integrados.

Lo que primordialmente se desea obtener con esta integración es un tiempo de respuesta menor y puntual según las eventualidades que puedan suscitarse con el fin de proteger a las personas o bienes.

CAPÍTULO II.

FUNDAMENTO TEÓRICO.

2.1. PROTOCOLO DE COMUNICACIÓN.

Entre los protocolos de comunicaciones utilizados para sistemas de control o automatización se tienen:

- Protocolo propietario o cerrado.
- Protocolo abierto o estándar.

El protocolo propietario o cerrado, es creado y orientado únicamente para comunicar los productos de un solo fabricante, es decir, no se puede integrar con productos de otros fabricantes impidiendo el crecimiento y la flexibilidad del sistema si así se lo requiriese. Lo cual si bien, en cuanto a costos a corto plazo representa una ventaja, a largo plazo se torna en una desventaja al tener que depender de un solo fabricante para el mantenimiento del sistema y la indisponibilidad de un repuesto en caso de cierre de la empresa productora de los dispositivos.

Como ejemplos de protocolos propietarios podemos destacar:

- BOSCH
- VIVIMAT
- BTICINO
- LUTRON

- SIMON
- COMUNITEC
- THUNDER
- VANTAGE

Por otra parte, un protocolo abierto o estándar, al encontrarse al alcance de cualquier empresa comprometida con su desarrollo, la difusión de éste es mucho mayor por lo cual muchos fabricantes alrededor del mundo han adoptado este protocolo para el desarrollo de sus productos produciéndose así la interoperabilidad y la integración entre los dispositivos haciéndolos capaces de intercambiar información y cooperar en el sistema, haciéndolo flexible y funcional sin la necesidad de desarrollar software o hardware a la medida.

Los beneficios de la interoperabilidad saltan a la vista, no teniendo que depender de un solo fabricante los costos de los proyectos bajan en su costo, además hace que cada desarrollador o fabricante se esfuerce para crear la mejor solución y eso se traduce en calidad, y permite a los responsables del mantenimiento o monitorización del sistema operarlo utilizando herramientas estándar sin importar el fabricante de cada subsistema.

Como protocolos estándar o abiertos citamos:

- DEVICE NET
- ISO/IEC 14908 o LONWORKS
- X10
- BACNET
- KNX-EIB
- BATIBUS
- ZIGBEE
- BLUETOOTH

De los cuales se podrían emplear dispositivos con los siguientes protocolos KNX-EIB, X10 o LONWorks debido a que los dispositivos que utilizan éstos no se encuentran en etapa de desarrollo sino en etapa de comercialización a diferencia de los adicionales protocolos mencionados. A continuación en la Tabla 1, se realiza una comparativa de características generales de estos tres protocolos de comunicación.

Tabla 1. Comparativa entre protocolos abiertos.

	Medio de Transmisión	Velocidad de Transmisión	Topología	Puntos Fuertes	Puntos Débiles
KNX-EIB	•Par trenzado •Powerline •Radio frecuencia •Ethernet	9,6 kbps	• Libre • Bus	**Interoperabilidad:** Todos los dispositivos etiquetados con la marca KNX están obligados a comunicarse correctamente. **Múltiples desarrolladores:** Libertad para elegir dispositivos de diferentes fabricantes. **Estándar Internacional:** ISO/IEC 14543-3. **Software:** Existe una sola herramienta independiente de la aplicación y del fabricante usada para el diseño y configuración de los dispositivos KNX llamada "Engineering Tool Software"	**Seguridad:** Si se pincha el BUS de una red KNX se puede tener acceso a los mensajes. **Dificultad del manejo:** El software de configuración es robusto pero no es sencillo de manejar. **Coste:** Todos los dispositivos KNX son generalmente costosos lo que se convierte en una desventaja.
LONWorks	• Par trenzado • Powerline • Ethernet	78 kbps a 1,25 Mbps	•Libre •Bus	**Interoperabilidad:** Según Echelon es definida como "La capacidad de integrar productos de distintos fabricantes en sistemas flexibles y funcionales sin necesidad de desarrollar herramientas a medida". **Estándar Internacional:** ISO/IEC 14908. **En continuo desarrollo:**	**Facilidad de manejo:** Al igual que el ETS de KNX, LONMaker es muy robusto pero no es sencillo de manejar.

				Actualmente se implementan versiones más rápidas y eficientes del Neuron Chip y totalmente compatibles con millones de dispositivos inteligentes. **Coste:** Los dispositivos que implementan el protocolo son económicamente asequibles. **Software:** Para el diseño, implementación y configuración de los dispositivos existe una herramienta denominada LONMaker aunque cada uno de los desarrolladores han creado su propia plataforma pero no estandarizada.	Continúa…
X10	• Powerline	60 bps	• Libre	**Altamente difundido:** Este en un protocolo que está muy presente en el mercado mundial sobre todo en Norteamérica y Europa. **Simple de implementar:** Se conectan los módulos en los aparatos a controlar, se les asigna una dirección y a continuación se les puede enviar órdenes básicas mediante una PC u otro mando a distancia compatible con X10. **Coste:** De los tres protocolos es el que posee los dispositivos con menor costo, debido a ser un sistema sencillo y preparado para la instalación no profesional.	**Interferencias:** Debido a que comparte sus datos con la alimentación del aparato a controlar la calidad de la señal depende muchísimo de la calidad de la red eléctrica. Aunque se implementen filtros por esta misma razón pueden existir pérdidas de datos haciendo al sistema poco confiable. **Uni-direccional:** Los dispositivos X10 no pueden mostrar el estado del aparato una vez enviada la señal. **No versátil:** Ya que no dispone de funciones lógicas programables que permitan realizar operaciones complejas, en su mayoría son operaciones ON/OFF o DIMMER.

Por lo expuesto, finalmente se escoge LONWorks como protocolo de comunicación a ser implementado debido a que sus ventajas de coste, interoperabilidad y confiabilidad superan a las ventajas las de los otros protocolos tomados en cuenta.

2.2. TECNOLOGÍA ISO/IEC 14908.

ISO/IEC 14908 especifica un protocolo de comunicaciones para redes de control. El protocolo permite la comunicación peer-to-peer para el control de la red, es decir, ésta es una red de nodos en la que no existen clientes ni servidores fijos, sino que todos los nodos se comportan como iguales entre sí. Estos actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red.

Comercialmente este estándar es conocido como LONWorks, que viene del conjunto de palabras LON que representan Local Operating Network, desarrollado por la empresa Echelon. Este estándar abarca todos los elementos necesarios para diseñar, monitorear, controlar e implementar una red de dispositivos diversos, además describe de manera efectiva una solución completa a problemas relacionados con la automatización y control electrónico.

Está diseñado en una plataforma de bajo ancho de banda para los dispositivos de red a través de líneas de alta tensión, fibra óptica y otros medios.

El comienzo de las redes LONWorks se basó en conceptos muy simples:

- Los sistemas de control son fundamentalmente idénticos, independientemente de la aplicación final;
- Un sistema de control distribuido es significativamente más potente, flexible y ampliable que un sistema de control centralizado;

- Las empresas ahorran más dinero a largo plazo instalando redes distribuidas que instalando redes centralizadas;
- La tecnología LONWorks proporciona una solución a los múltiples problemas de diseño, construcción, instalación y mantenimiento de redes de control; redes que pueden variar en tamaño desde dos a 32000 dispositivos y se pueden usar en cualquier aplicación.

Este estándar se basa en un esquema propuesto por LON (Local Operating Network), que consiste en un conjunto de dispositivos o nodos que cuentan con micro-controladores, que los faculta como autónomos y proactivos, que se conectan entre uno o más medios físicos y que se comunican utilizando un protocolo común.

LONWorks permite la creación de soluciones de código abierto para sistemas de control, lo cual se puede traducir en ventajas inmediatas de las que podemos destacar:

- Es una tecnología certificada por diversos institutos de estandarización, lo que garantiza la calidad de los sistemas.
- El programador o integrador del sistema puede usar dispositivos multi-fabricante debido a la interoperabilidad de la plataforma.
- El usuario final ya no estaría obligado a la adquisición de los dispositivos a un solo desarrollador.
- Cuenta con el protocolo de comunicación LONTalk es independiente del medio y con un grupo de estándares multi-industrial denominado LONMark para el aseguramiento de la interoperabilidad de los dispositivos LONWorks.

Esta plataforma para el intercambio de información, utiliza el protocolo LONTalk el cual debe ser soportado por todos los dispositivos componentes de la red y ya que es de código abierto está al alcance de todos los fabricantes.

LONTalk ha sido creado para enfocarse en funciones de monitorización y control de dispositivos en un entorno industrial. Dentro de este marco industrial se han debido potenciar las siguientes funcionalidades:

- Fiabilidad: LONTalk soporta aviso de recibido de extremo a extremo con reintentos automáticos, lo que provoca que no se produzcan comandos no cumplidos.
- Independencia del medio de transmisión: El protocolo puede ser transmitido tanto por medios físicos o inalámbricos. Entre los cuales se encuentran, par trenzado, red eléctrica, radio frecuencia, cable coaxial y fibra óptica.
- Tiempo de Respuesta: Se utiliza un algoritmo propietario para la predicción de colisiones que consigue evitar la degradación de prestaciones que se produce por tener un medio de acceso compartido.

El protocolo define una jerarquía de direccionamiento que incluye la dirección de dominio, subred y nodo. Cada uno de los dispositivos o nodos se encuentran conectados físicamente a un canal. Un dominio es una colección lógica de nodos que pertenecen a uno más canales. Una subred es una colección lógica de hasta 127 nodos contenidos por un dominio. Se pueden definir hasta 255 subredes dentro de un único dominio. Todos los nodos de una subred deben estar conectados a un mismo canal. Cada nodo tiene un identificador único de 48 bits asignado durante la fabricación, que se usa como dirección de red durante la instalación y configuración.

TABLA 2. Jerarquías de red.

Jerarquía	Cantidad
Subredes por dominio	255
Nodos por subred	127
Nodos por dominio	32385
Grupos por dominio	255
Nodos por grupo	63

LONMark Internacional, es un grupo el cual proporciona los estándares para garantizar la interoperabilidad de los distintos dispositivos desarrollados por diversos fabricantes, y consta de los siguientes miembros:

- Fabricantes de equipos originales (OEMs).
- Desarrolladores independientes LONWorks (LIDs).
- Integradores de red (NIs).
- Consultores, instaladores y usuarios.

Las funciones principales de esta organización son las de, promover los beneficios de productos interoperables LONMark además de proveer de programas de publicidad para compañías desarrolladoras de productos LONMark y proveer de un foro para definir requerimientos de diseño para aplicaciones específicas.

2.2.1. ELEMENTOS DE LA RED LONWORKS.

- **Elementos físicos de la red LONWorks.**

Se toman como elementos físicos de red LONWorks a todos los equipos, nodos y dispositivos certificados por LONMark además del medio de transmisión de la red para concretar las comunicaciones, que en su mayoría son de par trenzado, y las herramientas de red, que nos ayudan a la correcta configuración, monitoreo y control de cada uno de los nodos que componen al sistema, los cuales se los detallará más adelante en este capítulo.

Los elementos físicos de la red a ser diseñada e implementada serán dispositivos de la familia “HOTELON” bajo la marca ISDE Ing, empresa española desarrolladora de nodos LONWorks.

- **Elementos lógicos de la red LONWorks.**

Bloques Funcionales.

Un bloque funcional representa lógicamente a un nodo de la LON y es el que contiene la función que deberá llevar a cabo el nodo físicamente. Estos bloques funcionales manejan las variables de red así como también las variables de configuración del nodo. La organización LONMark define plantillas estándares para estos bloques funcionales denominados Perfiles Funcionales Estándares (SFPs).

Variables de Red.

Cada nodo define una serie de variables de red que pueden ser compartidas por los demás nodos, cada nodo tiene variables de entrada, de salida y de configuración estándares o SNVTs que son definidas por LONMark para fomentar la interoperabilidad pero además pueden existir otras que han sido creadas por el desarrollador, si las SNVTs no cumplen con las necesidades del dispositivo, a las cuales se las denomina UNVTs.

Propiedades de Configuración.

Las propiedades de configuración son valores que los determina el usuario, que definen el comportamiento del dispositivo tales como, el punto de consigna, límite o throttle máximo.

LONMark define los Tipos de Propiedades de Configuración Estándares o SCPTs para fomentar la interoperabilidad. Los fabricantes de dispositivos pueden definir sus propios tipos de propiedades de configuración, a los que se los denomina Tipos de Propiedades de Configuración del Usuario o UCPTs, en el caso que una SCPT no cumpla con las necesidades del equipo. (Echelon, 2007)

2.3. NODO LECTOR DE PROXIMIDAD INP-120R/I (ISDE-Ing, 2005)

Conjuntamente con el lector de proximidad son los encargados de la permisión o negación del acceso a una persona, mediante la validación de tarjeta incluida en lista o por configuración horaria. Cuenta con 2 entradas libres de potencial y 2 salidas a relé como se observa en la Figura 11., y se detallan sus características técnicas en la Tabla 3.

FIGURA 11. Nodo lector de proximidad INP-120R/I

2.3.1. Características generales.

- Topología de conexión: Bus.
- Entrada RJ-45 para conexión con el nodo lector Wiegand de 26 bits.
- Transceptor RS-485-78K, programación y configuración remota.
- Compatible con sistema HOTELON®.
- Configuración horaria en tiempo real para realizar programaciones individuales.
- Insensible a la polaridad del bus y en la alimentación de 12Vcc.
- Proporciona 2 entradas libres de tensión y 2 salidas.

2.3.2. Especificaciones funcionales.

- Control de acceso o iluminación en función de tarjeta válida o inválida.
- Control de acceso a través de validación de tarjeta incluida en lista blanca.
- Flexible actualización de lista blanca.
- Salidas indicadoras para tarjeta válida o inválida.

2.3.3. Características técnicas.

TABLA 3. Características técnicas Nodo INP-120R/I.

Características	Descripción
Alimentación	12 VDC
Grado de protección	IP20
Número de entradas	2 (Libres de tensión)
Número de salidas	2 (Salidas a relé)
Transceptor	RS-485
Velocidad de comunicaciones	78kbps
Actualización de firmware	Mediante Bus
Sujeción mecánica	Carril DIN 6U

2.3.4. Conexión eléctrica y dimensiones.

A continuación se indican las dimensiones del nodo y los bloques de conexión del mismo con el lector de proximidad, así como su alimentación y sus salidas.

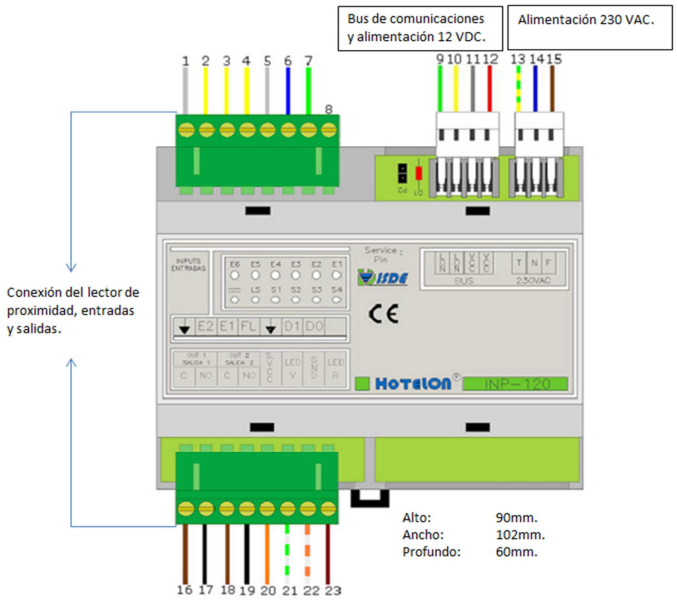


FIGURA 12. Conexiones y dimensiones del Nodo INP-120R/I.

Conexión con el Lector de Proximidad.

1. Común de entradas 1 y 2.
2. Entrada 1
3. Entrada 2
4. Salida de fin de lectura
5. GND
6. Dato 1 Lector Wiegand
7. Dato 0 Lector Wiegand
8. Sin utilizar
9. Comunicaciones LON
10. Comunicaciones LON
11. Alimentación 0Vcc
12. Alimentación 12Vcc
13. Tierra Alimentación
14. Neutro Alimentación 230Vac
15. Fase Alimentación 230Vac
16. Fase Circuito Salida 1
17. Salida Circuito 1
18. 12Vcc para Cerradura
19. Salida a Cerradura
20. Alimentación 12Vcc al lector
21. Led Verde o acceso permitido
22. Neutro Lector Wiegand/Led
23. Led Rojo o acceso denegado

2.3.5. Firmware.

Es el software que contiene todas las variables y parámetros de configuración posibles que se carga mediante el bus al nodo INP-120R/I.

TABLA 4. Firmware INP-120R/I

MODELO	TRANSCEPTOR	FIRMWARE
INP-120R	RS-485	XIF: F13130000001.XIF APB: F13130000001.APB

2.4. MÓDULO LECTOR DE PROXIMIDAD AR-721U

El módulo lector de proximidad va a ser el encargado de identificar y transmitir el código década tarjeta al nodo INP-120R/I, para la decodificación y permitir o denegar el acceso.

En el mercado existen varios modelos de terminales lectores de proximidad con el protocolo Wiegand 26, pero debido a sus costes asequibles y operatividad se ha tomado a este modelo de terminal como el escogido a ser implementado en el sistema.

Como se puede observar en la Figura 13.es de fabricante SOYAL y sus características técnicas se detallan en la Tabla 5.

FIGURA 13. Módulo lector de proximidad AR-721U.

- Varios formatos programables para la salida como son:
  - Wiegand 26 o 34
  - ABA-II
  - ASYNC
  - OMRON
- Integrado con watchdog para evitar que el sistema se detenga

- Fácilmente integrable con otros sistemas de control de acceso SOYAL u otros.

2.4.2. Características técnicas.

TABLA 5. Características técnicas Lector de proximidad AR-721U. (SOYAL, SOYAL, 2008)

Características	Descripción
Alimentación	9-16 VDC
Grado de protección	IP20
Interfaz de comunicación	WG 26/34, ABA-II, ASYNC, OMRON
Rango de proximidad para lectura	3-8 cm
Velocidad en baudios	9600 bps
Indicadores	Mediante LED bicolor y sonoro

2.4.3. Conexión eléctrica y dimensiones.

En la Figura 14., se indican las dimensiones del módulo lector de proximidad y las conexiones del mismo.

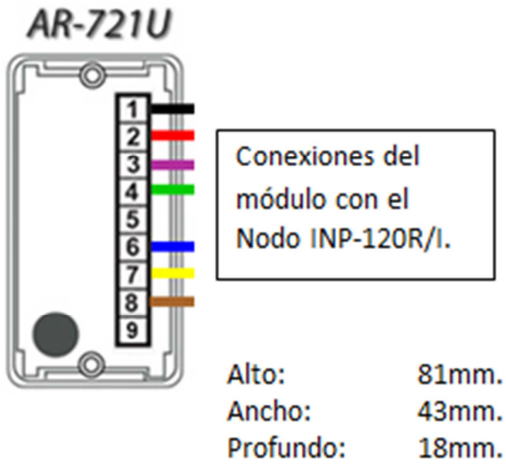


FIGURA 14. Conexiones y dimensiones del lector de proximidad AR-721U. (SOYAL, 2008)

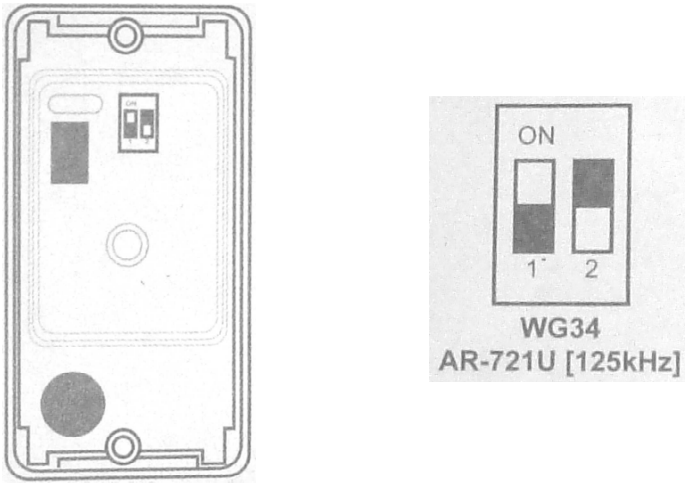
Descripción de conexiones.

1. Alimentación 0Vcc
2. Alimentación 12Vcc
3. Entrada de sonido de buzzer
4. Salida Wiegand Dato 0

5. Tarjeta presente
6. Salida Wiegand Dato 1
7. Entrada de Led en Rojo
8. Entrada de Led en Verde
9. Salida de sonido de buzzer

Selección de la interfaz de comunicaciones.

Al abrirle al módulo lector de proximidad, podemos observar en su interior un selector o switch de dos entradas (Figura 15), las cuales de acuerdo a la combinación permiten seleccionar el tipo de comunicación que va a ejecutar el módulo.



a) b)

FIGURA 15. a) Vista interna y ubicación del selector interno del módulo AR-721U. b) Selector en configuración Wiegand 34.

A continuación en la Tabla 6., se detallan, en una tabla de verdad, las combinaciones que permite realizar este selector.

TABLA 6. Selección de salida.

SALIDA	232(TTL)/ABA(DIP_SW1)	26/34(DIP_SW2)
Wiegand 26	OFF	OFF
Wiegand 34	OFF	ON
RS-232 (TTL)	ON	OFF
ABA-II	ON	ON

2.4.4. Tarjetas de proximidad.

Las tarjetas de proximidad para un sistema de control de accesos son la solución más eficiente en cuanto a costo y durabilidad ya que al no tener contacto su duración es indefinida. Suele usárselas como tarjetas de identificación, llaves para el control de accesos, tarjetas de pago o tarjetas de tránsito público.

Los chips de las tarjetas a usarse en este proyecto trabajan a una frecuencia relativamente baja de 125kHz. Su alcance está limitado al alcance de la lectora que como se ha dicho anteriormente es de 3 a 8 cm. Este tipo de tarjetas de baja frecuencia suelen utilizarse en servicios que no necesitan más que un dato por tanto son aptas para su uso en el transporte público y aplicaciones como tarjeta de identificación o tarjetas de pago.

Internamente esta tarjeta está compuesta por una antena de varias espiras y un chip el cual lleva grabado un código único de identificación.

El funcionamiento como se puede observar en la Figura 16., es simple, por medio de inducción electromagnética el lector de proximidad alimenta al chip de la tarjeta al aproximársele y éste a su vez emite un código único grabado en su memoria.

FIGURA 16. Principio de funcionamiento de una tarjeta de proximidad.

El proceso restante de la admisión o negación del acceso viene dado por el controlador.

2.5. NODO DE CONTROL AVANZADO INS-460R/I (ISDE-Ing, 2005)

Dispositivo que cuenta con 6 entradas libres de potencial y 4 salidas a relé como se observa en la figura 17., y se detallan sus características técnicas en la Tabla 7. Está pensado para el control, gestión y supervisión de alarmas o sistemas eléctricos.

FIGURA 17. Nodo de control avanzado INS-460R/I

2.5.1. Características generales.

- Topología de conexión: Bus.
- Transceptor RS-485-78K, programación y configuración remota.
- Compatible con sistemas DOMOLON® y HOTELON®.
- Configuración horaria en tiempo real para realizar programaciones individuales.
- Insensible a la polaridad del bus y en la alimentación de 12Vcc.
- Proporciona 6 entradas libres de tensión y 4 salidas a relé.
- Salida de alimentación de 12Vcc para los periféricos conectados al nodo.

2.5.2. Especificaciones funcionales.

- Sus entradas están preparadas para conteo de señales. Ejemplos típicos son la lectura de contadores de agua, electricidad, etc.
- Utilizado para zonas comunes en edificios con elementos de control y automatización.
- Las versiones con reloj incorporan un completo reloj, con segundo, minuto, día, hora, día de la semana, día del mes, mes y año con función de cambio automático Verano/Invierno.
- Todas las entradas trabajan con muy baja tensión (5V) dando un alto grado de seguridad a la instalación e incrementando la vida útil de los mecanismos al conmutar pequeñas tensiones y corrientes.
- Soporta pulsadores estándar, así como detectores de presencia, gas, fuego, humo, etc.
- Incorpora 4 relés de conmutación, para circuitos de hasta 8Amp, normalmente abiertos con funciones de inversión.
- En función del firmware cargado, la funcionalidad del nodo varía.
- Se suministra una librería completa de firmware para realizar funciones típicas de control y supervisión de cuadros eléctricos, transmisión de alarma, control remoto de actuaciones, etc.

2.5.3. Características técnicas.

TABLA 7. Características técnicas Nodo INS-460R/I.

Características	Descripción
Alimentación	12 VDC
Grado de protección	IP20
Número de entradas	6 (Libres de tensión)
Número de salidas	4 (Salidas a relé)
Características contacto de conmutación	8A/230Vac cosφ=1 5A/30Vdc
Transceptor	RS-485
Velocidad de comunicaciones	78kbps
Actualización de firmware	Mediante Bus
Sujeción mecánica	Carril DIN 6U

2.5.4. Conexión eléctrica y dimensiones.

A continuación en la Figura 18., se indican las dimensiones del nodo y los bloques de conexión del mismo, así como su alimentación y sus salidas.

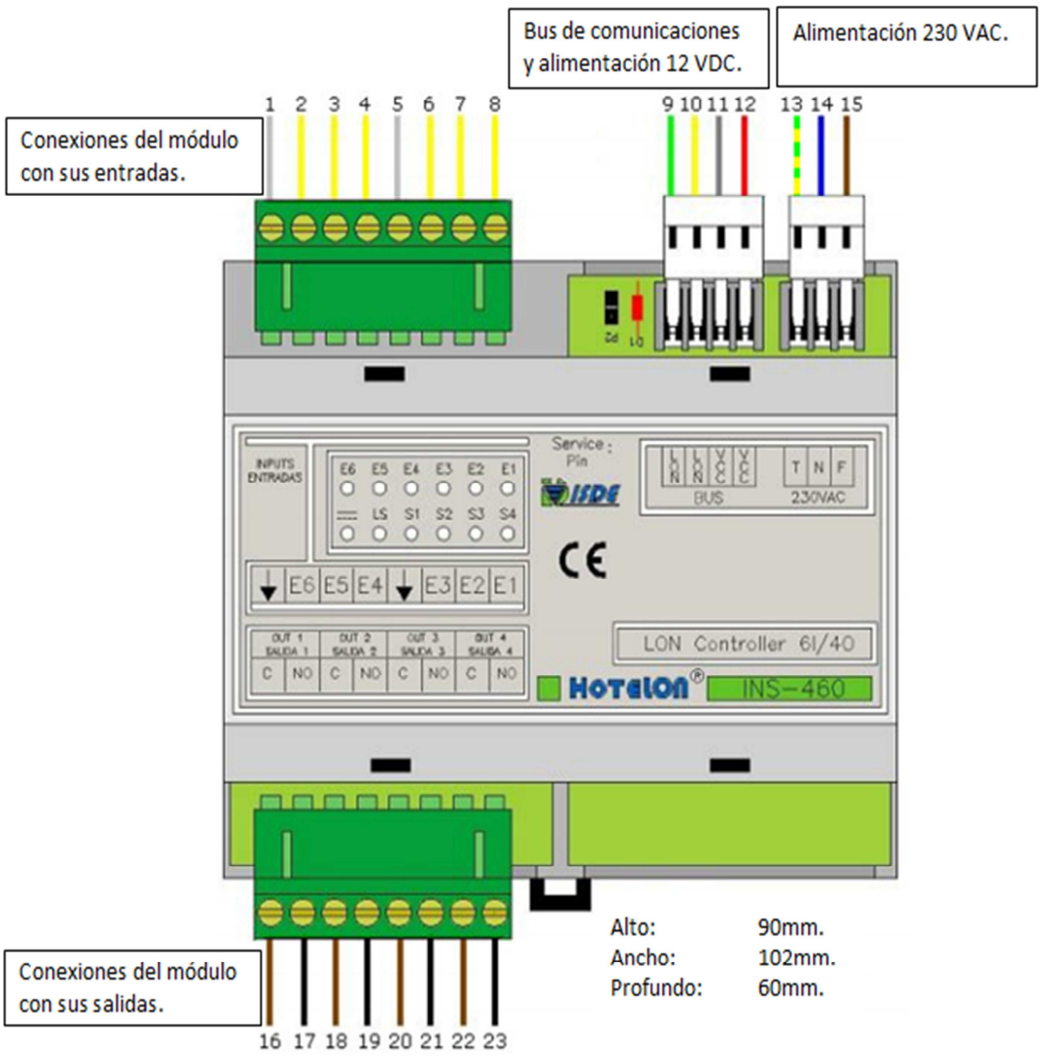


FIGURA 18. Conexiones y dimensiones del Nodo INS-460R/I.

Descripción de conexiones.

1. Común Entrada 6,5,4
2. Entrada 6
3. Entrada 5
4. Entrada 4
5. Común Entrada 3,2,1
6. Entrada 3

7. Entrada 2
8. Entrada 1
9. Comunicación LON
10. Comunicación LON
11. Alimentación Vcc
12. Alimentación Vcc
13. Tierra Alimentación
14. Neutro Alimentación 230Vac
15. Fase Alimentación 230Vac
16. Fase Circuito de Salida 1
17. Salida de Circuito 1
18. Fase Circuito de Salida 2
19. Salida de Circuito 2
20. Fase Circuito de Salida 3
21. Salida de Circuito 3
22. Fase Circuito de Salida 4
23. Salida de Circuito 4

2.5.5. Firmware.

El Firmware es el software que contiene todas las variables y parámetros de configuración posibles que se carga mediante el bus al nodo INS-460R/I.

TABLA 8. Firmware INS-460R/I

MODELO	TRANSCEPTOR	FIRMWARE
INS-460R	RS-485	XIF: A2B1302000001.XIF APB: A2B1302000001.APB

2.6. NODO DE CONTROL 8 ENTRADAS INS-080RNCV3/I (ISDE-Ing, 2005)

Módulo que cuenta con 8 entradas, libres de potencial, como se observa en la Figura 19., y se detallan sus características técnicas en la Tabla 9. Está pensado para la gestión y supervisión de alarmas o sistemas eléctricos.

FIGURA 19. Nodo de control 8 entradas INS-080RNCV3/I

2.6.1. Características generales.

- Topología de conexión: Bus.
- Transceptor RS-485-78K, programación y configuración remota.
- Compatible con sistemas DOMOLON® y HOTELON®.
- Configuración horaria en tiempo real para realizar programaciones individuales.
- Insensible a la polaridad del bus y en la alimentación de 12Vcc.
- Proporciona 8 entradas libres de tensión.

2.6.2. Especificaciones funcionales.

- Las versiones con reloj incorporan un completo reloj, con segundo, minuto, día, hora, día de la semana, día del mes, mes y año con función de cambio automático Verano/Invierno.
- La versión de nuestro equipo con entradas no asiladas trabaja con elementos que proporcionen un contacto libre de potencial dando un alto grado de seguridad a la instalación.
- Soporta pulsadores estándar, así como detectores de presencia, gas, fuego, humo, etc.
- En función del firmware cargado, la funcionalidad del nodo varía.
- Se suministra una librería completa de firmware para realizar funciones típicas de control y supervisión de cuadros eléctricos, transmisión de alarma, control remoto de actuaciones, etc.
- Conectorización extraíble para facilitar la instalación y mantenimiento.

2.6.3. Características técnicas.

TABLA 9. Características técnicas Nodo INS-080RNCV3/I.

Características	Descripción
Alimentación	12 VDC
Grado de protección	IP20
Número de entradas	8 (Libres de tensión)
Protocolo de comunicación	LONTalk
Transceptor	RS-485
Velocidad de comunicaciones	78kbps
Actualización de firmware	Mediante Bus
Sujeción mecánica	Carril DIN 6U

2.6.4. Conexión eléctrica y dimensiones.

A continuación en la Figura 20., se indican las dimensiones del nodo y los bloques de conexión del mismo, así como su alimentación y sus salidas.

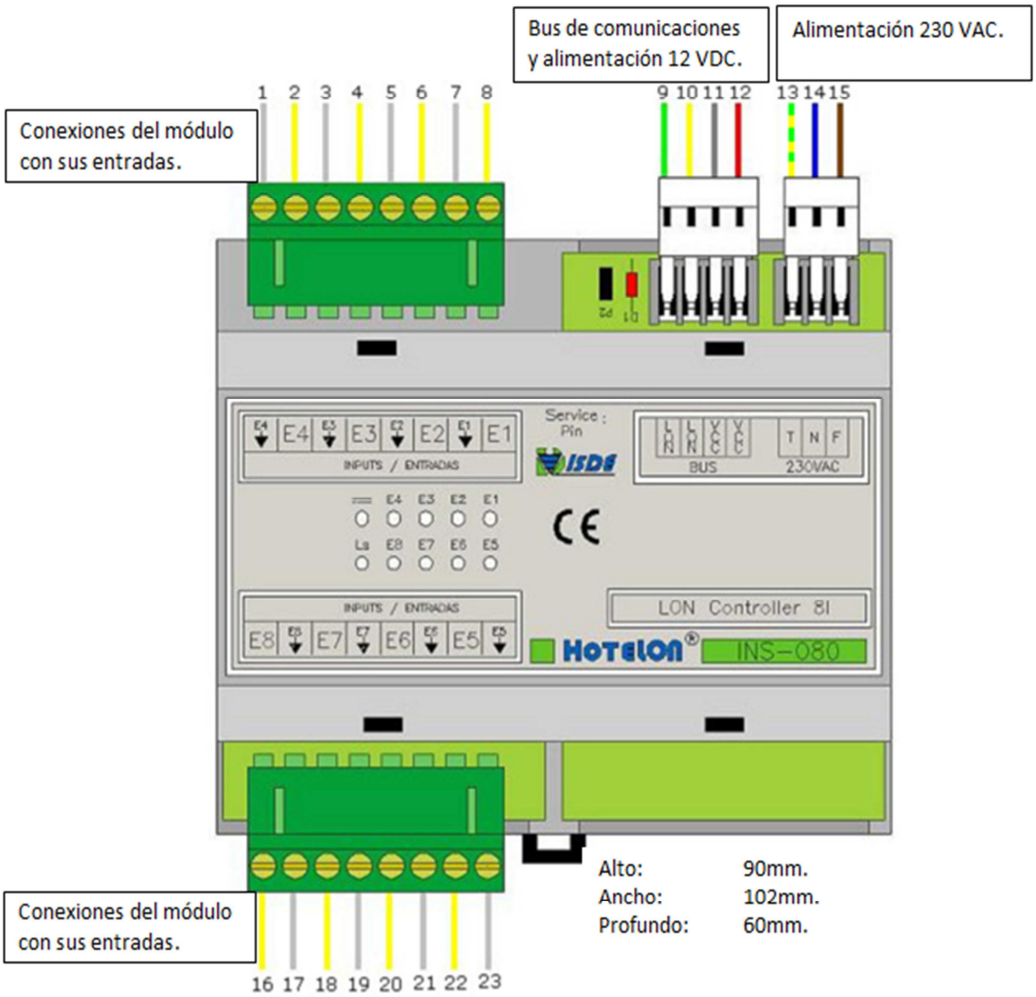


FIGURA 20. Conexiones y dimensiones del Nodo INS-080RNCV3/I.

Descripción de conexiones.

1. Común entrada 4
2. Entrada 4
3. Común entrada 3
4. Entrada 3
5. Común entrada 2
6. Entrada 2

7. Común entrada 1
8. Entrada 1
9. Comunicación LON
10. Comunicación LON
11. Alimentación Vcc
12. Alimentación Vcc
13. Tierra Alimentación
14. Neutro Alimentación 230Vac
15. Fase Alimentación 230Vac
16. Común entrada 8
17. Entrada 8
18. Común entrada 7
19. Entrada 7
20. Común entrada 6
21. Entrada 6
22. Común entrada 5
23. Entrada 5

2.6.5. Firmware.

El Firmware es el software que contiene todas las variables y parámetros de configuración posibles que se carga mediante el bus al nodo INS-080RNCV3/I.

TABLA 10. Firmware INS-080RNCV3/I

MODELO	TRANSCEPTOR	FIRMWARE
INS-080RNCV3	RS-485	XIF: A2A1300000002.XIF APB: A2A1300000002.APB

2.7. NODO DE CONTROL ESTÁNDAR 4E/2S INS-231 TR/V3 (ISDE-Ing, 2005)

Dispositivo que cuenta con 4 entradas libres de potencial y 2 salidas a relé, para el control de circuitos con un consumo máximo de 12Amp., como se observa en la Figura 21., y se detallan sus características técnicas en la Tabla 11. Cuenta con una entrada adicional para la medición de temperatura.

FIGURA 21. Nodo de control estándar INS-231TR/V3

2.7.1. Características generales.

- Topología de conexión: Bus.
- Transceptor RS-485-78K, programación y configuración remota.
- Compatible con sistemas DOMOLON® y HOTELON®.
- Insensible a la polaridad del bus y en la alimentación de 12Vcc.
- Proporciona 2 relés de conmutación de 12 A.
- Protegido contra sobreconsumos.
- Soporta sondas de agua.
- Entradas de pulsadores y sensores.

2.7.2. Especificaciones funcionales.

- Incorpora electrónica para soportar sondas de agua.
- Todas las entradas trabajan con muy baja tensión (5V) dando un alto grado de seguridad a la instalación e incrementando la vida útil de los mecanismos al conmutar pequeñas tensiones y corrientes.
- Soporta pulsadores estándar, así como detectores de presencia, gas, fuego, humo, etc.
- Incorpora 2 relés de conmutación, para circuitos de hasta 12Amp, normalmente abiertos con funciones de inversión.
- En función del firmware cargado, la funcionalidad del nodo varía.
- Se suministra una librería completa de firmware para realizar funciones típicas de control de iluminación, persianas, etc.
- Capacidad de multiproceso, posee tres procesadores independientes.
- En su configuración de fábrica soporta:
    - Encendido y apagado automático de luces por sensor de presencia en uno delos circuitos.
    - Encendido y apagado permanente de luces.

2.7.3. Características técnicas.

TABLA 11. Características técnicas Nodo INS-231TR/V3.

Características	Descripción
Alimentación	12 VDC
Consumo máximo	80 mA
Número de entradas	4 (Libres de tensión)
Número de salidas	2 (Salidas a relé)
Máxima potencia conmutada	2000w cosφ=1
Transceptor	RS-485
Velocidad de comunicaciones	78kbps
Actualización de firmware	Mediante Bus
Sujeción mecánica	Carril DIN 6U

2.7.4. Conexión eléctrica y dimensiones.

A continuación en la Figura 22., se indican las dimensiones del nodo y los bloques de conexión del mismo, así como su alimentación y sus salidas.

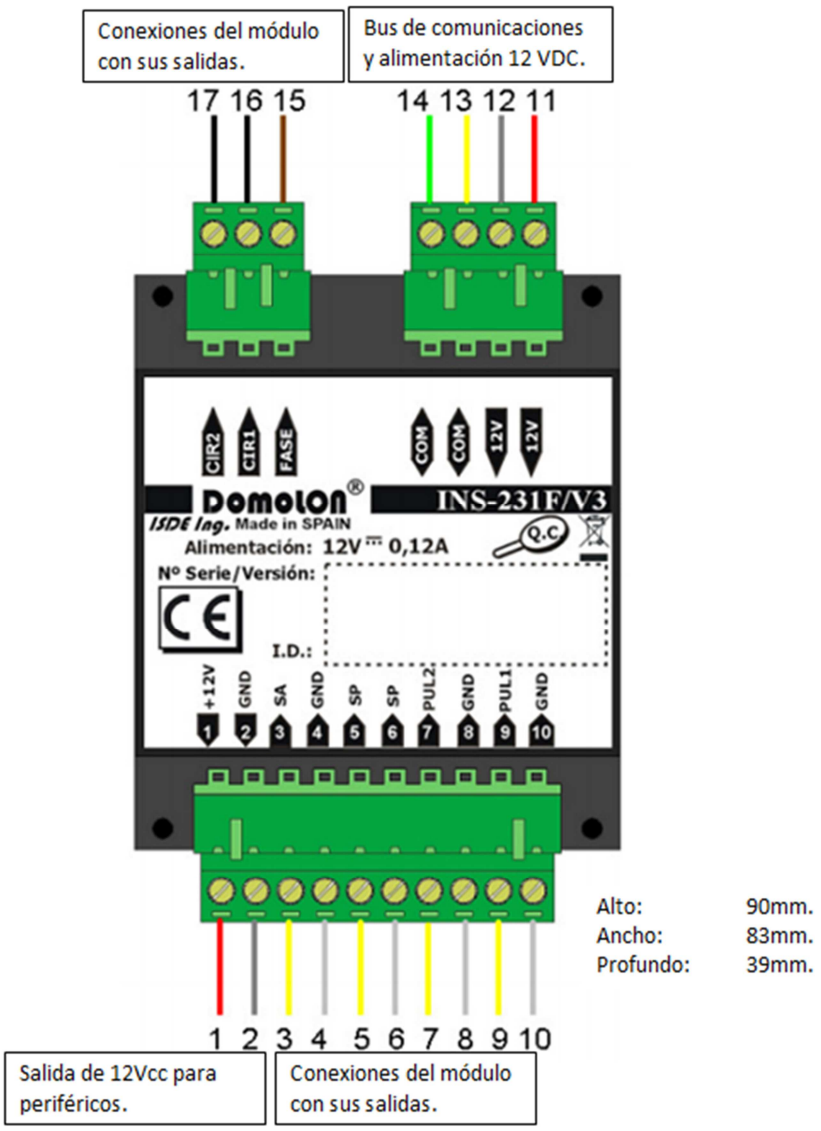


FIGURA 22. Conexiones y dimensiones del Nodo INS-231R/V3.

Descripción de conexiones. (ISDE-Ing, 2005)

1. Alimentación 12Vcc a periféricos
2. Alimentación 0Vcc a periféricos
3. Sonda de agua
4. Común sonda de agua

5. Detector de presencia
6. Detector de presencia
7. Pulsador 1
8. Común Pulsador 1
9. Pulsador 2
10. Común Pulsador 2
11. Alimentación Vcc
12. Alimentación Vcc
13. Comunicación LON
14. Comunicación LON
15. Fase de los circuitos de salida
16. Salida Circuito 1
17. Salida Circuito 2

2.7.5. Firmware.

El Firmware es el software que contiene todas las variables y parámetros de configuración posibles que se carga mediante el bus al nodo INS-231TR/V3.

TABLA 12. Firmware INS-231TR/V3

MODELO	TRANSCEPTOR	FIRMWARE
INS-231 TR	RS-485	XIF: F020700E56101.XIF APB: F020700E56101.APB

2.8. NODO TECLADO DE SEGURIDAD Y CONTROL INM-050 R/V3 (ISDE-Ing, 2005)

Dispositivo que cuenta funciones de seguridad y programación, puede abarcar cuatro zonas de vigilancia, tres de vigilancia retardada y una instantánea, indicación luminosa para conocer el estado de las zonas de vigilancia 1, 2, 3 e instantánea como se observa en la Figura 23., y se detallan sus características técnicas en la Tabla 13.

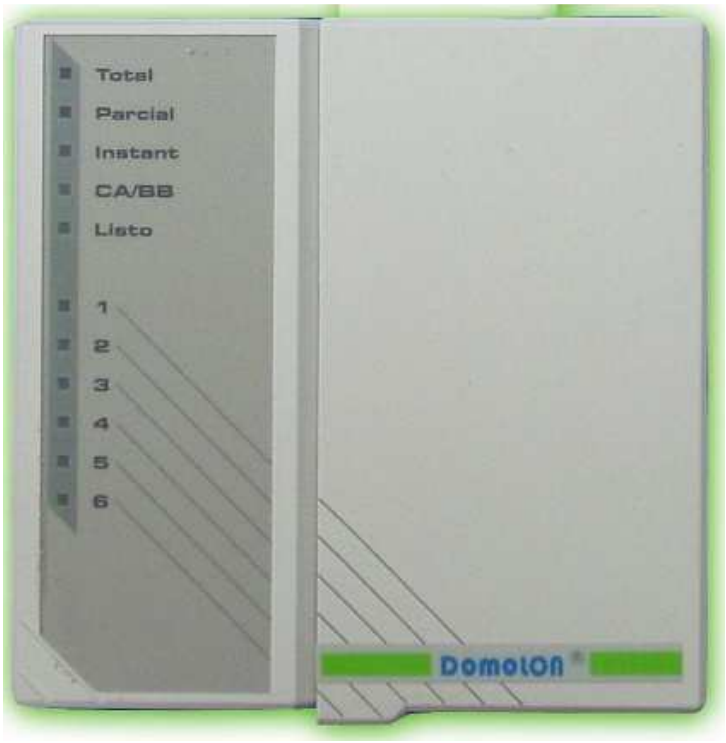


FIGURA 23. Nodo teclado de seguridad y control INM-050R/V3

2.8.1. Características generales.

- Topología de conexión: Bus.
- Transceptor RS-485-78K, programación y configuración remota.
- Compatible con sistemas DOMOLON® y HOTELON®.
- Insensible a la polaridad del bus y en la alimentación de 12Vcc.
- Función de pánico.
- Protegido contra sobreconsumos.
- Teclado de tacto suave y con retroiluminación.

- Montaje en superficie.

2.8.2. Especificaciones funcionales.

- Activación y desactivación de 1 zona instantánea.
- Activación y desactivación de tres zonas de vigilancia de forma total o parcial.
- Código de pánico.
- Funciones de programación de código de usuario, servicio y pánico.
- Bloqueo automático del teclado por introducción de tres códigos errados.
- Indicación luminosa para estado de zonas de vigilancia.

2.8.3. Características técnicas.

TABLA 13. Características técnicas Nodo INM-050R/V3.

Características	Descripción
Alimentación	12 VDC
Consumo máximo	50 mA
Señalización	Por diodos LED
Transceptor	RS-485
Velocidad de comunicaciones	78kbps
Actualización de firmware	Mediante Bus
Sujeción mecánica	Superficie

2.8.4. Conexión eléctrica y dimensiones.

A continuación en la Figura 24., se indican las dimensiones del nodo y los bloques de conexión del mismo, así como su alimentación y sus salidas.

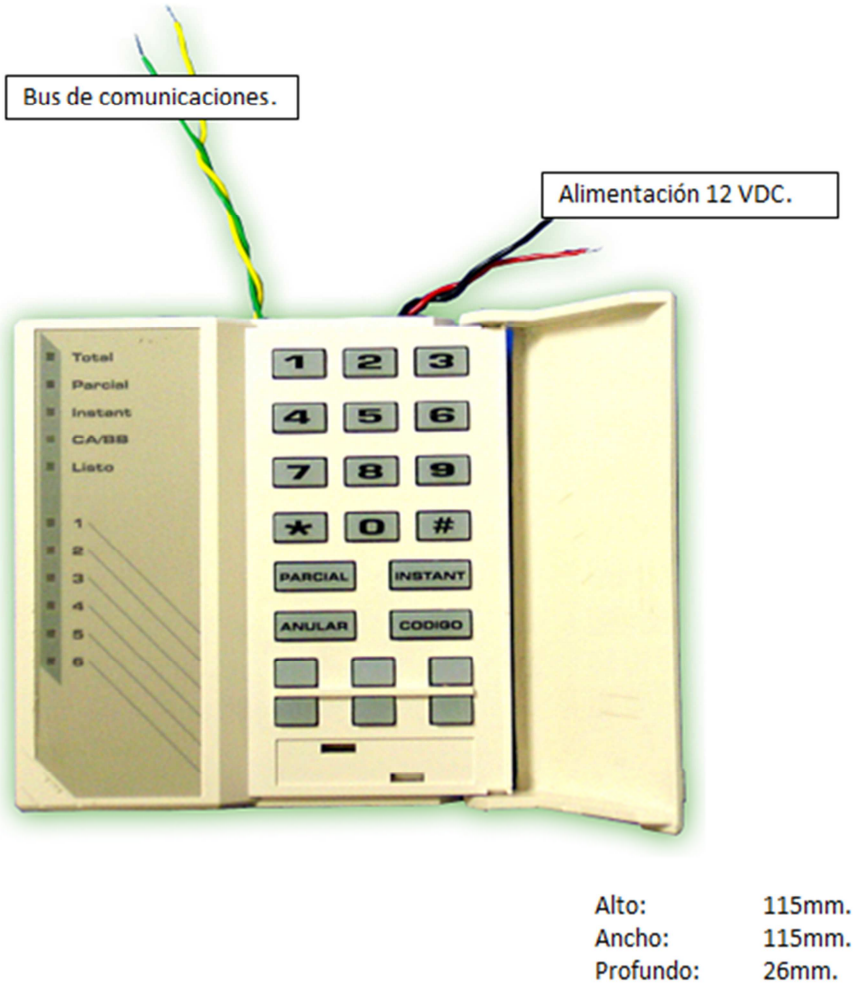


FIGURA 24. Conexiones y dimensiones del Nodo INM-050R/V3.

2.8.5. Firmware.

El Firmware es el software que contiene todas las variables y parámetros de configuración posibles que se carga mediante el bus al nodo INS-231TR/V3.

TABLA 14. Firmware INM-050R/V3

MODELO	TRANSCEPTOR	FIRMWARE
INM-050R	RS-485	XIF: A070701000101.XIF APB: A070701000101.XIF

2.9. DISPOSITIVOS PERIFÉFICOS.

Los dispositivos periféricos son los terminales, sensores o actuadores que realizan la función de indicar a la red LON el estado de la variable que cada uno de éstos esté controlando, ya sea presencia, humo o ruptura de cristal.

2.9.1. Detector de presencia.

El sensor de presencia elegido es montable en superficie como se puede observar en la figura 25., ya que todas las instalaciones civiles están concluidas.

FIGURA 25. Detector de presencia de superficie.

Características técnicas.

TABLA 15. Características técnicas del detector de presencia.

Características	Descripción
Alimentación	12VDC
Ángulo de detección	110º
Rango de detección	11m
Grado de protección	IP 44[1]

[1] Protegido contra el ingreso de objetos sólidos de hasta 1mm de diámetro y Protección contra salpicaduras de agua desde cualquier dirección.

Características funcionales.

- Sensor de luz integrado para regular funcionamiento.
- 3 botones de ajuste: sensibilidad, tiempo, luminosidad.

2.9.2. Detector de humo.

El detector de humo seleccionado para la implementación cuenta con un sensor fotoeléctrico y es montable en superficie.

FIGURA 26. Detector de humo de superficie.

Características técnicas.

TABLA 16. Características técnicas del detector de humo.

Características	Descripción
Alimentación	9-12VDC
Consumo	6mA
Indicación óptica	LED rojo
Grado de protección	IP 42[2]

[2] Protegido contra el ingreso de objetos sólidos de hasta 1mm de diámetro y Protección contra el goteo de hasta 15º de la vertical.

Características funcionales.

- Autochequeo automático de la valoración de humo.
- Pulsador de prueba incorporado para comprobación de funcionamiento.

2.9.3. Detector de ruptura de cristal o discriminador de ruido.

Este dispositivo está orientado a detectar una frecuencia sonora mayor a la programada y transmitir una señal de alerta al sistema de seguridad lo cual permitiría una activación temprana del sistema ante un ruido producido por un intento de ruptura de una ventana, por lo cual su ubicación será en frente de la fuente del sonido y lo más cerca del suelo.

FIGURA 27. Discriminador de ruido.

Características técnicas.

TABLA 17. Características técnicas del discriminador de ruido.

Características	Descripción
Alimentación	9-16VDC
Consumo	15mA
Cobertura máxima	9m Alta sensibilidad
Cobertura mínima	4,5m Baja sensibilidad

Características funcionales.

- Dos modos de funcionamiento, direccionable o con activación de relé.
- Alta inmunidad a señales de radiofrecuencia y electromagnéticas.
- Sensibilidad ajustable, configurado con su máxima sensibilidad cubre hasta 9 metros, mientras que configurado con su sensibilidad más baja es capaz de cubrir hasta 4.5 metros.
- Interruptor anti sabotaje como mecanismo de protección.

2.9.4. Sirena electrónica.

Este dispositivo permitirá mediante su fuerte emisión sonora advertir de la activación o violación del sistema de seguridad. Por lo cual se instalarán dos una interna para advertir al personal en horario de oficina y otra externa que advierta a las autoridades o a la comunidad.

FIGURA 28. Sirena electrónica.

Características técnicas.

TABLA 18. Características técnicas de la sirena electrónica.

Características	Descripción
Alimentación	12VDC
Consumo	300mA
Presión sonora	115dB
Frecuencia	2,4 a 4,2 kHz

2.10. GRABADOR DIGITAL DE VIDEO.

El Grabador Digital de Video o DVR escogido tendrá 8 canales de entrada y 3 Terabytes de capacidad de almacenamiento. Además mediante contactos secos como entradas, tiene la capacidad de comandar cada una de las cámaras conectadas a éste.

a)

b)

FIGURA 29. a) Vista frontal del DVR. b) Vista posterior del DVR.

Características técnicas.

TABLA 19. Características técnicas del DVR.

Características	Descripción
Alimentación	120 VAC
Número de canales de video	16 Ch
Capacidad del HDD	3 Tb
Entradas de audio	1
Entradas de alarma	16 Contactos secos
Salidas de alarma	4 Contactos secos
Puertos USB 2.0	2

Características funcionales.

- Video compresión avanzada H.264.
- Entradas de audio para todos los canales.
- Envío de Email de alarma con imagen.
- Opción para seleccionar el número de días a grabar.
- Reproducción simultánea de las 8 cámaras.

2.11. Cámaras análogas.

Estas cámaras serán instaladas en puntos críticos de las instalaciones de SRT HARDCOM S.A., y serán comandadas mediante contactos secos conectados al DVR generados por la red LON.

FIGURA 30. Cámara análoga.

Características técnicas.

TABLA 20. Características técnicas de la cámara análoga.

Características	Descripción
Alimentación	12 VDC
Salida	Conector BNC- Cable coaxial
Sensor de imagen	1/3 ¨ HDIS
Píxeles efectivos	720(H) x480(V)
Grado de protección	IP 66 [3]
Alcance de LED´s IR	20m
Iluminación mínima	0,1 Lux/ 0 Lux IR encendido

[3] Protegido contra el ingreso de polvo y contra chorros de agua desde cualquier dirección.

Características funcionales.

- Cámara análoga especialmente para exteriores ya que posee un grado de protección IP 66, que le brinda protección contra el ingreso de polvo o agua.
- La sujeción mecánica es por medio de tornillos y puede estar montada sobre pared o tumbado teniendo en cuanta que no tenga fuentes luminosas cerca porque esto podría deteriorar la calidad de la imagen.
- El alcance de sus LED´s IR, es de hasta 20 metros que permiten a la cámara con una luminosidad de 0 lux captar la imagen a la que se encuentra enfocada.

CAPÍTULO III.

DISEÑO DE LA INTERFAZ.

3.1. MEDIO DE TRANSMISIÓN.

Como se ha mencionado este protocolo es independiente del medio de transmisión por lo cual se deberá adoptar el medio de transmisión que más se acople o sea el más conveniente de acuerdo a las necesidades de la aplicación, a continuación se muestra en la tabla 21., los tipos de medios de transmisión que se pueden tomar en cuenta.

TABLA 21. Tipos de medios de transmisión.

NOMBRE	CANAL	DESCRIPCIÓN
Par trenzado	TP/FT-10	- La velocidad de transmisión es de 78 kbps. - La topología es libre. - La máxima distancia entre dispositivos en topología libre es de 500 metros. - Puede transmitir 144/168 paquetes por segundo.
	RS-485	- La velocidad de transmisión es de 35 Mbps hasta 10 metros y de 100 kbps en 1200 metros. - La topología es de bus.
Red eléctrica	TP/LPT-10	- La velocidad de transmisión es de 5 kbps. - Requiere una fuente acoplada regulada. - Puede transmitir hasta 20 paquetes por segundo.
Radio frecuencia	RF-10	- Puede alcanzar grandes distancias.

En este caso se adoptará y se implementará el canal TP/FT-10.

3.2. INTERFAZ DE RED IAUSB-F.

El dispositivo a utilizar que soporta el canal de comunicación TP/FT-10 es el modelo IAUSB-F de marca Echelon como se muestra en la figura 31., y se presentan sus características técnicas en la tabla 22.

FIGURA 31. Interface de red IAUSB-F.

3.2.1. Características generales.

- Soporta canal de LONWorks de par tranzado FTT-10 de topología libre.
- Transceptor FTT-10.
- Compatible con sistemas DOMOLON® y HOTELON®.
- Rendimiento de procesamiento y funcionamiento más altos posibles de la red.

3.2.2. Características técnicas. (U10/U20 USB Network Interface, 2006)

TABLA 22. Características técnicas Interfaz de red IAUSB-F.

Características	Descripción
Transceptor	FTT-10
Velocidad de comunicaciones	78kbps
Compatibilidad USB	Compatible con el certificado USB 2.0. Compatible con USB 1.1 y sistemas USB de alta velocidad, periféricos y cables.
Indicadores luminosos	Servicio (Ámbar), Transmitir (Verde), Recibir (Verde).

3.3. INTERCAMBIO DINÁMICO DE DATOS (DDE).

Es un protocolo creado por Microsoft para que aplicaciones compatibles con éste puedan compartir información.

Las aplicaciones DDE están clasificadas en cuatro categorías: cliente, servidor, cliente/servidor y monitor. Una comunicación DDE siempre tiene lugar entre una aplicación cliente, que la inicia, y una aplicación servidor. La aplicación cliente solicita datos o servicios a una aplicación servidor y ésta responde, positiva o negativamente a la petición. Para lograr la comunicación entre aplicaciones la aplicación cliente debe conocer los pedidos de los que dispone la aplicación servidor que por lo general no son estandarizados. En una aplicación cliente/servidor coexisten ambas cualidades, es decir la misma solicita y suministra información. Mientras que una aplicación monitor es capaz de interceptar mensajes dirigidos a otras aplicaciones, aunque no puede tener acceso a ellos.

La aplicación “Servidor” para comunicar nuestra red LONWorks con la interfaz Humano Máquina se denomina LNS DDE SERVER desarrollada por la compañía ECHELON®.

3.3.1. Servidor LNS DDE.

El Servidor LNS DDE, es un paquete de software que permite a cualquier aplicación compatible con el sistema operativo Windows® monitorear y controlar a una red de control LONWORKS®.

Aplicaciones típicas para el Servidor LNS DDE incluyen interfaces con aplicaciones HMI, ingreso de datos, y procesos gráficos. LNS es el sistema operativo estándar para las redes LONWORKS. Basado en una poderosa arquitectura, LNS permite acceso simultáneo a múltiples instaladores o personal de mantenimiento para la modificación de una base de datos común. Mediante el enlace LNS y el protocolo DDE de Microsoft,

aplicaciones Windows compatibles con DDE pueden interactuar con dispositivos LONWorks mediante cualquiera de los siguientes métodos:

- Leer, monitorear y modificar el valor de cualquier variable de red.
- Supervisar y cambiar propiedades de configuración.
- Recibir y enviar mensajes en la aplicación.
- Evaluar, habilitar, deshabilitar y anular objetos LONMark.
- Evaluar y controlar dispositivos.

El servidor LNS DDE conecta redes LONWorks con interfaces para el control de sistemas en edificios, fábricas, plantas de procesamiento y otras aplicaciones industriales y comerciales.

Este software es compatible con aplicaciones “Cliente” tales como: Wonderware InTouch®, Intellution Fix®, USDATA Factory Link®, National Instruments Lab View and Bridge View® y adicionalmente con otros cientos de aplicaciones DDE. El servidor LNS DDE también soporta los protocolos SuiteLink y FastDDE de Wonderware para un desempeño mejorado con InTouch.

3.4. WONDERWARE INTOUCH.

3.4.1. Generalidades.

El software InTouch creado por la compañía Wonderware®, ofrece funciones de visualización gráfica, gestión de operaciones, control y optimización, todo esto conocido como HMI “Interfaz Humano - Máquina”.

Ningún otro HMI puede compararse con InTouch en términos de innovación, integridad de arquitectura, conectividad e integración de dispositivos.

Esto se traduce en sistemas basados en estándares que permiten incrementar al máximo la productividad, optimizar la efectividad del usuario, mejorar la calidad y reducir los costos operacionales, de desarrollo y mantenimiento. (Wonderware®, 2009)

FIGURA 32.Ejemplo de interfaz con Wonderware InTouch.

Este software es capaz de integrarse prácticamente con cualquier sistema de automatización, unidad terminal remota (RTU), dispositivos electrónicos

inteligentes (IED), controladores lógicos programables (PLC) o bases de datos.

Los beneficios al utilizar esta tecnología son muchos de los cuales se puede destacar:

- Posee gran capacidad de integración de dispositivos y conectividad a prácticamente todos los dispositivos y sistemas.
- Sus capacidades de representación gráfica y la interacción con sus operaciones permiten entregar la información correcta a las personas correctas en el momento correcto.

Si se habla de sus beneficios no se puede dejar de lado sus capacidades:

- Gráficos y símbolos que visualmente dan vida al sistema sobre el cual se necesita realizar el control, o su gestión.
- Alarmas distribuidas en tiempo real con visualización histórica que permite realizar su análisis.
- Librería gráfica con más de 500 objetos prediseñados y personalizables.

3.4. REQUERIMIENTOS PARA EL HMI.

3.4.1. Requerimientos del usuario.

Al usuario le interesa tener una interfaz en la cual pueda monitorear todas las regiones de sus oficinas ya sea mediante indicadores en la interfaz como en video en tiempo real, además de controlar los accesos a espacios de interés.

3.4.2. Requerimientos de aplicaciones.

Aplicación “LNS DDE Server”.

- **Requerimientos de Hardware (Recomendado).**

- Procesador: Pentium II (450 Mega Hertz) o más veloz.
- Memoria RAM: 256 Mega Bytes.

- Disco duro: Al menos 20 Mega Bytes disponibles.
- CD-ROM o DVD drive para instalación.
- Periféricos: Teclado y mouse.

- **Requerimientos de Software (Mínimo).**

- Sistema operativo Windows 2000 o XP.

Aplicación "Wonderware InTouch".

- **Requerimientos de Hardware (Recomendado).**

- Procesador: Velocidad de 1.2 Giga Hertz o más veloz ya sea de 32 o 64 bits.
- Memoria RAM: Capacidad de 1 Giga Bytes.
- Disco Duro: Al menos 4 Giga Bytes libres para sistema operativo de 32 bits y al menos 6 Giga Bytes libres para sistema operativo de 64 bits.
- Resolución de video: Adaptador de video Súper VGA (1024x768) o mayor.
- CD-ROM o DVD drive para instalación.
- Periféricos: Teclado y mouse.

- **Requerimientos de Software (Mínimo).**

- Sistema operativo Windows XP Service Pack 3.

3.5. CONSIDERACIONES EN EL DISEÑO DE LA HMI. (Pere Ponsa, 2009)

Para el diseño de la interfaz se seguirán las directrices recomendadas por la guía ergonómica de diseño de interfaces de supervisión (GEDIS), esta guía indica diez pasos a seguir para la consecución de la interfaz tales como la arquitectura, navegación, colores, fuentes, simbologías, etc., de las cuales solamente pueden ser aplicados 7 de los 10 pasos ya que no se trata de una interfaz que detalle un proceso, y éstos se detallarán a continuación.

Arquitectura y Navegación.

En esta etapa se definirán de manera general todas las pantallas con las que contará la interfaz. Este mapa deberá establecer las relaciones lógicas que cada una de las pantallas tendrá con las demás de manera que posteriormente ayude con el diseño de la navegación del sistema.

Por tanto la interfaz contará con 11 pantallas distribuidas y relacionadas de la siguiente manera:

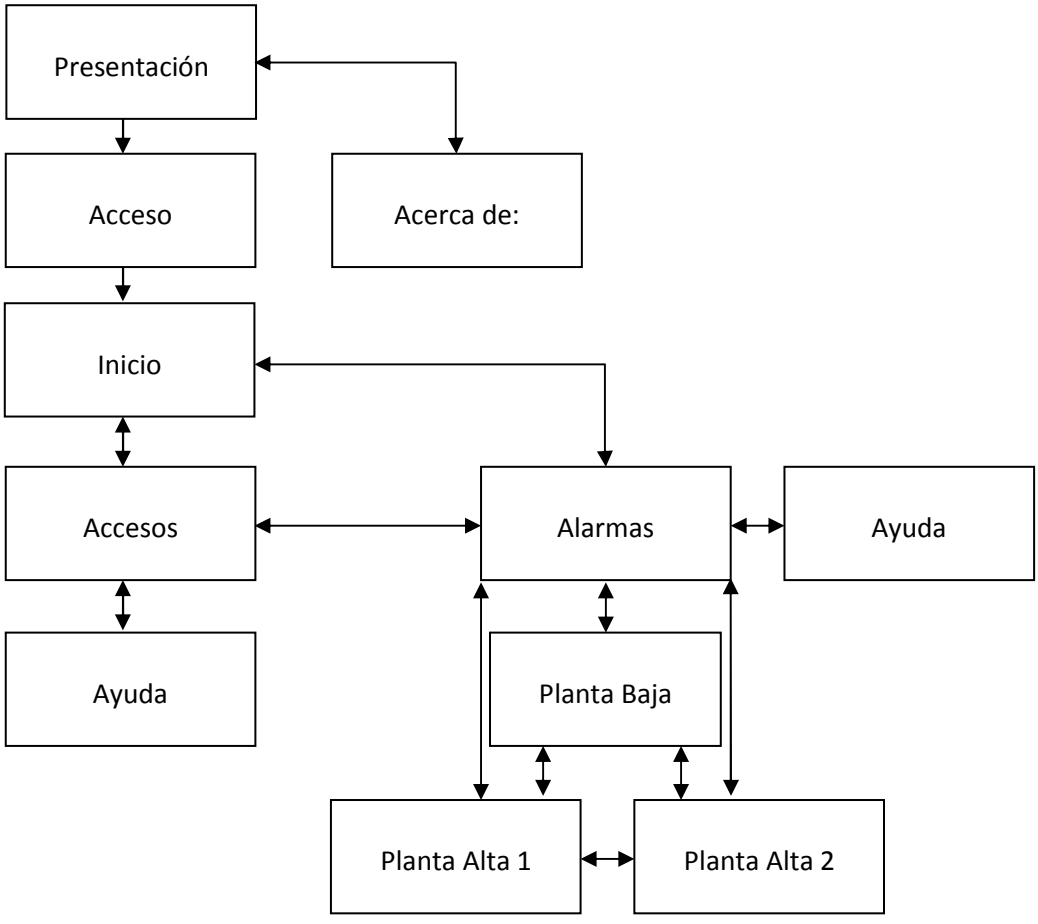


FIGURA 33. Arquitectura de la Interfaz.

Distribución de Pantalla.

En la distribución de la pantalla se definirá dónde va a ir cada elemento gráfico que constituirá la interfaz así como la generación de plantillas que se utilizarán para todas las pantallas.

Para esta interfaz se contará con 3 plantillas y 11 pantallas independientes. Por tanto las plantillas a usarse se definirían para Ayuda, Accesos y Alarmas.

En la plantilla para ayuda se ha distribuido como se puede observar en la figura 34., en la parte superior el título de la pantalla, bajo éste sobre que trataría la ayuda descrita en esta pantalla y bajo este subtítulo dos particiones, a la izquierda el elemento u objeto que puede ser la representación de un dispositivo o simplemente un botón y en la partición derecha se describe a mencionado elemento de manera comprensible para el usuario de la interfaz. Finalmente en la parte inferior de la pantalla un botón que le permitirá al usuario volver a la pantalla desde la cual solicitó la ayuda.

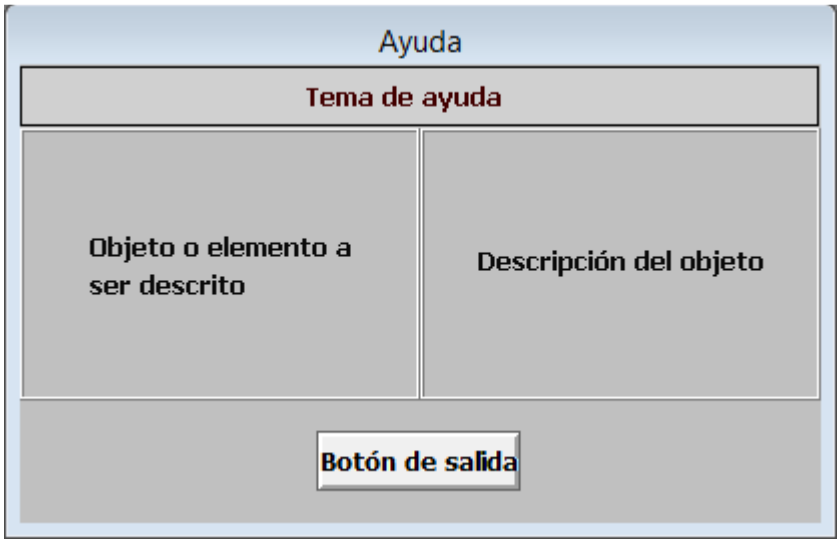


FIGURA 34. Plantilla para pantallas de Ayuda.

Para la pantalla de control de accesos se usará el modelo mostrado en la figura 35., el cual en su título muestra Accesos, bajo el título la pantalla se

divide en dos particiones debido a que solamente en dos sectores se realizará el control de accesos, los cuales llevarán por subtítulos de la pantalla el nombre del sector al cual corresponda. Dentro de estas particiones irán los mímicos de cada uno de estos sectores y bajo cada uno de estos su panel de control desde donde se realizará la apertura del acceso según corresponda. Mientras que en la parte inferior en la zona central se ubicará el panel de navegación que permitirá acceder a ventanas de alarmas o ayuda.

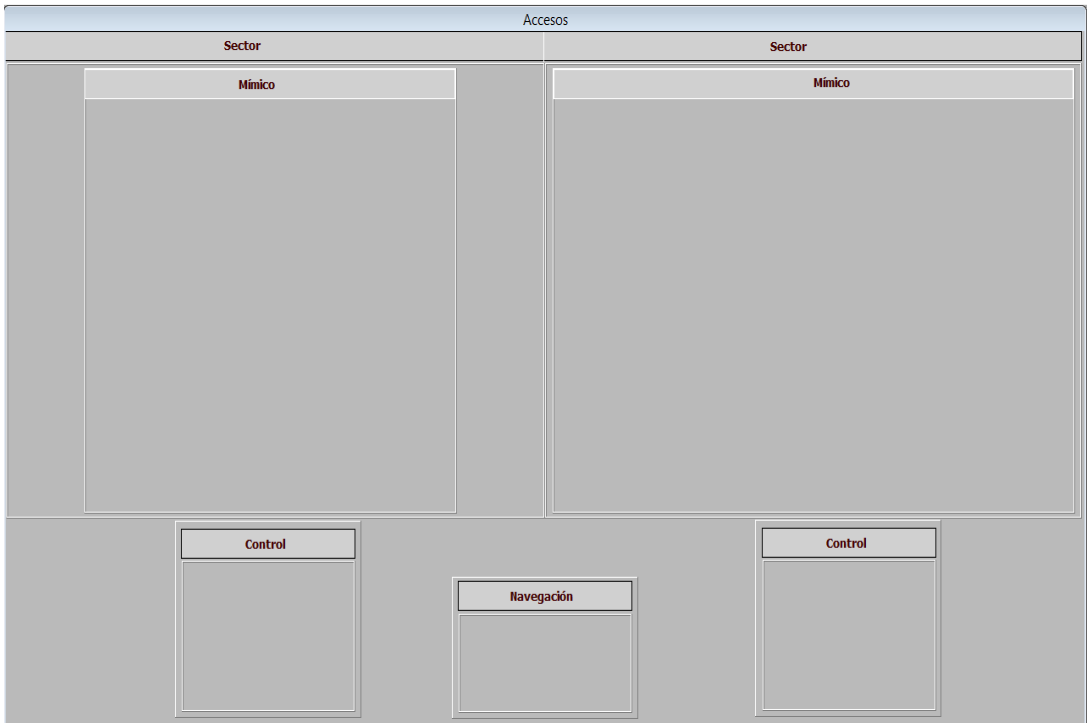


FIGURA 35. Plantilla para pantalla de Accesos.

La tercera plantilla será para las pantallas de alarmas, habrá tres pantallas de alarmas, una por cada planta. Estas contarán al igual que las anteriores, con un título denominado Alarmas (figura 36), más un número que indicará el número de planta que se está monitoreando. Bajo el título se tendrá el mímico de la planta que se está supervisando, en la zona inferior central se ubicará el panel de navegación y en sus costados se mostrará la Leyenda de los símbolos que se observarán en el mímico para un rápido

discernimiento del operador sobre lo que esté sucediendo según en las instalaciones de la empresa.

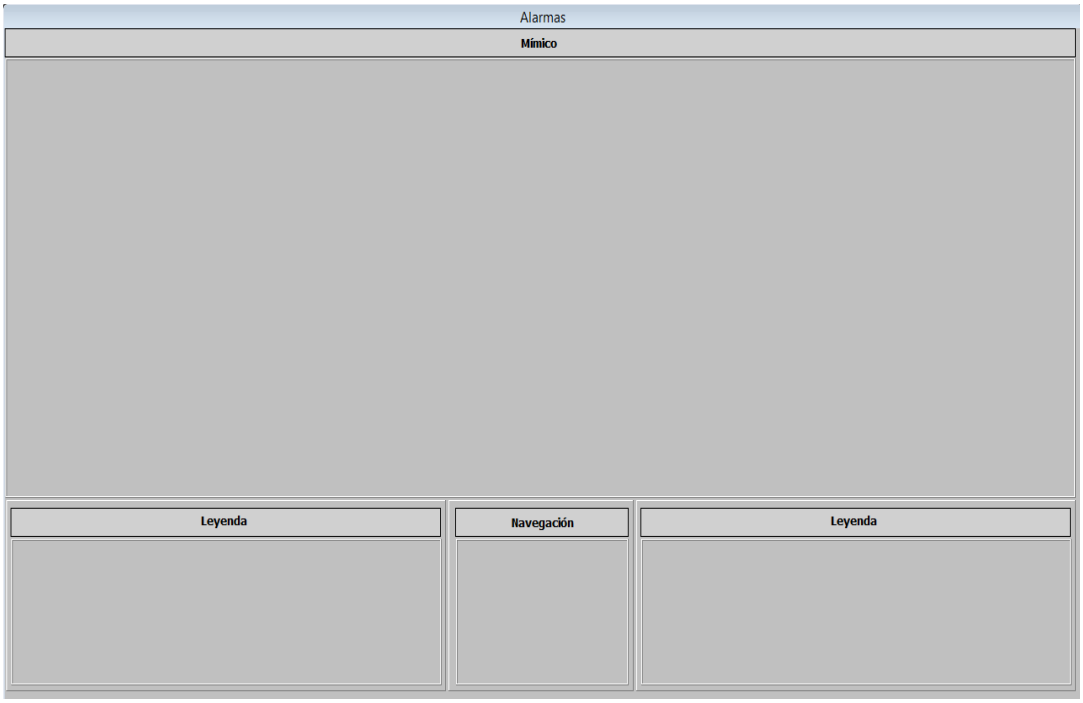


FIGURA 36. Plantilla para pantallas de Alarmas.

Uso del Color.

Siendo el color uno de los elementos más importantes que componen la interfaz la combinación de estos debe ser la adecuada de modo que no ocasione cansancio a la vista del operario, por tanto los colores a usarse deben ser compatibles en sus contrastes, por ejemplo no usar combinaciones como rojo con azul, rojo con verde o azul con amarillo ya que no se distinguirían adecuadamente los bordes y las delimitaciones de los objetos.

A continuación se determinarán los colores a utilizarse en las diferentes pantallas.

- **Color de cuadros de texto:** Azul con bordes negros.

FIGURA 37. Ejemplo de color para cuadro de texto.

- **Color de texto:** Blanco para subtítulos (dentro de cuadros de texto azul), y negro para texto en general.

FIGURA 38. Ejemplo de color para de texto.

- **Color del fondo de pantalla:** En todas las pantallas se utilizará el color Gris.
- **Color representativo de estado de dispositivos:** Cada uno de los dispositivos junto a su símbolo contará con un círculo relleno el cual indicará el estado del dispositivo. El color verde indicará que el dispositivo periférico se encuentra en línea mientras que el color rojo indicaría que el dispositivo se encuentra alarmado, como se puede observar en la figura 39.

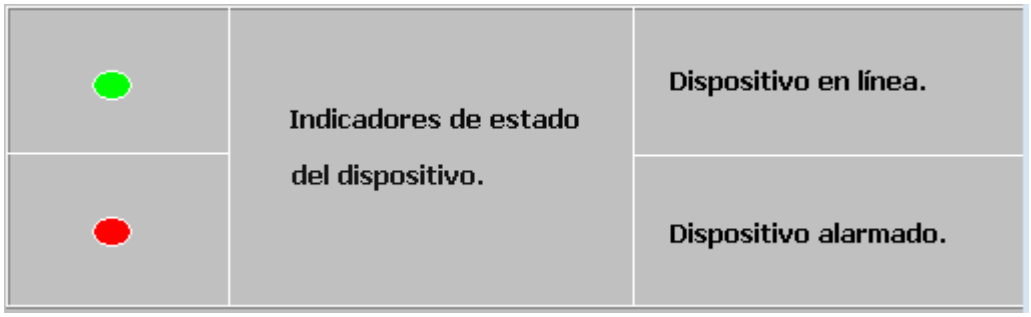


FIGURA 39. Ejemplo de color para estado de dispositivos.

- **Color de fondo de los mímicos:** En el caso de los mímicos se utilizará el color negro debido a que la mayoría del tiempo el operario se encontrará observando una pantalla que contenga mímicos y el color negro no causará cansancio visual al operario.

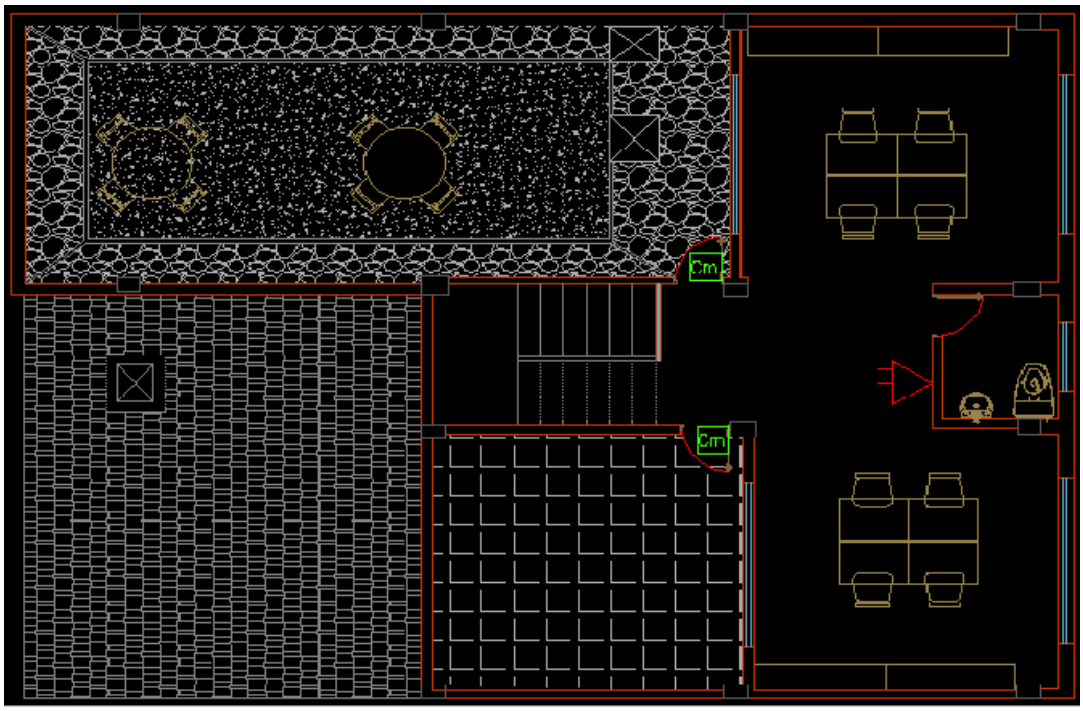


FIGURA 40. Ejemplo de color para fondo de mímicos.

- **Color de botones:** El color de los botones será gris claro de modo que contraste del color del fondo de pantalla y su texto de color negro.

FIGURA 41. Ejemplo de color para botón y su texto.

Información Textual

Por lo general la información que genera el sistema es mediante texto por lo cual se debe definir sus características las cuales serían: el uso de fuentes, el tamaño del texto, la alineación, el espaciamiento, los acrónimos y las abreviaturas.

La guía ergonómica de diseño de interfaces de supervisión nos da las siguientes directrices:

- No usar más de tres fuentes en la interfaz
- No usar más de tres tamaños de la misma fuente

- Un tamaño de fuente menor a 8 es difícil de leer a distancia por el operario
- No usar letras mayúsculas en todas las letras del texto, se deben combinar con minúsculas
- El color del texto debe contrastar con su fondo y se debe respetar el código antes definido.
- Usar el mismo color en todo el texto y no solo en ciertos caracteres
- Espaciar el texto tanto horizontalmente como verticalmente para evitar aglutinamientos

De acuerdo a estas directrices la fuente seleccionada para todo el texto de la interfaz es “Tahoma”, con estilo de fuente “Negrita” (figura 42), para que contraste de mejor manera y sean más visibles cada uno de los caracteres sobre su fondo y de tamaño de fuente 10.

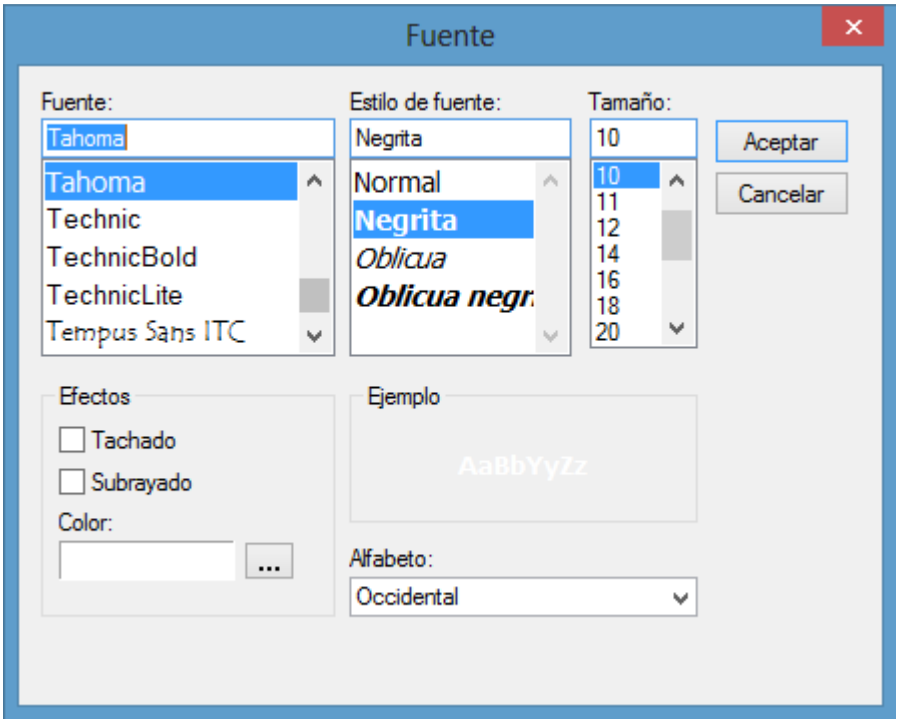


Figura 42. Fuente de texto de la interfaz.

Estados de los Equipos y dispositivos

En esta etapa se definirá el estándar gráfico de símbolos e íconos que representan a los diversos dispositivos del sistema de seguridad como son: sensores de movimiento, sensores de humo, contactos magnéticos, lectores de proximidad, cerraduras electromagnéticas o sirenas.

Gedis también dicta directrices en cuanto al diseño de estos símbolos:

- Los símbolos deben ser simples y de un tamaño suficientemente visible
- Se deben evitar detalles y realismo innecesarios
- Utilizar figuras geométricas simples para definir los símbolos e íconos
- De darse el caso, se puede reforzar la señalización del estado del dispositivo con un texto que también lo indiquen.

Figura 43. Ejemplo de dispositivo en línea (Izquierda), alarmado (derecha).

Comandos e Ingreso de datos

Aquí se establece cómo va a realizar la intervención el operador al suministrar datos al sistema de manera que éste se comporte de acuerdo a sus objetivos. Las operaciones que realiza el usuario son las de ejecutar comandos, seleccionar opciones o introducir datos. Las características principales que deben cumplir los comandos son su visibilidad y su facilidad de operación y para lograr esto se puede conseguir de la siguiente manera:

- Los comandos deben estar claramente etiquetados
- El área de acción sobre el comando debe ser lo suficientemente grande como para que sea fácilmente operado
- Los diferentes tipos de comandos deben representarse siempre con los mismos tipos de botones para que el operador los identifique rápidamente

- El operador debe ser retroalimentado inmediatamente sobre el resultado de su acción

Dentro de los comandos e ingreso de datos en la interfaz del sistema solamente se tiene un espacio para el ingreso de datos, que es destinado para el ingreso de la contraseña que permitirá el acceso total a la interfaz. En cuanto a los comandos que ejecutará el operador serán para la apertura remota de las puertas, tanto para la puerta de acceso principal como para la de la bodega principal.

3.6. Aplicación en Wonderware® InTouch.

Dentro de lo que a la aplicación respecta, Wonderware® InTouch, será utilizado para realizar todo el diseño de la interfaz de control y supervisión del sistema de seguridad conjuntamente con el Servidor LNS DDE creado por la compañía ECHELON.

Nuevamente tomando como guía a GEDIS iniciamos con el diseño de las pantallas.

Tendremos inicialmente la pantalla de presentación, figura 44.

Figura 44. Pantalla de presentación de Interfaz.

Como se puede observar en la figura, inicialmente cumplimos con la distribución de la pantalla, teniendo un título de pantalla en la parte superior y un submenú asociado a la pantalla en cual nos permitirá acceder a la interfaz de control o darnos una introducción sobre la interfaz a manera de “Acera de:”. En cuanto al uso del color el texto de color blanco contrasta perfectamente con el fondo azul del cuadro de texto. La pantalla que se muestra en la figura 45, aparecerá si se oprime el botón “Ayuda”, en la pantalla de presentación.

Figura 45. Pantalla “Acerca de:”, información de la interfaz.

Esta pantalla informa de manera general al operador sobre que se trata la interfaz a la que va a ingresar, para qué empresa se ha desarrollado el proyecto y quién ha diseñado el proyecto.

Volviendo a la pantalla “Presentación” (figura 44.). Si se oprime el botón acceder nos aparecerá la pantalla que se muestra en la figura 46., en la cual nos pedirá la clave de acceso y aparecerá el botón de ingreso si y solo si la contraseña es la correcta.

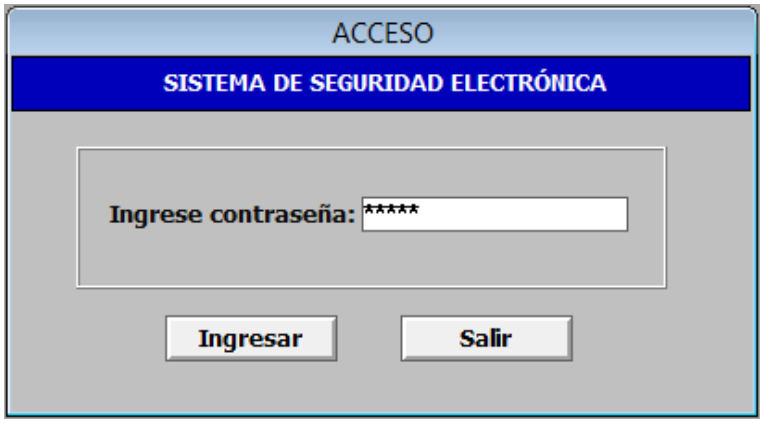


Figura 46. Pantalla “Acceso”.

En esta pantalla se mantiene el uso del color, texto blanco con fondo azul, y en la distribución de pantalla destaca claramente donde el operador debe introducir los datos y los botones asociados a la ventana le permiten ingresar a la interfaz si la contraseña ingresada es la correcta o salir nuevamente a la pantalla “Presentación”.

En esta pantalla “Acceso”, se tiene la opción de ingresar, accediendo a la interfaz nos aparecerá la pantalla de navegación principal, figura 47., a la cual se la ha denominado “Inicio”.

Figura 47. Pantalla “Inicio”.

Esta pantalla ofrece dos opciones, ingresar al sistema de accesos y operarlo, ingresar al sistema de alarmas y supervisarlo u obtener información sobre cada uno de los sistemas antes de acceder a ellos. Como se puede observar el uso del color es una constante el texto blanco contrastado con el fondo azul, en la mitad de esta pantalla los botones de navegación separados por divisiones y en la parte inferior un botón de ayuda.

Al oprimir el botón de ayuda nos aparecerá la siguiente pantalla:

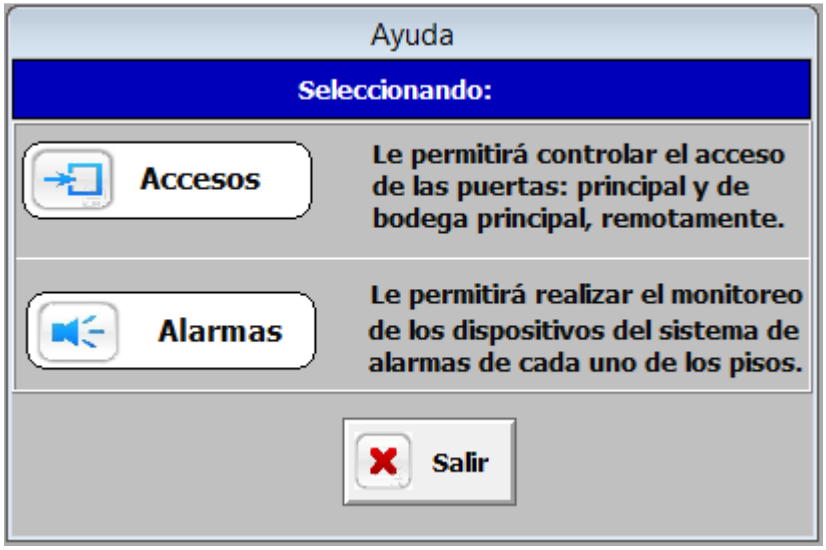


Figura 48. Pantalla “Ayuda”, para selección de sistema.

Esta pantalla nos brinda información general acerca de cada uno de los sistemas y lo que puede realizar el operador sobre cada uno de ellos.

Oprimiendo el botón salir en la pantalla de la figura 48., volverá a la pantalla “Inicio”, para nuevamente ofrecernos las opciones de sistema de accesos o sistema de alarmas.

Pulsando el botón “Ingresar” del área del sistema de accesos, nos aparecerá la pantalla que muestra la figura 49., la cual ya ocupa la pantalla completa y donde se puede observar que se cumple con la distribución de la pantalla propuesta anteriormente en el siguiente orden, área de subtítulos, área de mímicos, área de control y área de navegación.

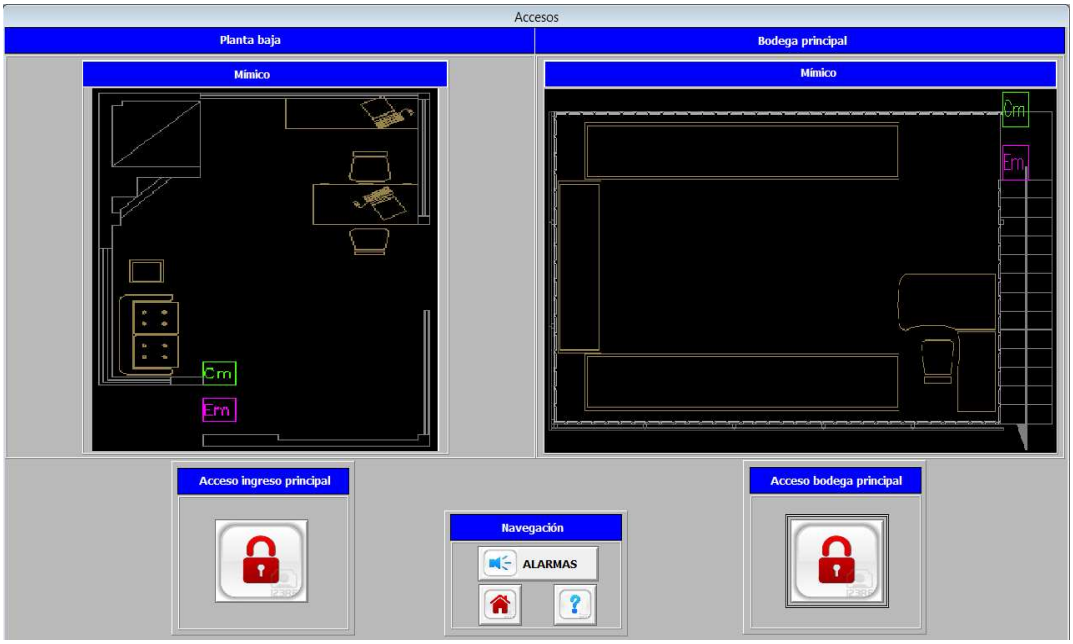


Figura 49. Pantalla “Accesos”.

En esta pantalla como se observa claramente en cuanto al uso del color todos los subtítulos son de color blanco contrastado con un fondo azul, además se tienen botones de comandos claramente identificados para la apertura remota de las puertas de acceso principal y la puerta de la bodega principal.

En la zona inferior central se tienen los botones de navegación, el superior denominado accesos y dos inferiores en la izquierda el botón de inicio y a la derecha el botón de ayuda. El primero, denominado accesos nos mostrará un nuevo submenú, mostrado en la figura 52., donde podremos escoger la planta donde deseamos realizar la supervisión del sistema de alarmas.

El al pulsar el botón de inicio en la pantalla “Accesos”, nos volverá a la pantalla mostrada en la figura 48., donde podríamos si se quiere volver a ingresar al sistema de accesos, escoger el sistema de alarmas o solicitar información sobre los sistemas.

Escogiendo el botón “Ayuda”, en la pantalla “Accesos”, se desplegará una nueva ventana, figura 50., que nos informará sobre cada uno de los símbolos que componen esta pantalla y su significado o comando que maneja.

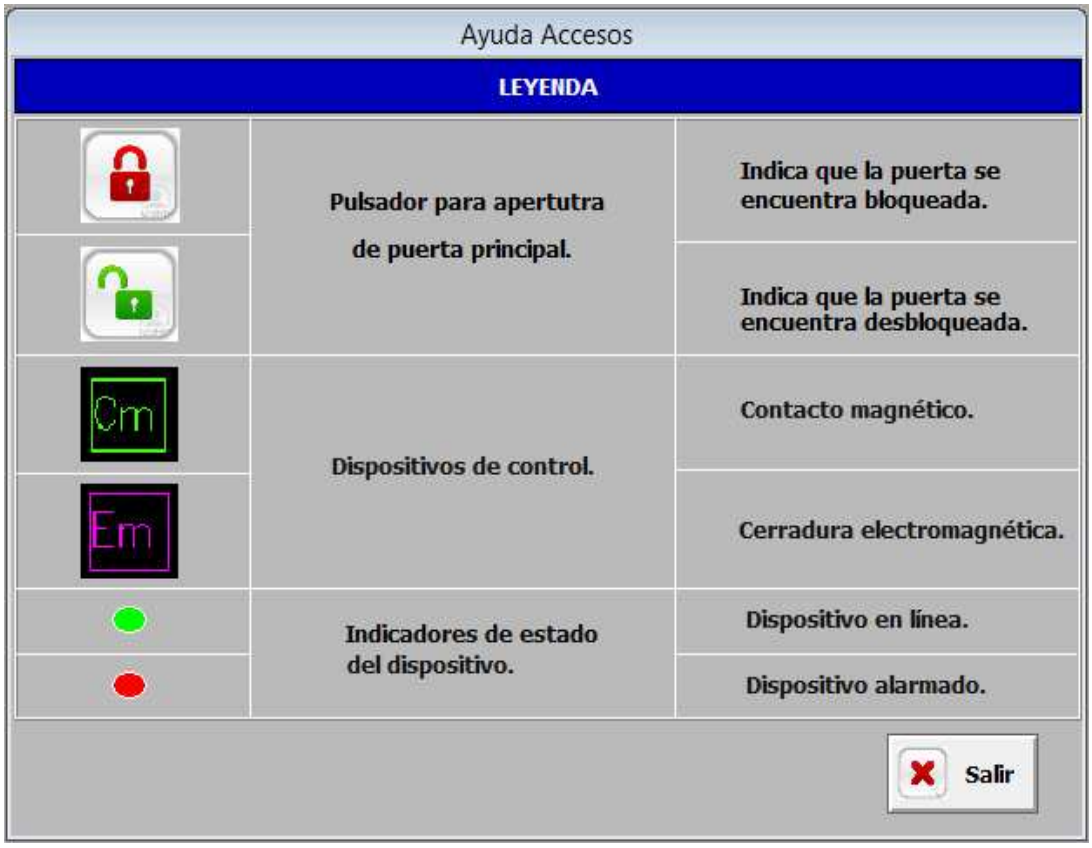


Figura 50. Pantalla “Ayuda Accesos”.

En la zona izquierda de la derecha se observan cada uno de los botones, símbolos e indicadores de estado de los dispositivos que componen a la pantalla “Accesos” de la figura 49., en la zona central lo que cada uno representa y en la zona derecha una breve descripción de cada uno de ellos.

Figura 51. Pantalla “Alarmas”.

Como se observa en la figura 51, tenemos en la parte superior un símbolo que se asocia con el sistema, seguido de tras botones que al seleccionarlos nos abrirán nuevas pantallas que nos permitirán monitorear los dispositivos del sistema de alarmas de la planta que hayamos seleccionado, y finalmente un botón “Salir” que nos volverá a la pantalla anterior.

Ya sea que escojamos el botón “Alarmas”, en el menú de navegación principal o escojamos este botón en la pantalla “Accesos”, nos aparecerá la pantalla mostrada en la figura 51., y al pulsar cualquiera de los botones nos mostrará la zona deseada para monitorear, por ejemplo seleccionando el primer botón desde arriba ingresaremos a monitorear los dispositivos que componen al sistema de alarmas en la planta baja como se observa a continuación en la figura 52.

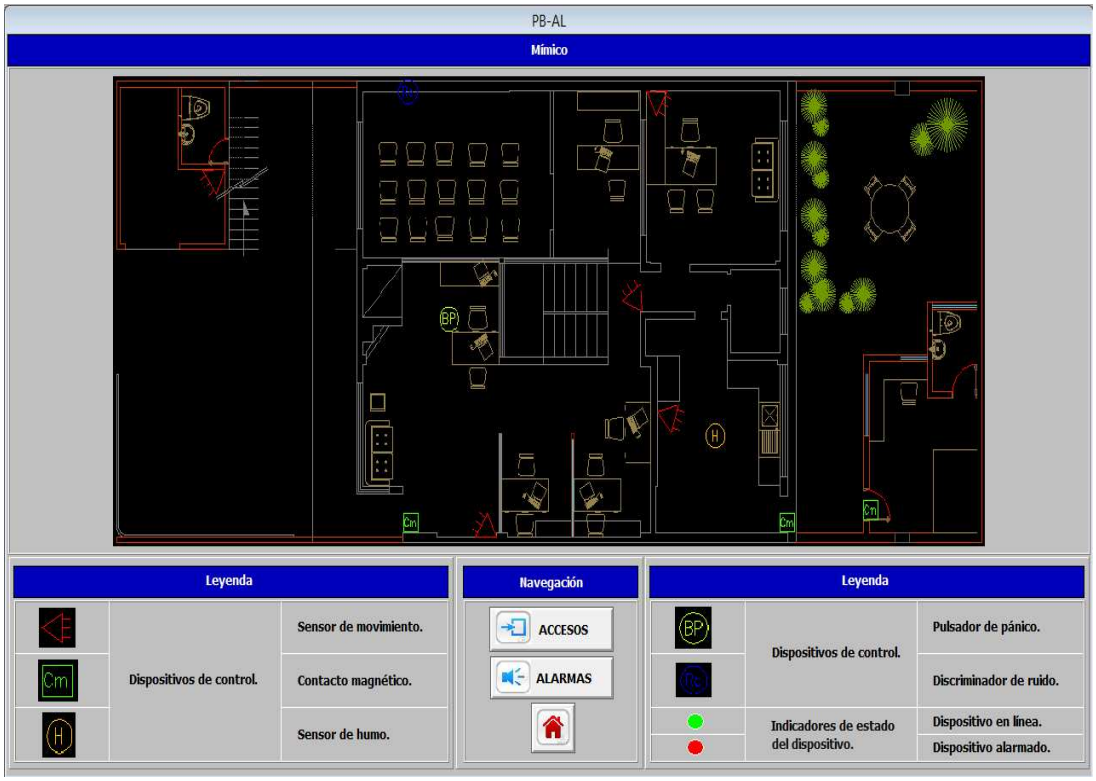


Figura 52. Pantalla “Alarmas Planta baja”.

En esta pantalla como ha sido en todas las demás pantallas se ha cumplido con el esquema establecido, en la zona superior un subtítulo, el texto de color blanco con su recuadro de fondo azul, en la zona central de la pantalla el mímico que representa a las instalaciones de la planta baja donde constan, en la zona superior izquierda la bodega menor, en la zona central con la recepción, oficinas de recursos humanos, contrataciones públicas, sala de capacitación, cocina y en la zona derecha un jardín y un taller, y en cada una de las áreas los dispositivos que la componen al sistema de alarmas.

En la zona central inferior los botones de navegación, y nótese que esta ventana carece de botón de “Ayuda”, debido a que a los costados izquierdo y derecho de los botones de navegación se muestra toda la leyenda de los dispositivos que componen al mímico y lo que cada uno de éstos representa.

En cuanto a los botones de navegación con que cuenta esta pantalla éstos servirán para dirigirnos al sistema de accesos, es decir nos aparecerá

la pantalla mostrada en la figura 49., el siguiente botón nos abrirá la ventana indicada en la figura 51., para escoger cualquier otra de las dos plantas del sistema de alarmas para monitorearlo y finalmente botón representativo de inicio, el cual cerrará la ventana actual y mostrará la ventana “Inicio” (figura 47).

Volviendo a la pantalla “Alarmas”, seleccionando el segundo botón “Planta Alta 1”, la interfaz nos mostrará la siguiente figura:

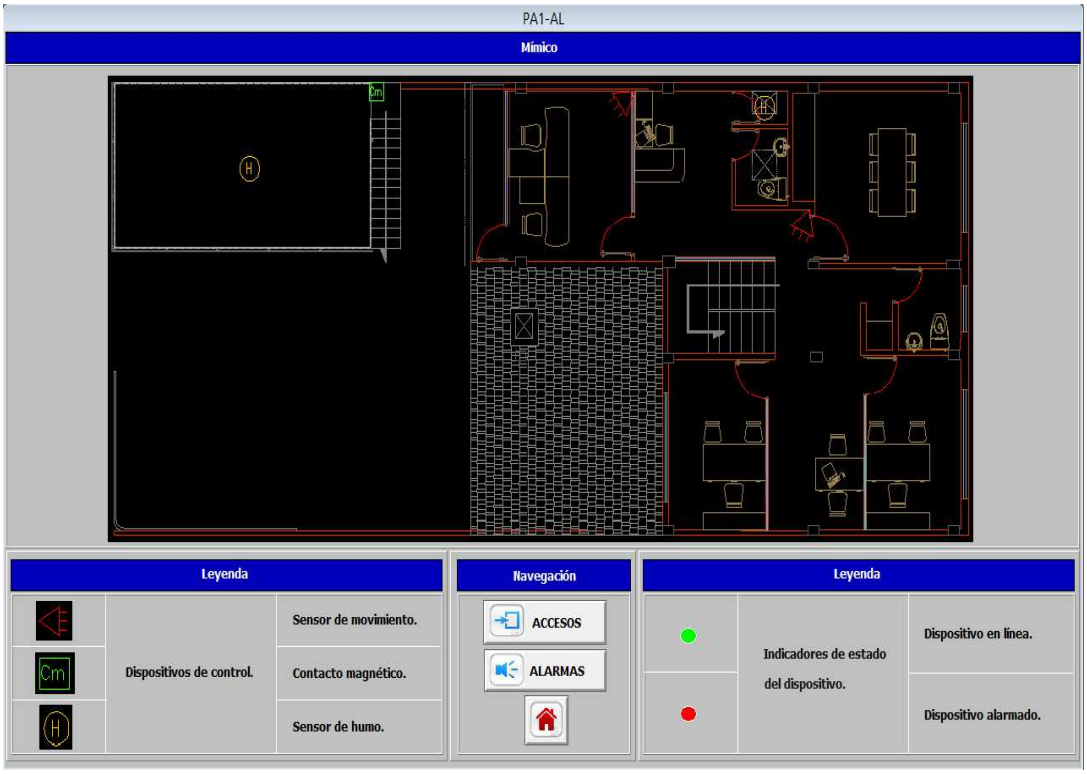


Figura 53. Pantalla “Alarmas Planta alta 1”.

Como se observa de la misma manera que la figura 52., esta pantalla cumple con los mismos parámetros de forma variando solamente con lo que tendría que ver con el mímico ya que esta pantalla está representando a la planta alta 1, que en su zona izquierda cuenta con la bodega principal y en la parte derecha con las oficinas de gerencia general, gerencia financiera, secretaría, sala de reuniones, hall y baños. Nuevamente en la zona central inferior se tienen los botones de navegación y en sus costados la leyenda de cada uno de los símbolos que componen al sistema en esta planta.

Finalmente si en la pantalla 51., se escoge el botón “Planta alta 2”, se nos desplegará la ventana mostrada a continuación:

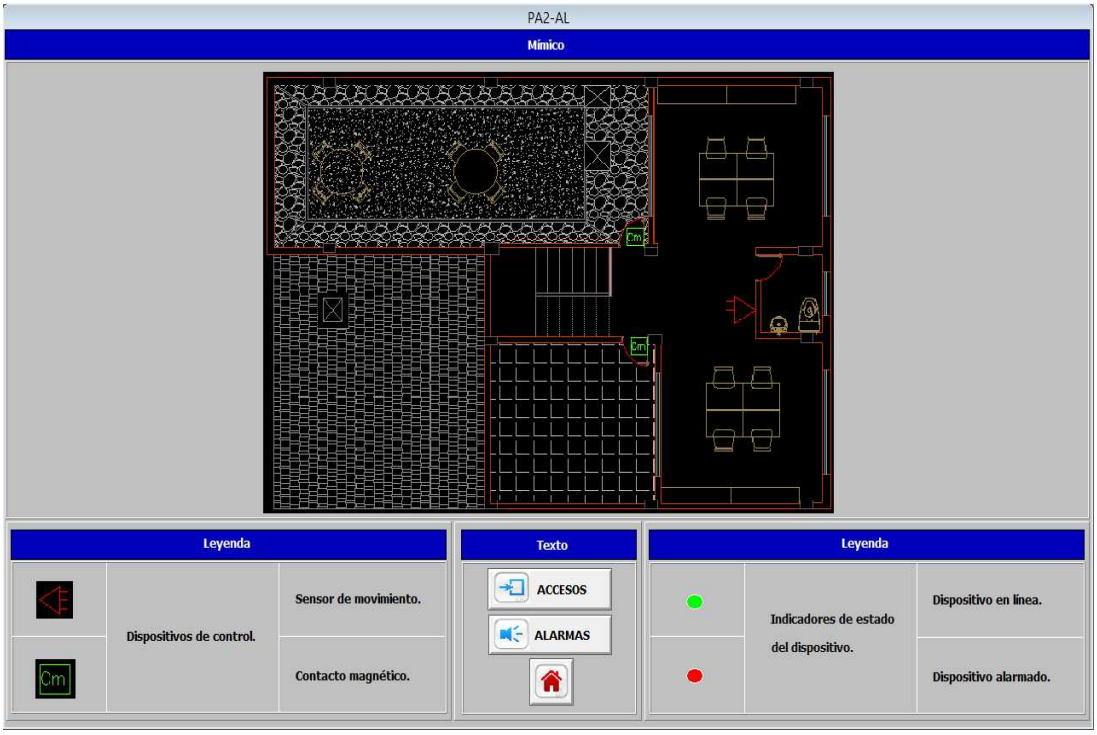


Figura 54. Pantalla “Alarmas Planta alta 2”.

Al igual que la figura 52. y la figura 53., esta también cumple con la plantilla diseñada previamente en donde consta de un subtítulo en la parte superior, un mímico en la parte central, los botones de navegación en la zona central inferior y a sus costados la leyenda de los dispositivos presentes en el mímico. En cuanto al uso del color el texto se ha mantenido de color blanco con sus cuadros de fondo azul y sus bodes negros para los subtítulos, y de color negro para el texto en general. Los botones de navegación como en las anteriores ventanas cuentan con uno de “Accesos” para mostrarnos el sistema de accesos, además de uno denominado “Alarmas”, que nos abrirá la pantalla mostrada en la figura 51., para elegir a que otra planta de las instalaciones queremos realizar el monitoreo del sistema de alarmas y finalmente el botón asociado con la pantalla “Inicio”.

Mientras que en los costados de este panel de navegación se tiene la leyenda de cada uno de los dispositivos que componen al sistema en esta área de las instalaciones como son, sensores de movimiento y contactos magnéticos.

Como se observa en ésta zona de las instalaciones se cuenta con dos terrazas y las oficinas de operaciones de la empresa.

CAPÍTULO IV.

IMPLEMENTACIÓN.

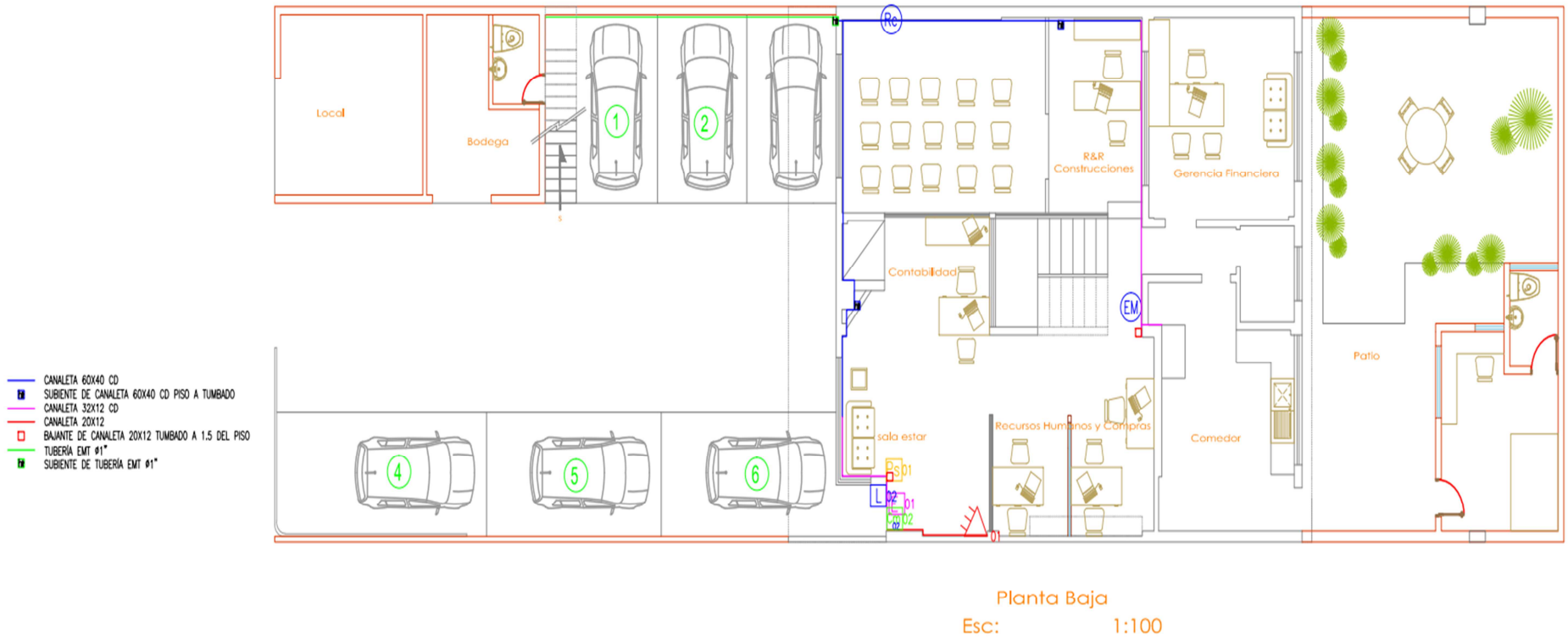
En este capítulo se tratará la implementación del sistema de seguridad en lo que tiene que ver con el montaje de cada uno de los dispositivos, la creación de la red LON así como la instalación de la interfaz, es decir la implementación física y la implementación lógica del sistema.

4.1. IMPLEMENTACIÓN FÍSICA DEL SISTEMA DE SEGURIDAD.

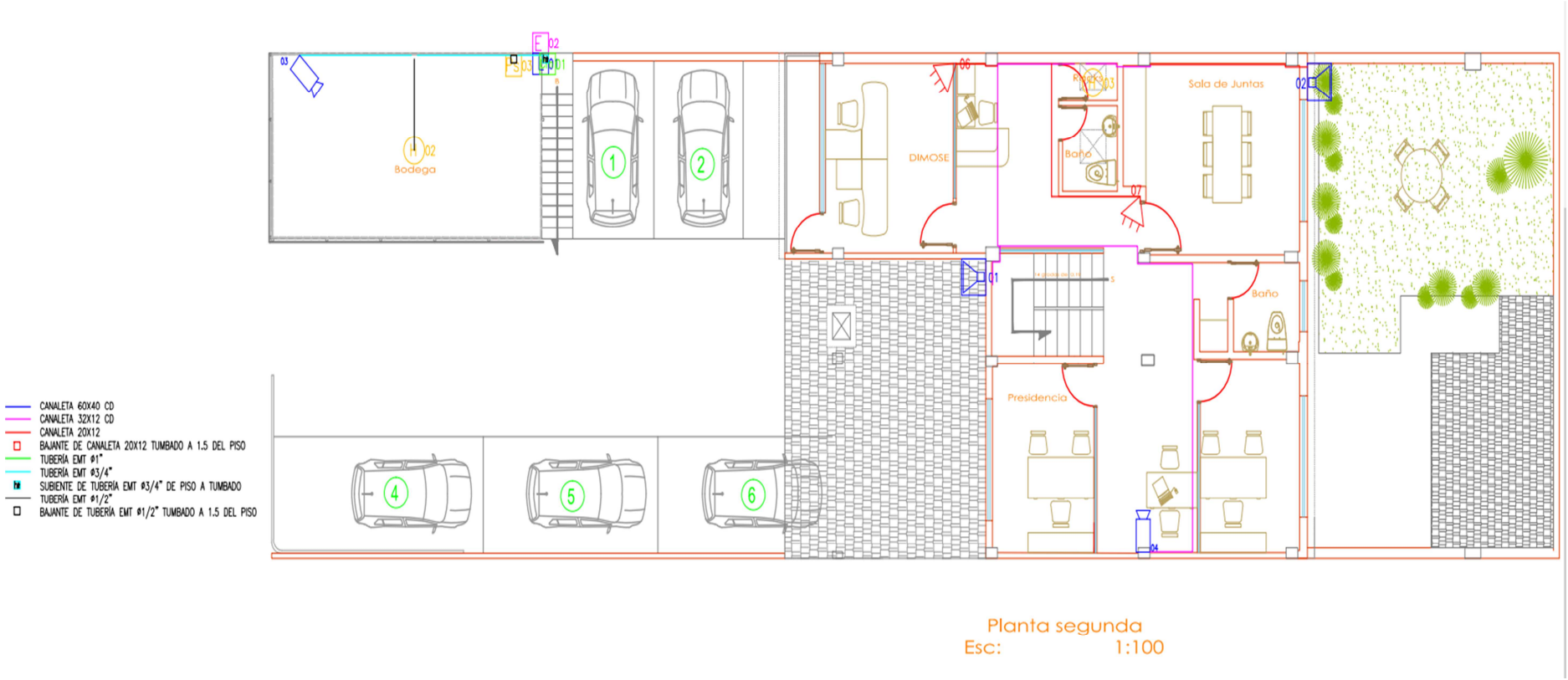
Como se pudo haber visto en el capítulo anterior, las instalaciones SRT HARDCOM S.A. comprenden de cuatro áreas, tres plantas y una bodega. En cada una de estas áreas se han implementado dispositivos que integran los distintos sistemas que son accesos, alarma, detección de incendio y CCTV.

4.1.1. Instalación de la Ductería y Cableado.

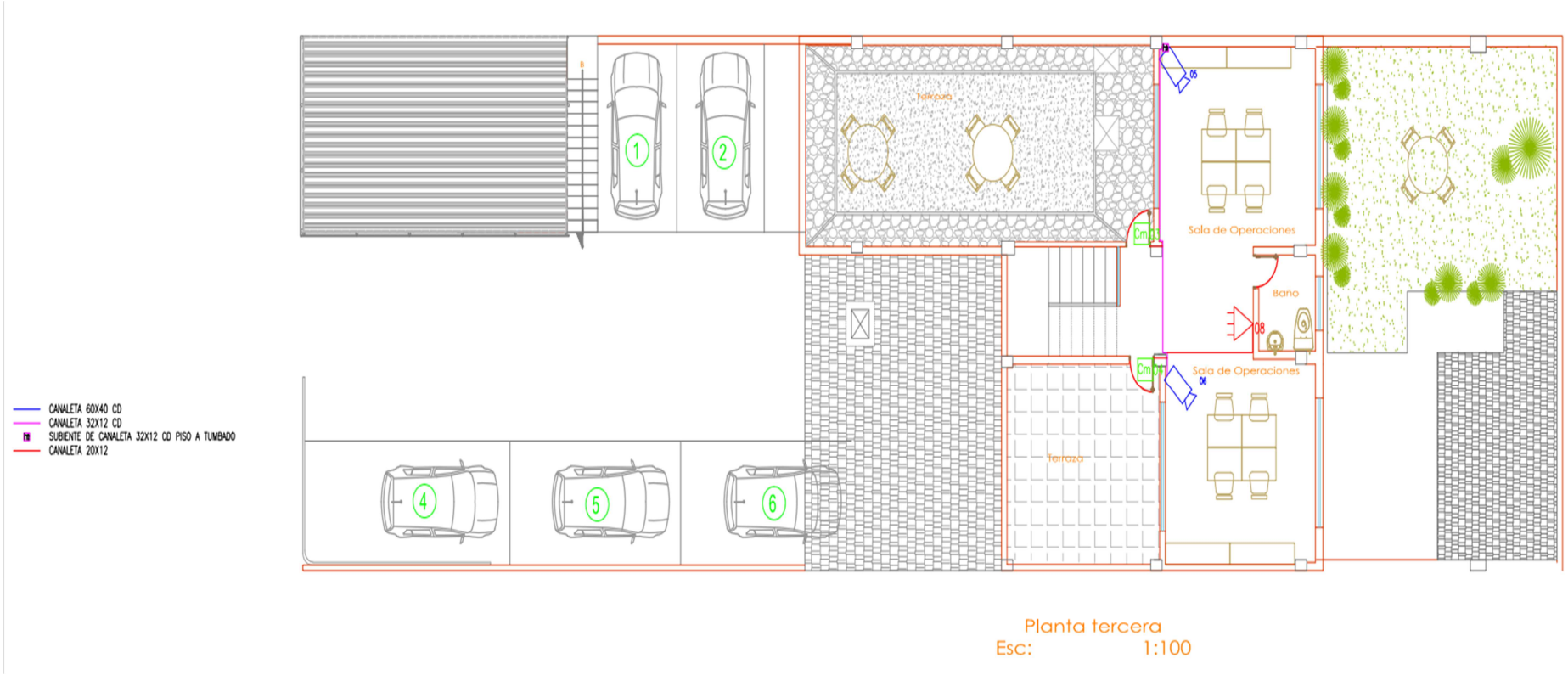
En este apartado se adjuntarán los planos arquitectónicos con ubicación de la ductería y cableado que ha sido necesario implementar para que todos los dispositivos periféricos se integren al sistema de seguridad, además del listado de los materiales utilizados para el cometido.



a) Ductería y cableado en Planta Baja



b) Ductería y cableado en Planta Alta 1



c) Ductería y cableado en Planta Alta 2

Figura 55. Planos arquitectónicos de la ductería, cableado y ubicación final de los dispositivos en las oficinas

A continuación se muestra la tabla con los materiales totales que se empleados donde constan el cableado, la ductería y los accesorios adicionales.

Tabla 23. Lista de materiales utilizados para el cableado y la ductería

DETALLE	CANTIDAD	UNIDAD
CABLES		
Cable UTP Categoría 5e, 4 pares, 100 ohmios CMR	1,00	B
TUBERÍAS Y ACCESORIOS		
Tubería EMT de 3/4" con accesorios	14,03	m
Tubería EMT de 1" con accesorios	43,07	m
Tubería EMT de 1/2" con accesorios	4,99	m
Caja de paso octogonal	2,00	u
Caja de paso reforzada 15x15	4,00	m
CANALETAS		
Canaleta DEXON con división 60x40 y accesorios	15,49	m
Canaleta DEXON con división 40x25 y accesorios	1,24	m
Canaleta DEXON con división 32x12 y accesorios	6,12	m
Canaleta DEXON sin división 20x12 y accesorios	43,13	m
Canaleta ranurada ploma 60X40 mm	5,00	m
ELECTRICO		
Sucre 3x18AWG	501,93	m
RIEL DIN	5,00	m
ADICIONALES		
Gabinete de seguridad 60x40x20	1	u

4.1.1.1. Trabajos de cableado y ductería en Planta Baja.

A continuación se muestra el cableado que se ha instalado en la planta baja de las instalaciones de SRT HARDCOM S.A.

Figura 56. Bajante desde el cuarto de equipos.

En la figura 56. se puede observar la bajante directamente desde el cuarto de equipos conteniendo lo cables que conectarán los dispositivos de la bodega principal como cámara sensor de humo y control de accesos. También el cableado para los dispositivos que irán instalados en la planta baja donde consta el control de accesos de la planta baja, semsor de movimiento y estación manual.

Figura 57. Canaleta ubicada en la sala de capacitaciones.

Esta canaleta es la continuación de la canaleta mostrada en la figura 56. y atraviesa la sala de capacitaciones y la esquina de este cuarto para posteriormente salir al patio y conectar la bodega con las oficinas. Como se observa, una canaleta continúa de la esquina hacia la derecha y es la que continuará con los cables para el control de acceso para el ingreso principal, cuyas terminaciones se observan en la figura 58.

Figura 58. Cableado para la instalación del control de accesos.

Figura 59. Ductería hacia bodega.

En la figura 59., se muestra la ductería que necesariamente fue instalada para conectar los dispositivos como cámara, control de acceso y sensor de humo, con el cuarto de equipos ubicado en la planta alta uno de las oficinas

a) Cableado para los dispositivos de control de accesos para la bodega principal.

b) Cableado para el sensor de humo de la bodega principal.

c) Cableado y tomacorriente para la cámara análoga.

Figura 60. Cableado de dispositivos de la bodega principal.

La figura anterior muestra el cableado y la ductería instalada para cumplir con las ubicaciones de los dispositivos que se había diseñado anteriormente.

Finalmente en la figura 61., se observa el cableado y la canaleta donde va a ir ubicada la estación manual del sistema de detección de incendios.

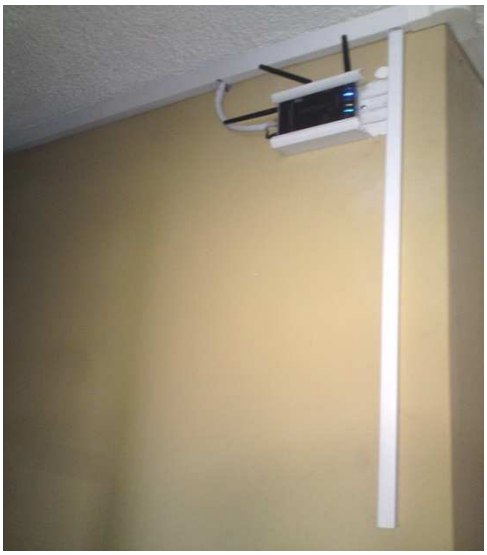


Figura 61. Cableado y canaleta para estación manual.

4.1.1.2. Trabajos de cableado y ductería en Planta Alta Uno.

En esta planta es donde se encuantra el cuarto de equipos y donde se ha determinado que van a ir ubicados el gabinete conteniendo a los nodos de control y además del DVR. Inicialmente en la figura 62. se muestra el cableado que llega desde todos los dispositivos distribuídos por todas las áreas de las instalaciones de SRT HARDCOM S.A., hacia el mencionado cuarto de equipos.

a) Estado inicial del cableado.

b) Cableado una vez adecuado el CCTV.

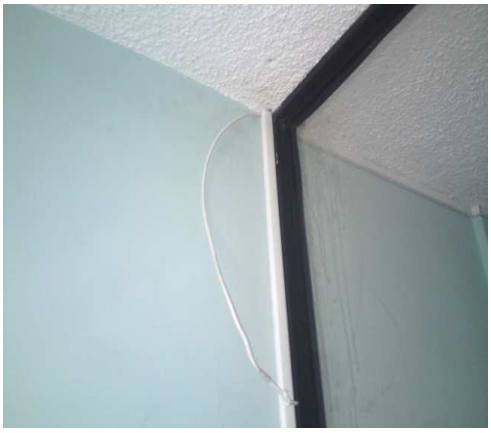
c) Cableado una vez instalado el gabinete.

Figura 62. Cableado en el cuarto de equipos.

La organización del cableado dentro del cuarto de equipos se la realizó en dos etapas la primera etapa concluyó cuando se terminaron las adecuaciones y se puso en marcha el Circuito Cerrado de Televisión. Y la segunda etapa cuando se realizó la identificación de todos los conductores y su organización dentro del gabinete.

Desde aquí partirán todos los conductores y en la figura 63., se observa junto al tumbado la canaleta que conduce hacia la oficina de DIMOSE donde va instalado un sensor de movimiento.

a) Canaleta desde cuarto de equipos hacia oficina de DIMOSE.



b) Cableado para el sensor de movimiento.

Figura 63. Canaleta y cableado para el sensor de movimiento en DIMOSE.

Ahora en el hall de la planta alta uno se muestra la ductería utilizada para contener el cableado que alimentará y conectará dispositivos como sensor de movimiento, teclado INS-050, cámara análoga y la sirena externa.

Figura 4.64. Ductería y cableado en hall de la planta alta uno.

a) Cableado y canaleta para sensor de movimiento.

b) Cableado y canalete para el teclado INS-050.

c) Cableado y cajetín para la instalación de la sirena externa.

Figura 65. Cableado y ductería para los dispositivos de la planta alta uno.

En las figuras anteriormente mostradas se observa la ductería implementada y previamente diseñada para la instalación de los dispositivos periféricos de los sistemas Anti-intrusión y para el circuito cerrado de televisión.

4.1.1.3. Trabajos de cableado y ductería en Planta Alta Dos.

En la siguiente figura se muestra, a la izquierda, la canaleta que contendrá los conductores que a su vez conectarán la cámara análoga orientada al área de operaciones, al sensor de movimiento y a los contactos magnéticos ubicados en las puertas de las terrazas. En la derecha se observa el cableado que alimentará y llevará la señal de la cámara enfocada en la sala de reuniones hasta el DVR.

Figura 66. Cableado y ductería instalada en la Planta Alta dos.

4.1.2. Implementación del sistema de accesos.

El sistema de accesos está compuesto por el control del ingreso del personal a dos áreas de interés específico que son, la puerta principal de las oficinas y la puerta de la bodega principal. A continuación en la Figura 67.,

se muestran estos puntos de interés una vez instalados los terminales. Los dispositivos a instalarse en cada uno de los accesos serían, un módulo lector de proximidad en el exterior, un pulsador de salida en el interior y una cerradura electromagnética también en el interior del área.

Figura 67. Dispositivos terminales del Sistema de Accesos.

4.1.3. Implementación del sistema de alarmas.

El sistema de alarmas cuenta con dispositivos de seguridad en las cuatro áreas, ya descritas, de las instalaciones de SRT HARDCOM S.A., por lo cual se ha tomado un dispositivo de cada área para su documentación.

Dispositivo montado en la bodega principal.

En la bodega principal se ha realizado el montaje de un contacto magnético en su puerta, seguidamente se muestra la Figura 68., donde se indica el cableado del dispositivo y su instalación.

Figura 68. Contacto magnético ubicado en la puerta de la bodega.

Dispositivo montado en la planta baja de las oficinas.

El sistema de alarma en la planta baja cuenta con contactos magnéticos en su puerta principal. A continuación se muestra el cableado y el montaje de este dispositivo.

Figura 69. Contacto magnético ubicado en la puerta de ingreso.

Dispositivos montados en la planta alta uno de las oficinas.

En la planta alta uno de las oficinas se han instalado como dispositivos terminales, el teclado de alarmas, dos sensores de movimiento orientados a las áreas vulnerables que son la entrada a esta planta y un ventanal, además se instalará la respectiva sirena que será la encargada de emitir el aviso sonoro en caso de que el sistema de alarma se active, y va ubicada en

el exterior. En las siguientes figuras se muestra la el montaje de los dispositivos.

Figura 70. Teclado de Alarmas INM-050R.

Figura 71. Sensor de Movimiento ubicado en Hall.

Figura 72. Sensor de movimiento ubicado en oficina DIMOSE.

Figura 73. Sirena exterior.

Dispositivos montados en la planta alta 2 de las oficinas.

Los dispositivos a instalarse en esta área de las instalaciones son contactos magnéticos para las puertas de sus terrazas y un sensor de movimiento dirigido a la entrada de ésta planta. En las figuras mostradas a continuación se muestra el montaje de estos dispositivos en los lugares ya mencionados.

Figura 74.Sensor de Movimiento ubicado en el ingreso de la planta.

Figura 75. Contacto magnético ubicado en la puerta a “Terraza 1”.

Figura 76. Contacto magnético ubicado en la puerta a “Terraza 2”.

4.1.4. Implementación del sistema de detección de incendios.

El sistema de detección de incendios consta de un sensor de humo en el área más vulnerable a sufrir un accidente de este tipo que es la bodega principal, además de una estación manual en la planta baja. En las figuras 77., y 78., se muestra la instalación de estos dispositivos en las áreas mencionadas.

Figura 77. Detector de Humo en “Bodega”.

Figura 78. Estación Manual en “Planta Baja”.

4.1.5. Implementación del Circuito Cerrado de Televisión.

Se han instalado cuatro cámaras en lugares estratégicos que abarcan las áreas de interés de la empresa donde se encuentran sus valores y que deben ser constantemente supervisadas. Se mostrará a continuación el montaje de cada una de ellas.

Figura 79.Cámara en Bodega principal.

Figura 80. Cámara en planta alta 1.

Figura 81. Cámara en planta alta 2, oficina de bodeguero.

Figura 82. Cámara en planta alta 2, área de operaciones.

4.1.6. Implementación de los Dispositivos de Control y Monitoreo.

Todos los dispositivos de que realizarán el control y el monitoreo del sistema de seguridad están instalados en el cuarto de equipos de las oficinas. Se ha acondicionado un gabinete con tapa transparente que contendrá a todos los nodos de control LONWorks y además la alimentación para cada una de las cámaras. Se muestra en la figura 83., la adecuación final del gabinete para el montaje de los nodos de control.

Figura 83. Gabinete adecuado para contener nodos de control.

Por tanto a este punto llega todo el cableado que conectan a los dispositivos periféricos con los nodos de control. A continuación en la siguiente figura se muestra todo el cableado que llega al gabinete para ser conectado a los nodos de control y la tentativa ubicación de cada uno de ellos.

Figura 84. Cableado desde los dispositivos periféricos al gabinete.

Finalmente en la siguiente figura se muestra la conexión de los nodos de control con sus dispositivos periféricos y la identificación de cada uno de ellos.

Figura 85. Nodos de control.

Además de los nodos LONWorks se ha implementado un grabador digital de video el cual se encuentra ubicado en el rack del cuarto de equipos y un switch de red que complementa la funcionalidad del DVR ya que le permite ser monitoreado remotamente desde cualquier red y a cualquier momento. Junto al DVR y conectada al servidor de SRT HARDCOM S.A., se encuentra la interfaz USB que permitirá la interactividad del sistema de seguridad con la HMI diseñada en Wonderware InTouch.

Figura 86. Grabador Digital de Video (DVR).

Figura 87. Switch de red para DVR.

Figura 88. Interface de red IAUSB-F.

A continuación se muestra la red que se ha implementado para cumplir con la integración completa del sistema de seguridad, nótese que tanto el grabador digital de video como el servidor están conectados al mismo conmutador por solicitud del usuario, por tanto el DVR no va a ser el único que podrá ser monitoreado remotamente, sino que también la interfaz del sistema que ha sido desarrollada en InTouch también podrá ser operable y monitoreada remotamente mediante la implementación de un escritorio remoto.

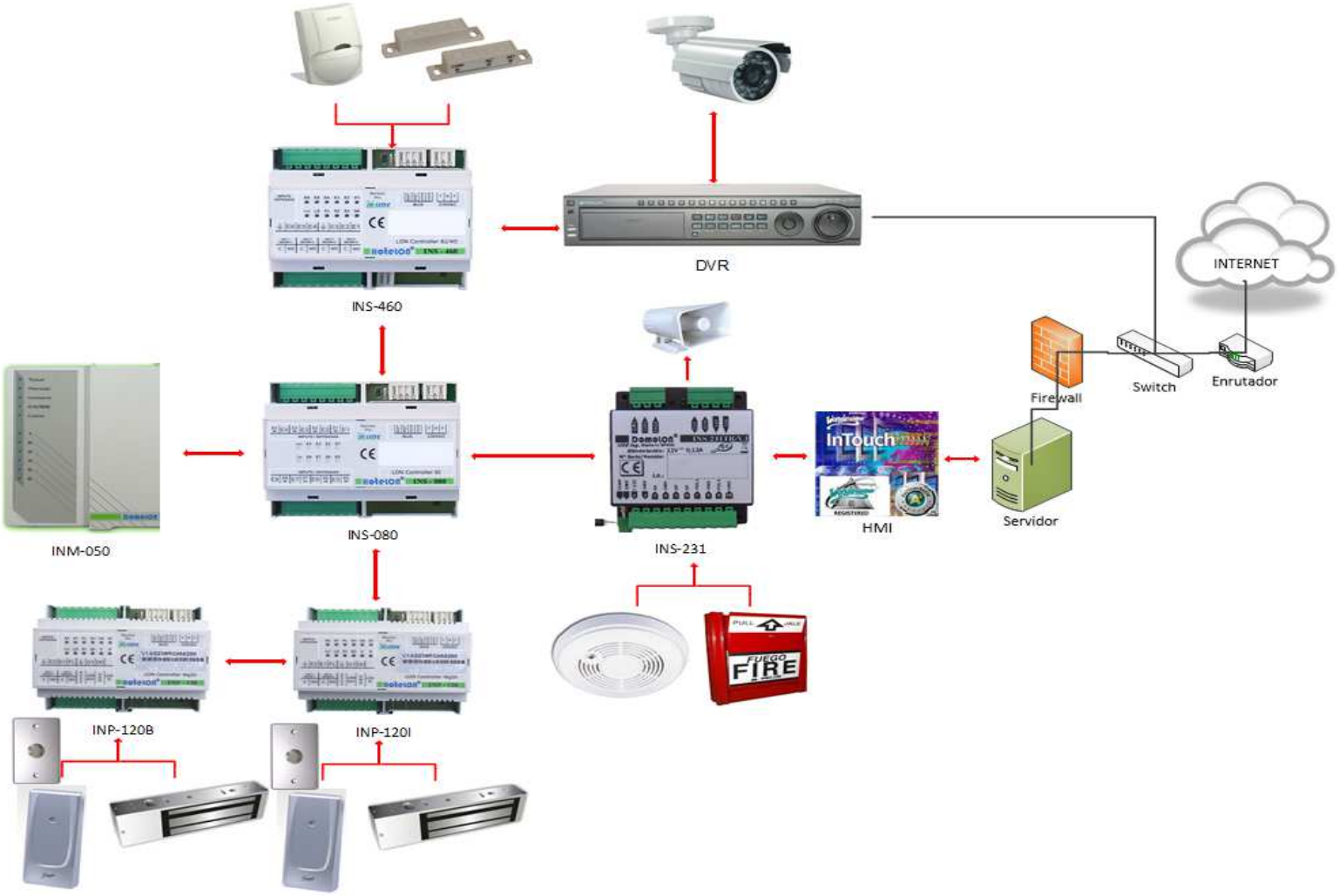


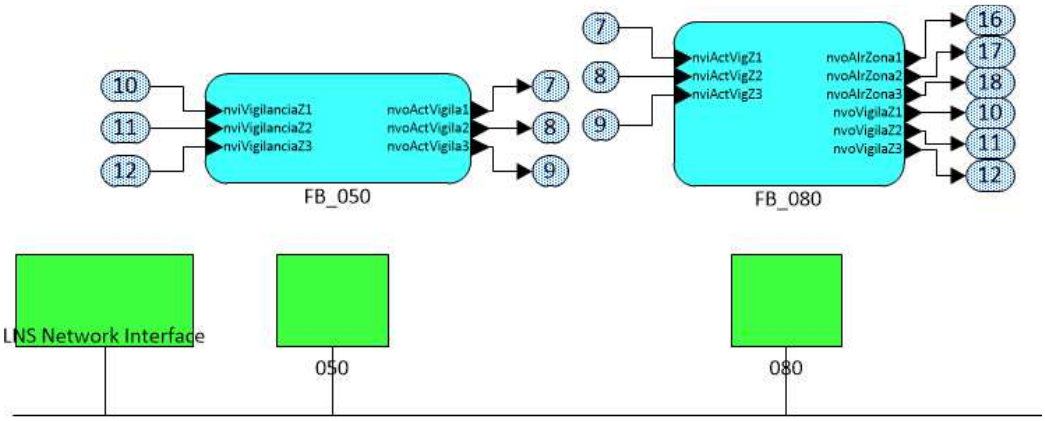
Figura 89. Red Completa del Sistema de Seguridad Electrónica.

4.2. IMPLEMENTACIÓN LÓGICA DEL SISTEMA DE SEGURIDAD.

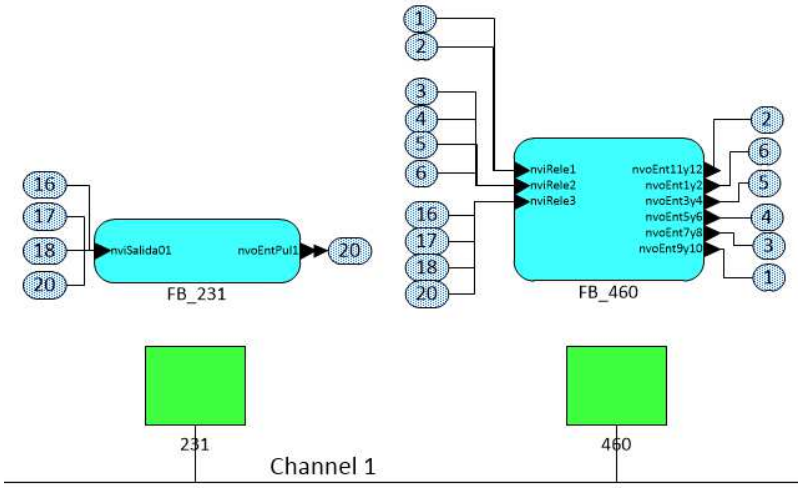
Así como se muestra la implementación del “Hardware” del sistema se mostrará a continuación la programación de cada uno de los nodos LONWorks, la configuración del DVR y la interacción de todos los dispositivos mediante señales lógicas como físicas.

4.2.1. Implementación de la red LON. (ECHELON, 2012)

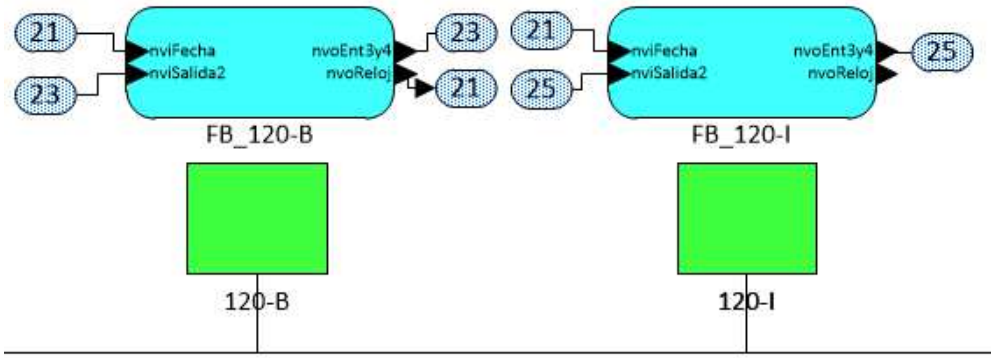
La implementación lógica de la red se ve reflejada en la figura 90., donde constan los nodos representados lógicamente en el software LONMaker, la red que los enlaza, y también como están conectados unos con otros mediante sus variables de red.



a) Interfaz USB-LON; Nodo INM-050; Nodo INS-080



b) Nodo INS-231; Nodo INS-460



c) Nodos INP-120, Accesos de Bodega y Oficinas

Figura 90. Programación de los nodos y su representación en LONMaker.

En la figura 90., se muestran las conexiones de las variables de red entre el teclado de accesos y el supervisor que obligatoriamente necesita el teclado que en este caso será el nodo INS-080 configurado con firmware de seguridad. En el nodo INM-050 (Teclado de accesos), se configura la contraseña que deberá ingresar el usuario, la habilitación del sonido de las teclas, el tiempo de bloqueo en caso de que se haya superado el número de intentos erróneos, este nodo es el encargado de generar las señales para que el nodo supervisor esté informado de que el usuario ha armado o desarmado la alarma. En el nodo supervisor se programarán, el número de veces que es necesario que se active una zona para considerar activar la alarma, el tipo de cambio de flanco que el nodo detectará para cada una de las zonas independientemente, los tiempos de entrada y salida del usuario de las instalaciones antes de que se arme la alarma, este tiempo es configurable independiente para cada zona, además genera señales de retroalimentación, con respecto al armado o desarmado de la alarma, dirigidas al teclado para evitar que se produzcan falsas alarmas. El nodo supervisor es el encargado de emitir las señales lógicas a los nodos INS-460 e INS-231 para que actúen por él, mediante sus salidas físicas, en caso de producirse una activación de la alarma por una violación del sistema. Son emitidas por el nodo supervisor tres señales que corresponden a cada una de las zonas con las que se está cubriendo todas las áreas requeridas por el usuario.

Tanto el nodo INS-231 como el nodo INS-460 reciben lógicamente estas tres señales y mientras que a la activación de la alarma el nodo INS-231 activa su salida 1 para la alimentación de la sirena, el nodo INS-460 al recibir esta misma señal activa una de sus salidas que va comunicada con una entrada del DVR que a su vez recibiendo este estado lógico en su primera entrada, envía un correo electrónico a los usuarios previamente configurados dando el aviso de que se ha producido la activación de la alarma.

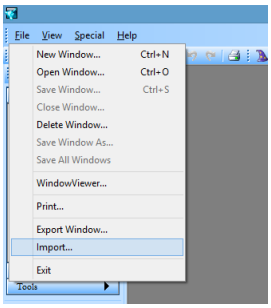
El encargado de recibir las señales del sistema de detección de incendio es también el nodo INS-231, éste al recibir una activación de incendio ya sea mediante el sensor de humo o de la estación manual, activa directamente su salida 1 alimentando a la sirena y lógicamente se emite la señal para que también actúe el nodo INS-460 activando su salida que tiene comunicación con el DVR y al igual que si se produjese una activación de la alarma envía un correo alertando al usuario de que se ha activado el sistema de detección de incendios.

4.3. Implementación de la HMI.

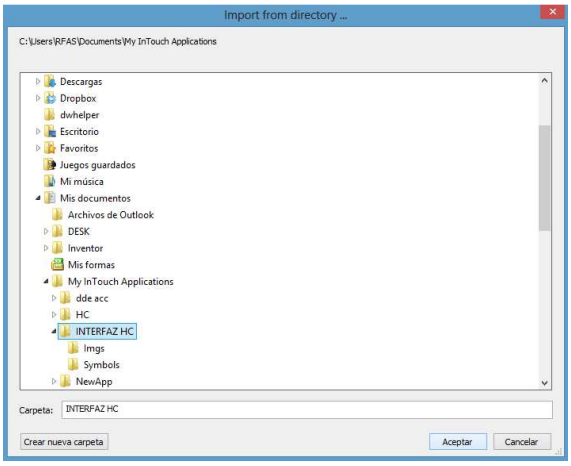
La implementación de la interfaz será desarrollada en el servidor de la empresa, es decir, todos los software que se han mencionado en capítulos anteriores serán instalados en el computador servidor por solicitud del usuario ya que es el único que siempre va a permanecer encendido y mediante el cual se podrá monitorear local o remotamente en cualquier momento del día.

4.3.1. Configuración de Wonderware InTouch. (Wonderware®, 2007)

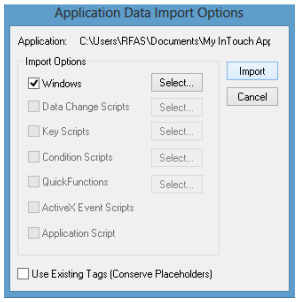
Una vez instalado el software se procederá a importar las ventanas de la interfaz que ha sido diseñada previamente como se observa en la figura 4.37.



a) Ejecución del comando en la ventana principal.



b) Búsqueda en el directorio.



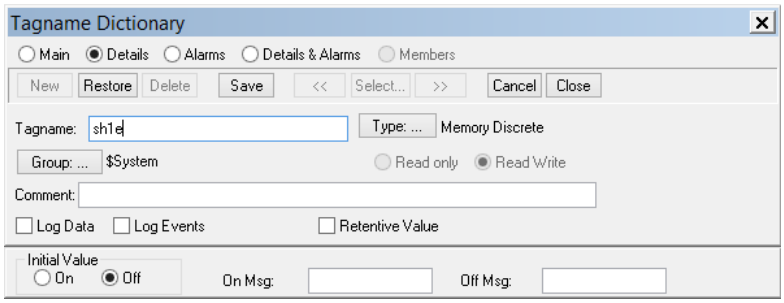
c) Selección de elementos a importar.

Figura 91. Importación de las ventanas de la interfaz.

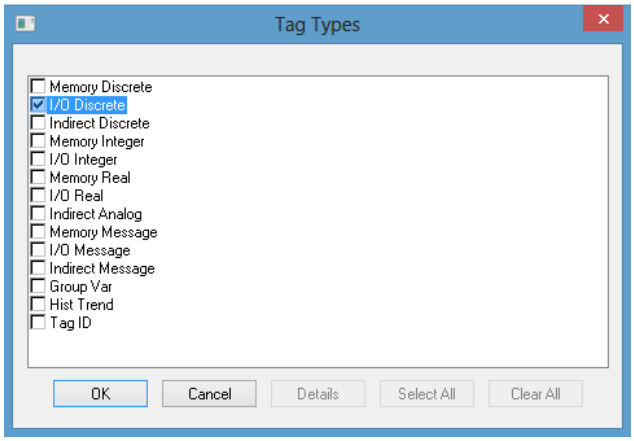
Al realizar la importación de las ventanas se importan también los window scripts que se ha realizado para ciertas ventanas así como la configuración de las ventanas para que sigan a la arquitectura que se ha establecido.

El siguiente paso a seguir para realizar la integración de la interfaz con el sistema es la creación de “Tags” en InTouch y que estas vayan asociadas con las variables de red con las que se maneja la red LON.

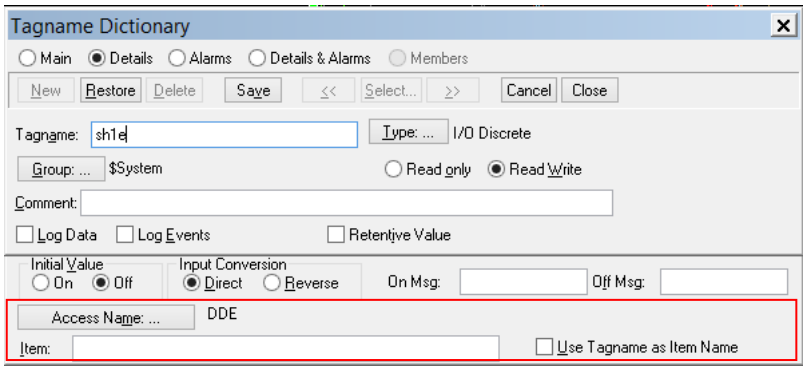
Por tanto, estos tags van a ser en su mayoría del tipo “I/O Discrete”, tomando de ejemplo a la variable que controlará el indicador de estado del sensor de humo, y a continuación se debe crear el “Access Name” para este tipo de variable y el ingreso de los parámetros necesarios para conectarse con el servidor LNS DDE. A continuación en la siguiente figura se muestran todos los pasos mencionados anteriormente en imágenes.



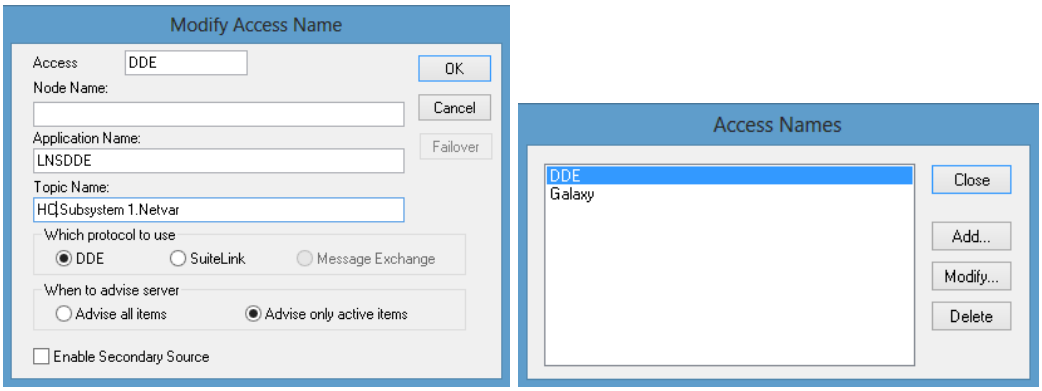
a) Creación del “Tag”



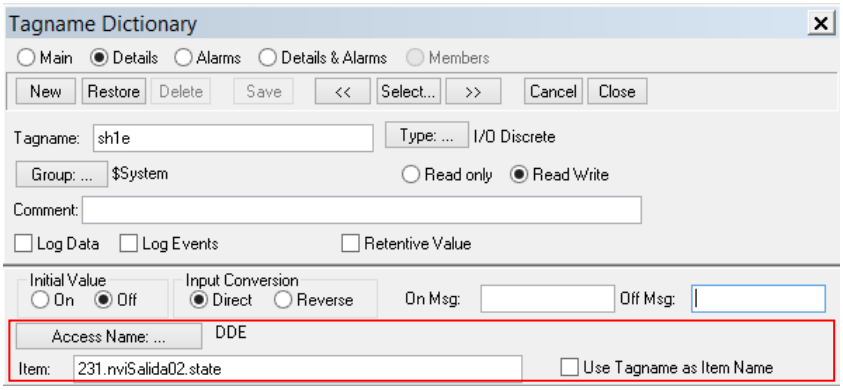
b) Definición del tipo de dato.



d) Habilitación para la creación del “Access Name”.



e) Creación del “Acces Name”, introducción de parámetros y aparición del “Access Name” creado.



f) Asociación del “Tag” con la variable de red.

Figura 92. Asociación de “Tags” con variables de la red LON.

Para conocer el “Ítem” con el que se enlazará el tag se puede consultar o directamente copiarlo desde el servidor LNS DDE, (ECHELON, LNS DDE User´s Guide, 2002) como se muestra a continuación.

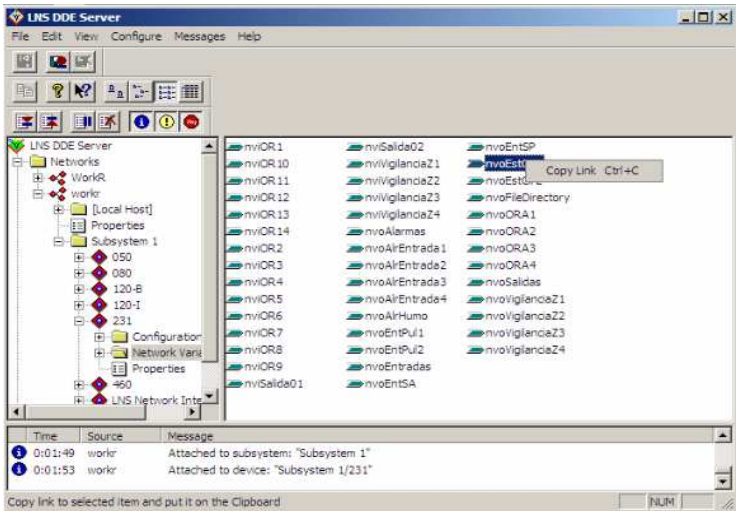


Figura 93. Obtención del enlace de la variable de red desde LNS DDE.

Este procedimiento se realizará para cada uno de los indicadores de los sensores, periféricos como la cerradura electromagnética y para el control de accesos.

4.4. Configuración del DVR. (DAHUA, 2013)

Como se ha hecho mención anteriormente este equipo tiene 16 entradas por contactos secos mediante los cuales se integrará al sistema se seguridad.

Inicialmente se muestran a continuación en la siguiente figura las señales captadas por las cuatro cámaras que han sido habilitadas.

Figura 94. Señales de cámaras instaladas en las oficinas de HARDCOM S.A.

A continuación se mostrarán las configuraciones tanto locales como remotas que han sido realizadas para que el DVR mediante estas conexiones se convierta en el terminal mediante el cual se alerta al usuario de que se ha activado la alarma.

Configuración Local.

Con el monitor dedicado que se ha destinado para el DVR se deberán realizar configuraciones de red, tramos horarios y que acciones deberá tomar el DVR en caso de que se produzca una alarma local.

En la figura 95., se muestra el ingreso al “Menú principal” y posteriormente hasta “Ajustes” donde se realizará todo lo antes mencionado.

a) Ingreso a menú principal del DVR.

b) Ingreso a ajustes en DVR.

Figura 95. Navegación en la interfaz del DVR.

En este punto se ingresará inicialmente a “RED”, para realizar las respectivas configuraciones.

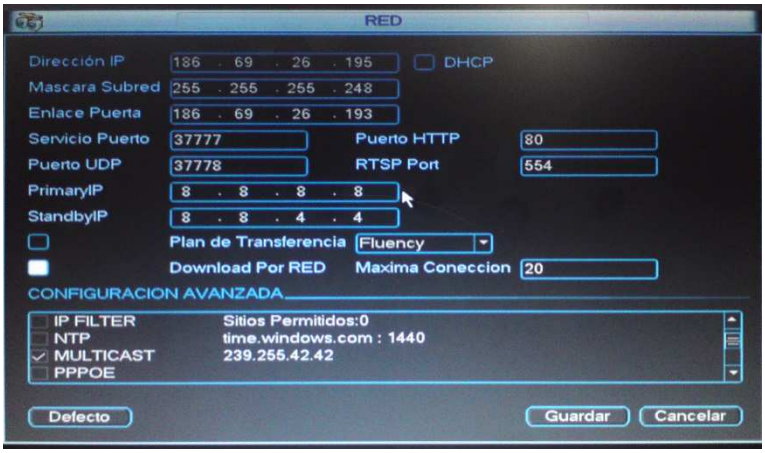


Figura 96. Configuración de RED del DVR.

Se asignará al DVR una dirección IP pública de manera que a éste se pueda tener acceso mediante cualquier terminal móvil ya sea Smartphone o computador desde cualquier lugar del mundo. Para esto fue necesaria la implementación de un switch de red adicional al cual está conectado el DVR y el firewall de la empresa. Además se habilita la descarga de los archivos de video desde la red y un máximo de hasta 20 conexiones simultáneas.

Volviendo a la figura 95.b., e ingresando a la opción “Alarma”, aquí se configurarán las acciones que debe tomar el DVR cuando tenga activada

una de sus entradas, es decir se haya producido una activación de la alarma.

Entonces, para la entrada 1, configuramos el tipo de contacto a “Normalmente Abierto”, y se le habilita para que envíe correos a los destinatarios que se los configurará remotamente y además que comience a grabar en todos los canales habilitados.

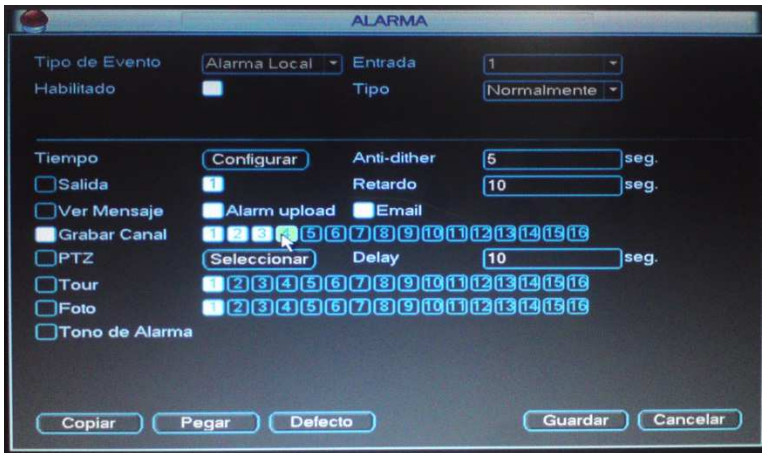


Figura 97. Configuración de “Alarma” del DVR.

Se ha realizado esta configuración con respecto a que inicien la grabación las cámaras, debido a que como se puede observar en la figura 98., los tramos horarios de lunes a viernes están definidos a que se graben desde las seis am, hasta las veintidós pm, por tanto si no se produjese una alarma durante toda la noche las cámaras solo estarán para monitoreo mas no para la grabación del video haciendo más eficiente el uso del espacio del disco duro al no grabar las veinticuatro horas del día.

Ingresando en “Horario”, en la figura 95.b, se configurarán los tramos horarios de cada día de la semana en los cuales el DVR grabará los canales, se han creado dos tramos horarios uno de lunes a viernes y otro para sábado y domingo. En el primero el tramo horario va desde las seis am que el personal comienza el ingreso a las oficinas hasta las veintidós pm que se retiran y a partir de esta hora solo se grabarán los eventos en las oficinas si se produjese una activación de la alarma. Mientras que para el fin de

semana se ha dispuesto para que el sistema grabe todos los sucesos que ocurren durante las cuarenta y ocho horas.

a) Tramo horario de lunes a viernes.

b) Tramo horario para sábado y domingo.

Figura 98. Tramos horarios de grabación del DVR.

Configuración remota.

Ejecutamos la aplicación “Internet Explorer” e introducimos la dirección IP asignada anteriormente en la configuración local.

Nos pedirá permisos para instalar controles ActiveX y aceptamos estas instalaciones, a continuación nos aparece esta pantalla.

Figura 99. Pantalla de acceso al DVR.

Se ingresa el nombre de usuario y la contraseña y se accede. Al ingresar nos aparece la pantalla mostrada a continuación:

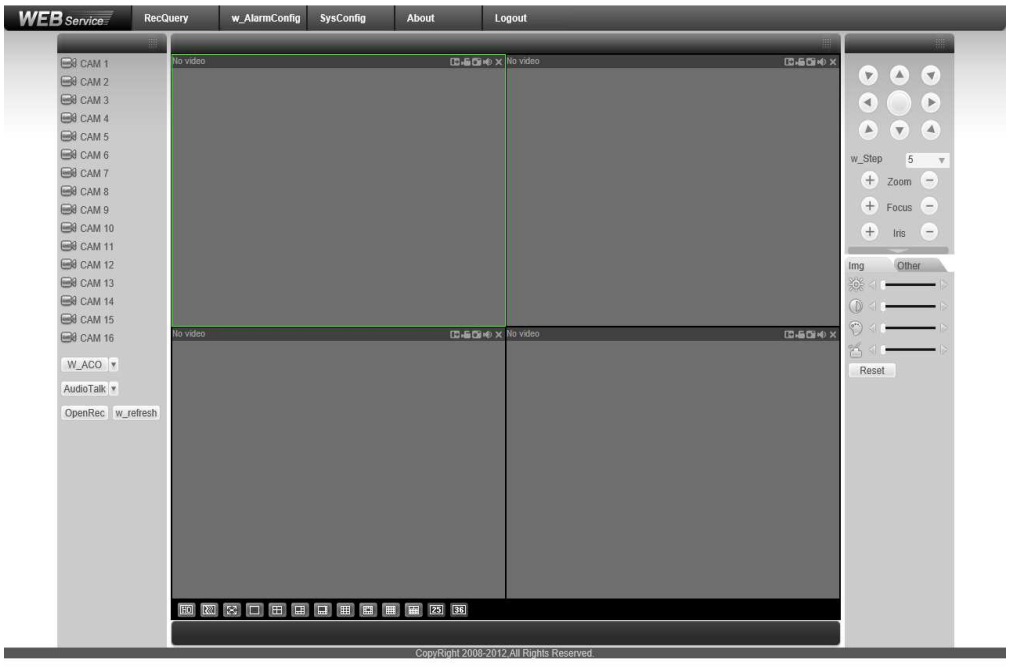


Figura 100. Pantalla principal de la interfaz DVR.

Remotamente también se puede realizar la configuración de os tramos horarios y la configuración de la alarma, pero a continuación se

muestra la configuración del servidor de correos que únicamente se la puede realizar remotamente.

En la parte superior de la pantalla principal se encentra una barra de tareas donde se ingresará en “SysConfig” para las configuraciones remotas. En la siguiente figura se muestra todos los ítems que deben ser ingresados para la correcta funcionalidad de este servicio. El DVR tendrá asignada una dirección de correo desde la cual remitirá los correos a los destinatarios.

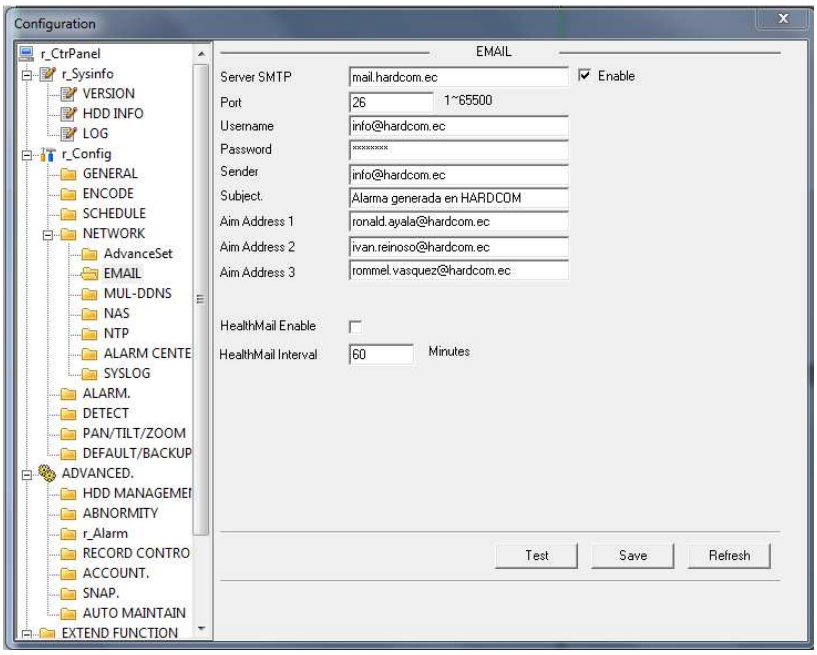
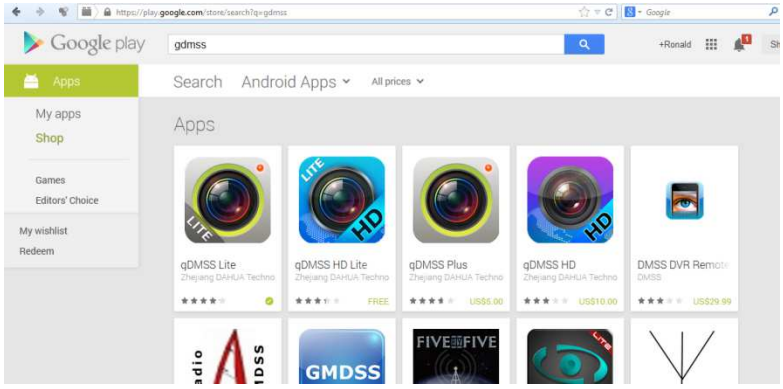


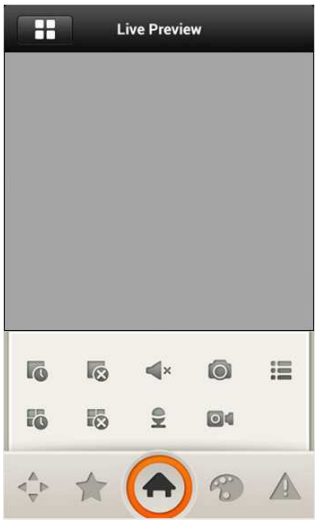
Figura 101. Ventana de configuración remota.

Debido a que todos los servicios adicionales ya se han configurado localmente solo ésta sería la configuración remota para un computador.

Ya que el DVR permite ser monitoreado vía WAN existe una aplicación gratis para Smartphone denominada “gDMSS “, (DAHUA, 2010) desarrollada por la compañía DAHUA para este cometido. En la siguiente figura se muestran los pasos para la configuración de este servicio adicional.



a) Descarga de la App gDMSS lite desde Google Play.



b) Pantalla principal de la App.

c) Menú de la App.

d) Pantalla “Device manager” o administrador de dispositivos.

e) Ingreso de datos datos para que se realice la conexión con el DVR.

Figura 102. Pasos para la instalación de la App.

En la figura anterior se muestran los pasos a seguir para obtener la App y poder realizar el monitoreo remoto del sistema de vigilancia. Inicialmente se procede a descargar e instalar la aplicación. Al ejecutar la aplicación, en la pantalla principal se da un toque en el botón del menú ubicado en la esquina superior izquierda, a continuación nos aparece el menú y dando un toque en el botón “Device Manager” se abre una nueva ventana donde se muestran los dispositivos que han sido previamente asociados con la aplicación, ya que es la primera vez en ejecutarse la App se debe añadir nuestro DVR dando un toque en el botón ubicado en la parte superior derecha denominada “Add”, en este punto aparece una nueva ventana donde se deberán ingresar todos los parámetros de red que identifican al DVR dentro de la red de acceso mundial, una vez ingresados los datos quedaría registrado el DVR, las pruebas correspondientes se realizarán en el siguiente capítulo.

CAPÍTULO V.

PRUEBAS Y RESULTADOS.

Realizada ya la implementación completa del sistema se procedieron a realizar pruebas de cada uno de los sistemas, para observar su comportamiento individual en un inicio y una vez superados los problemas individuales se procedió a realizar pruebas colectivas donde la interacción de los sistemas definió el correcto funcionamiento del sistema.

Con la realización de estas pruebas se encontraron inconvenientes y soluciones a éstos, los cuales se detallan también a continuación.

A continuación se detallarán las pruebas realizadas a cada uno de los sistemas.

5.1. Pruebas realizadas al Sistema de Detección de Incendios.

- Prueba al Sensor de Humo.
    - Energización e indicadores visuales.
    - Pruebas con humo y verificación de estado de alarma del sensor.
    - Llegada de la señal de alarma del sensor hacia los controladores.
- Prueba a la Estación Manual.

- Activación de la estación manual y verificación de la llegada de la señal al controlador.

Los inconvenientes encontrados al efectuar estas pruebas fueron: con respecto al sensor de humo, su señal en estado de alarma no llegaba al controlador asignado su motivo había sido una mala identificación del par trenzado que acarreaba esta señal lógica hasta el controlador, ya que se encontró el origen del error se pudo corregir el problema.

5.2. Pruebas realizadas al Sistema de Control de Accesos.

- Pruebas al Lector de Proximidad.
  - Energización e indicadores visuales.
  - Lectura y configuración horaria de códigos de tarjetas.
  - Apertura y cierre de cerradura de acuerdo a configuración horaria de tarjetas.
- Pruebas al Pulsador de Salida.
  - Verificación de llegada de señal emitida hacia el controlador.
  - Apertura de cerradura al emitir la señal.
- Pruebas a la Cerradura Electromagnética.
  - Energización e indicadores visuales.

Al momento de efectuar las pruebas se determinaron problemas básicamente con las cerraduras electromagnéticas ya que no se acoplaban correctamente, para solucionar este problema fue necesario elaborar platinas a medida para que la cerradura acople perfectamente con su placa metálica y asegure adecuadamente el ingreso al área al que ha sido determinado el acceso.

5.3. Pruebas realizadas al Sistema Anti-Intrusión.

- Pruebas a Contactos Magnéticos.
  - Verificación de llegada de señal emitida por el dispositivo hacia el controlador.
- Pruebas a Sensores de Movimiento.

- Energización e indicadores visuales.
- Verificación de activación de indicador en el sensor.
- Verificación de llegada de señal emitida por el sensor en estado de alarma hasta el controlador.

En las pruebas realizadas a los sensores de movimiento se determinó que fue necesario modificar su sensibilidad debido a que por defecto este tipo de sensores vienen con una sensibilidad demasiado baja ya que se debían realizar movimientos muy exagerados para que éste actúe por lo tanto fue necesario incrementar la sensibilidad de todos los sensores de movimiento instalados.

- Prueba realizada a Sirenas.
  - Energización y verificación de indicador sonoro.
- Pruebas realizadas al teclado de accesos INM-050.
  - Activación y desactivación de las 3 zonas de vigilancia.

El teclado y su supervisor se han configurado de modo que la zona 1 se active en 40 segundos una vez que el usuario ingresa la orden de armado, mientras que la zona 2 y la zona 3 se activan en 5 segundos después de que el usuario haya ingresado la orden de armado.

a) Zona 2 y Zona 3 activadas en espera de la activación de la Zona 1 para completar el armado.

b) Zona 1,2 y 3 activadas y Armado del sistema Anti-Intrusión.

Figura 103. Armado parcial del sistema Anti-Intrusión.

Como se puede observar en la figura 103.a., se puede observar que no se encuentra encendido el indicador de “Armado”, ni tampoco el de la “Zona 1”, solamente se encuentran encendidos los de la “Zona 2” y “Zona 3”, mientras sigue el conteo hasta que se cumplan los 40 segundo que dispone el usuario para salir de las instalaciones hasta que el sistema anti-intrusión se arme por completo. Finalmente en la figura 103.b., se muestra que los indicadores de “Armado” y el de “Zona 1” se encuentran activados sin titilar, este es el estado que indica que el sistema se encuentra completamente armado.

De igual manera para el ingreso el usuario dispondrá de 40 segundos para desarmar el sistema después de su ingreso antes de que el sistema entre en estado de alarma.

5.4. Pruebas realizadas al Circuito Cerrado de Televisión.

- Pruebas a las Cámaras Análogas.
  - Energización e indicadores visuales.
  - Verificación de llegada de señal de video emitida por el dispositivo hacia el grabador digital de video.
- Prueba realizada al Grabador Digital de Video.
  - Verificación del monitoreo local.

En la siguiente figura se muestran las imágenes reales de las pruebas que se han realizado al sistema de video tanto en el monitoreo local como remoto.

Figura 104. Pruebas de monitorización local.

Como se observa, en la parte superior la cámara 1 se encuentra enfocando al hall de la planta alta 1, la cámara 2 enfoca la sala de reuniones de la empresa, mientras que la cámara 3 está orientada para permitir el monitoreo de las actividades que se realizan en el área de operaciones y finalmente la cámara 4 enfoca el ingreso a la bodega y su interior.

- Verificación del monitoreo remoto.

Figura 105. Pruebas de monitoreo remoto desde computador.

En la figura 105., una vez realizadas todas las configuraciones descritas en el capítulo anterior, se podrían seleccionar los canales de la lista que se encuentra en la zona izquierda de la interfaz y monitorearlos remotamente desde el navegador web, así como realizar descargas de tramos horarios que pueden ser solicitados por el usuario realizando los pasos descritos más adelante.

Como se había mencionado en el capítulo anterior se puede realizar el monitoreo del Circuito Cerrado de Televisión tanto desde un computador así como desde un Smartphone, de modo que a continuación se muestra en la figura 106., la selección de los canales que se van a monitorear.

Figura 106. Lista de canales disponibles del DVR.

Una vez que se han seleccionado los canales a ser monitoreados se regresa a la pantalla principal de la aplicación que se puede observar en la figura 107.

A continuación se muestra una captura de pantalla del terminal desde el cual se realizó el monitoreo.

a) Vista de la aplicación con el terminal en posición vertical.

b) Vista de la aplicación y monitoreo de cada una de las cámaras con el terminal en posición horizontal.

Figura 107. Monitoreo remoto desde dispositivo Android OS.

- Verificación de la descarga y reproducción de videos por tramos horarios solicitados por el usuario.

El DVR mediante su interfaz para el monitoreo remoto desde el navegador web en el computador, brinda la opción tanto de la descarga como de la reproducción en línea, de cualquiera de sus canales, por tramos horarios determinados por el usuario para su revisión o análisis. En la figura siguiente se indican los pasos para realizar la descarga del video desde el DVR una vez que se ha ingresado remotamente al mismo.

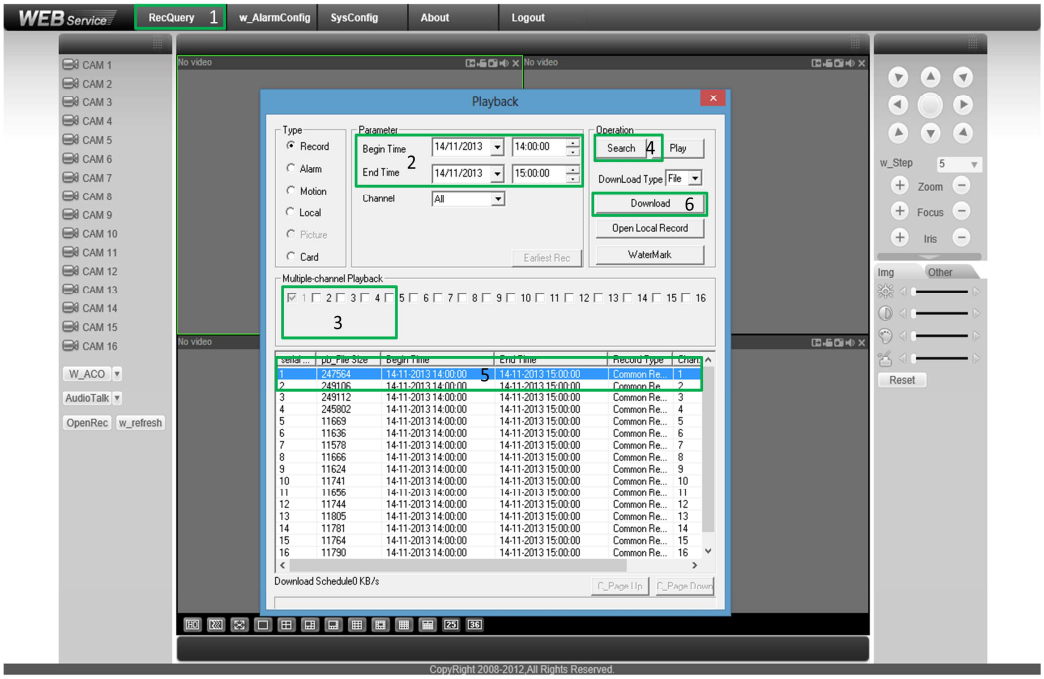


Figura 108. Pasos para descargar video en tramo horario desde el DVR.

En la figura anterior se muestran los pasos a seguir para realizar la descarga remota del video en tramo horario desde el DVR. Inicialmente una vez ingresado a la plataforma se hace clic en el primer botón de la barra de herramientas, a continuación se abre una nueva ventana denominada “Playback”, aquí se ingresará el tramo horario del cual se solicitará el video, también de que canales se va a solicitar el video. En el ejemplo propuesto se realizaría la descarga de una hora específica en un mismo día del canal 1, a continuación se realiza la búsqueda y se selecciona el único que tiene en lista el canal 1 y se procede a descargar.

Para la reproducción en línea el proceso es similar hasta la búsqueda del video como se muestra a continuación.

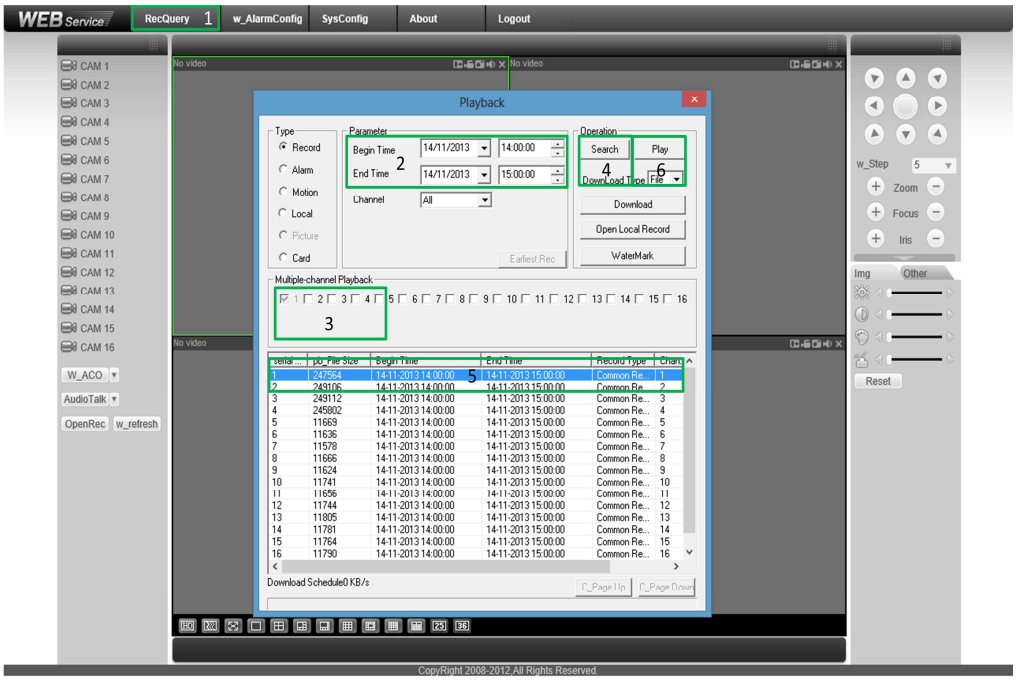


Figura 109. Pasos para reproducir en línea.

- Verificación del funcionamiento de las entradas de alarma hacia el DVR y el envío de correos.

Esta prueba se trata de la más importante debido a que el DVR es el encargado de generar los correos hacia los destinatarios en caso de que se produjese una alarma por perdida de video en alguna de sus cámaras, por incendios o por la activación de la alarma debido a una intrusión en las instalaciones de SRT HARDCOM S.A.

Una vez realizada la configuración de parámetros que se muestra en la figura 4.46., se genera inicialmente un correo de prueba que será emitido a los tres destinatarios que se ha decidido que sean los que deben estar pendientes de estas alarmas.

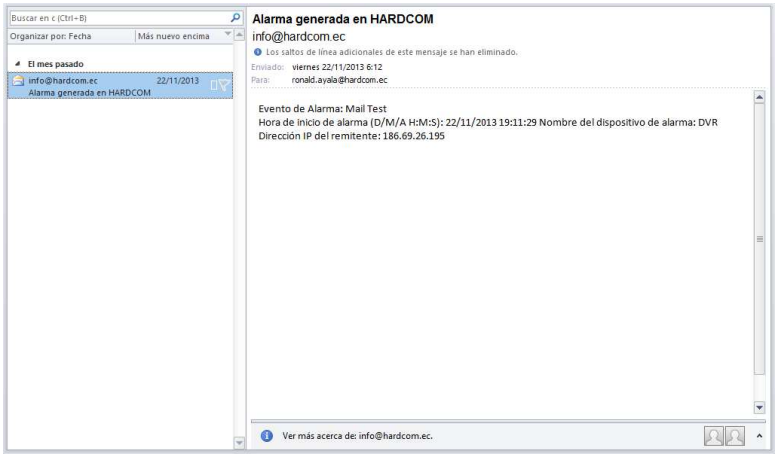


Figura 110. Correo de prueba enviado por el DVR.

En la figura anterior se muestra que el DVR ha sido capaz de generar y enviar los correos a los destinatarios, en este momento resta realizar pruebas reales de generación y envío de correos. Entonces al producirse una de las alarmas indicadas anteriormente, el DVR genera y envía un correo a los tres destinatarios como se puede observar a continuación.

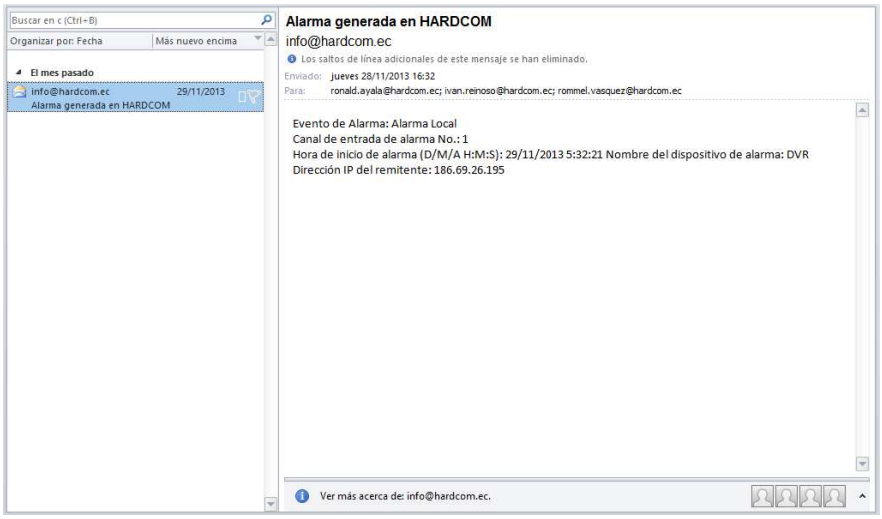


Figura 111. Correo generado por Activación de Alarma.

El correo de la figura 111., es el que genera y envía el DVR al haberse producido una activación de la alarma debido a una violación del sistema de seguridad. En el correo se detalla el evento, “Alarma Local”, que se ha producido para el envío del correo además de la hora y fecha en que se produjo y el nombre y la dirección IP del DVR del que ha sido emitido el correo electrónico.

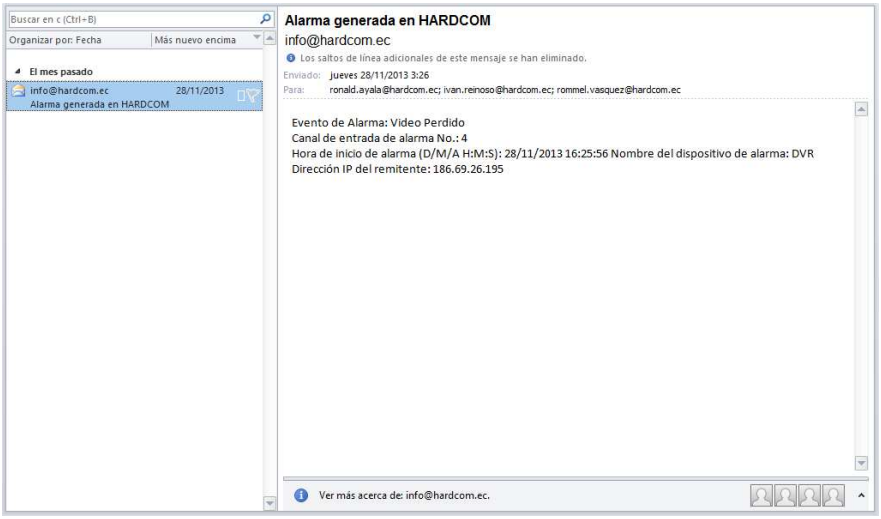


Figura 112. Correo generado por Video Perdido.

Otro de los motivos por lo que el DVR puede generar y enviar un correo electrónico es debido a la pérdida de video en uno de sus canales, esto se lo configuró de esta manera para que el usuario al recibir este correo esté enterado de que una de sus cámaras está con problemas y opte por realizar una revisión de la misma.

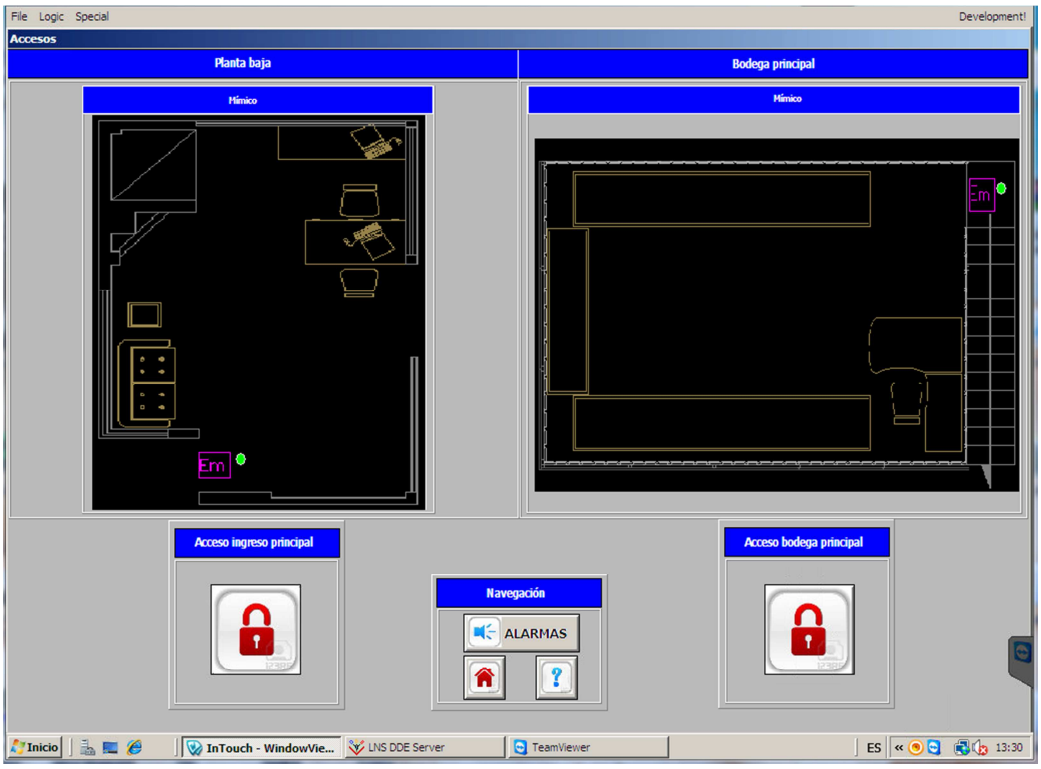
5.5. Pruebas realizadas a la interfaz de usuario o HMI.

La pruebas que se realizarán a la interfaz serían en cuanto a la comunicación y respuesta en tiempo real de los datos o indicadores que presenta la interfaz del control de accesos y del sistema anti – intrusión.

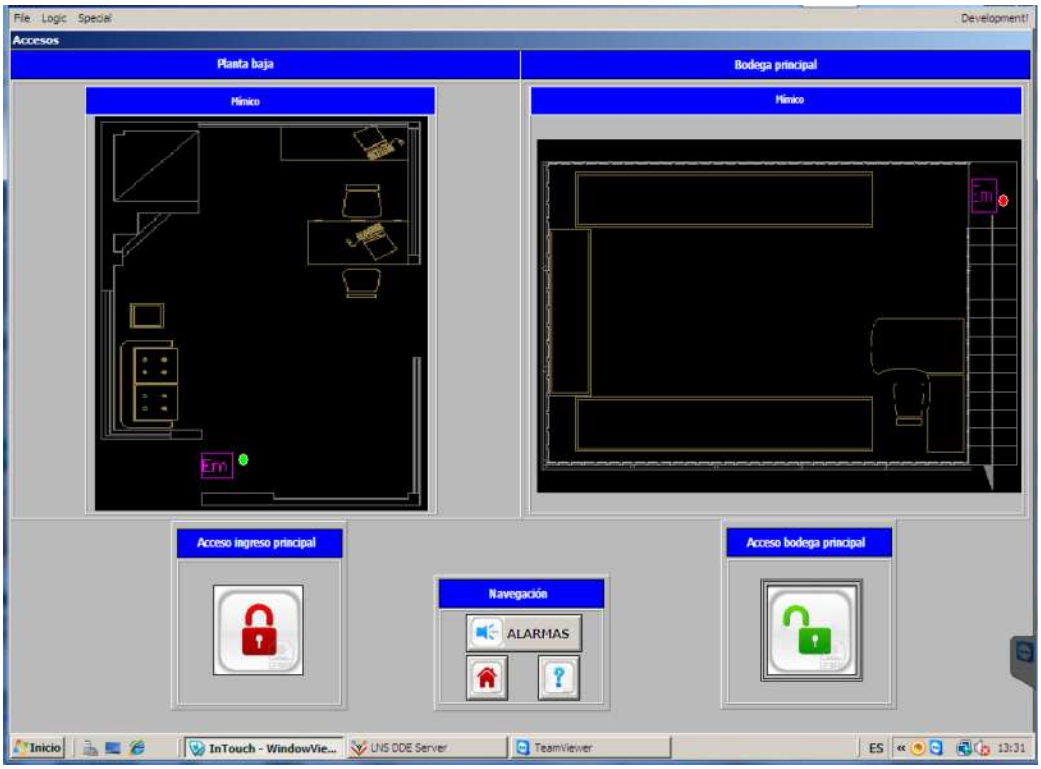
- Pruebas a la interfaz del control de accesos.
  - Verificación física del estado del actuador y estado que presenta la interfaz.
  - Verificación física del cambio de estado al realizar el pulsado del botón de la interfaz para la apertura remota de la puerta ya sea del ingreso principal como de la bodega.

A continuación en la figura se muestra el estado normal de los actuadores mientras no se da ninguna orden de apertura de las puertas, seguidamente mediante la pulsación del botón correspondiente a la puerta de la bodega nótese que tanto como el botón como el indicador del actuador cambian de

estado, el botón a su figura de “Desbloqueo de puerta” y el indicador pasa a color “Rojo” indicando que se ha desactivado el electroimán.



a)Estado normal de los actuadores.

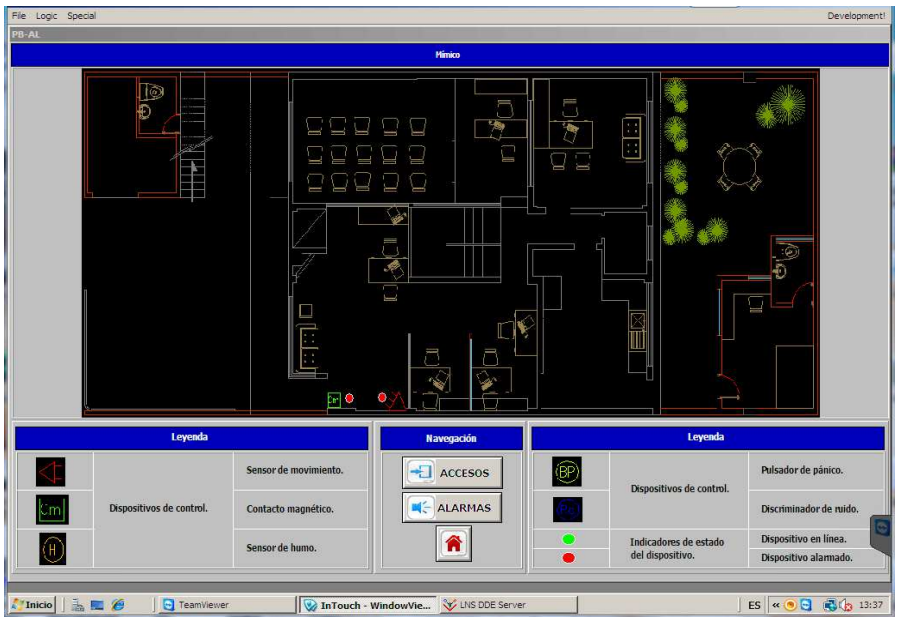


b) Apertura de puerta de la bodega.

Figura 113. Interfaz de control de accesos.

- Pruebas a la interfaz del sistema Anti-Intrusión.
  - Verificación física del estado del sensor o actuador y el estado que presenta la interfaz.
  - Tiempos de actualización entre la ejecución del evento y su presentación en la interfaz.
    - Pruebas en la interfaz de la Planta baja.

a) Estado en línea de los dispositivos.

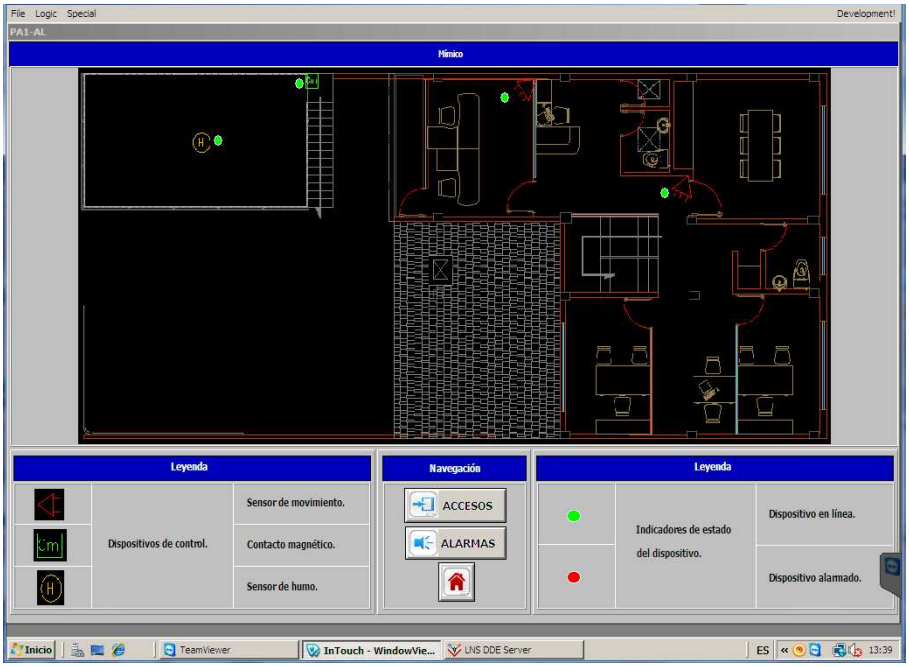


b) Estado en detección de los dispositivos.

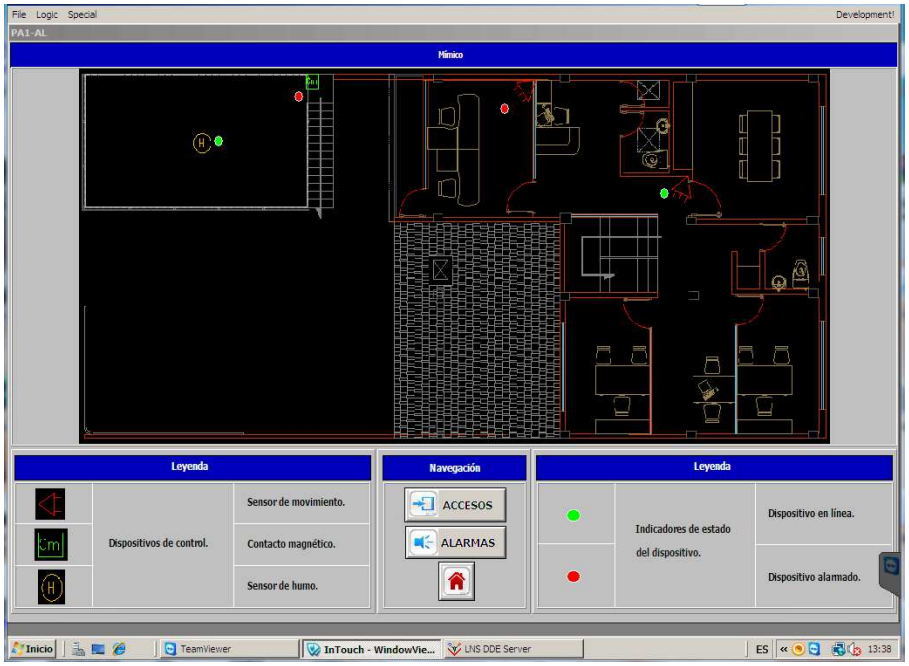
Figura 114. Estado de los dispositivos de la planta baja.

En la figura 114., se muestran los estados de los dispositivos en estado normal y una vez que han sido activados por el ingreso de una persona por la puerta principal provocando la apertura del contacto magnético y la detección de movimiento.

- Pruebas de la interfaz de la planta alta 1.



a) Estado en línea de los dispositivos.

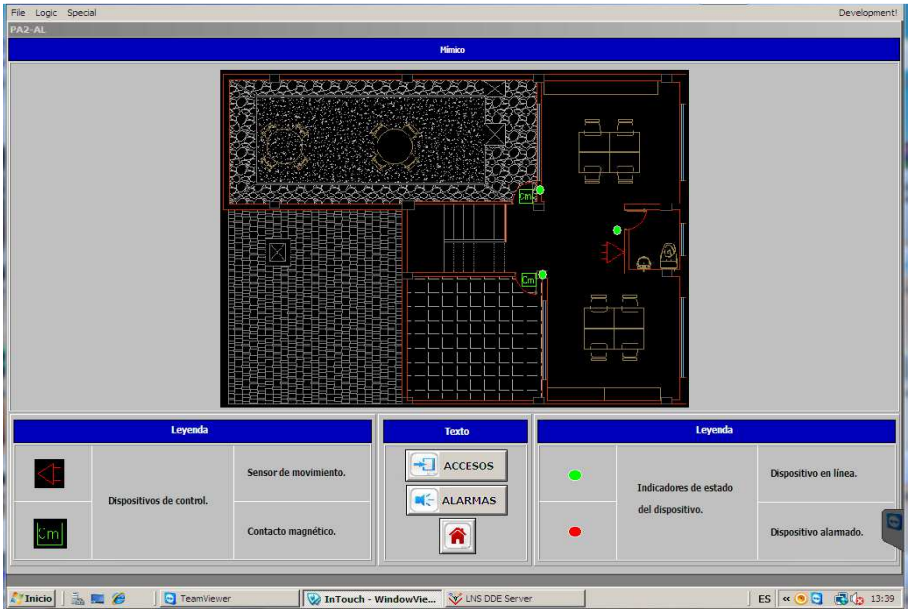


b) Estado en detección de los dispositivos.

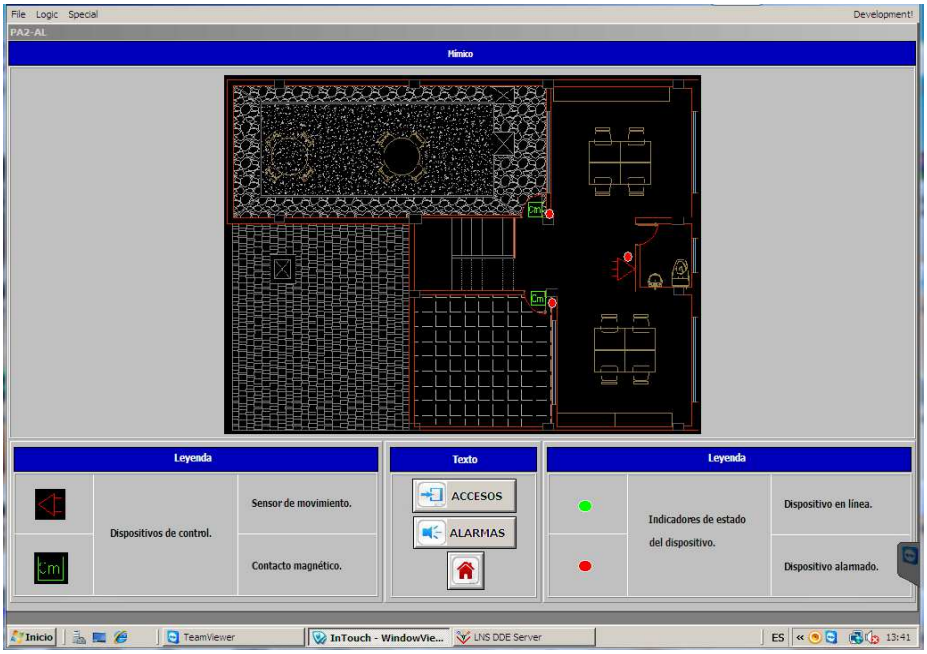
Figura 115. Estado de los dispositivos de la planta alta 1.

Para mostrar la activación de los dispositivos se pidió al usuario que abriera la puerta de la bodega e ingresara a la oficina de DIMOSE para verificar el estado en detección del contacto magnético y del sensor de movimiento de la oficina.

- Pruebas de la interfaz de la planta alta 2.



a) Estado en línea de los dispositivos.



b) Estado en detección de los dispositivos.

Figura 116. Estado de los dispositivos en la planta alta 2.

En la figura 116., se muestran los estados en línea y en detección de los dispositivos, esta vez para que entren en modo de detección se ha pedido al usuario que abras las puertas de la terraza y por consiguiente se activará también el sensor de movimiento.

El tiempo de actualización desde que sucede el evento hasta que se presenta el cambio de estado en la interfaz corriendo el escritorio remoto desde un computador de la red local es de 1 segundo, mientras que el tiempo de actualización al estar corriendo el escritorio remoto desde una red externa es de 3 segundos.

Tabla 24. Tiempos de respuesta del sistema

	Tiempo de actualización	
	En red local	**En red mundial**
Sensores	1 segundos	3 segundos
Actuadores	1 segundos	3 segundos
	Tiempo de envío de correos	
DVR	1 segundo	

En la tabla 24., se muestra adicionalmente el tiempo que transcurre desde que el evento de alarma ha ocurrido hasta que el usuario recibe el correo electrónico habiendo pasado por el proceso del grabador digital de video que genera y envía el correo.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES.

6.1. CONCLUSIONES

- Se logró repotenciar nodos de control ISDE-ING, INS-460 e INS-231 que disponía la empresa, integrándolos en el sistema de los que no se estaban aprovechando todas sus capacidades y representaban una pérdida tanto económica como tecnológica para la empresa.

- La efectiva solución que representa el haber utilizado el protocolo LONWorks como plataforma para el sistema de seguridad electrónica permitió que la flexibilidad y la gran capacidad de integración de éste estándar sean la clave para la ejecución del proyecto y la superación de las expectativas.

- La pérdida o retraso de datos pudo haberse evitado realizando una ductería diferente para cada tipo de cable a ser trasladado, desde un principio, ya que al mezclar las instalaciones eléctricas con el cableado

de control se produjeron interferencias emitidas por el cableado eléctrico.

- El haber implementado el sistema de seguridad electrónica basado sobre un estándar, aplicado y reconocido internacionalmente, dio paso a la integración del sistema con la interfaz desarrollada en InTouch mediante el protocolo de intercambio dinámico de datos manejado por ambas plataformas.

- La flexibilidad que presentan los nodos de control LONWorks desarrollados por ISDE-ING se convierten en una ventaja al momento de la selección de los dispositivos periféricos ya que no se tiene como referencia a un solo fabricante.

- Este sistema de seguridad electrónica desarrollada para la empresa SRT HARDCOM S.A., al haber cumplido con las normas y requerimientos exigidos para la ejecución de sus proyectos ha decidido incluir en su carta de servicios el uso de tecnología estándar LONWorks en trabajos de similares características.

- A opinión del usuario se logró desarrollar una interfaz agradable a la vista, intuitiva y eficiente, objetivo alcanzado siguiendo las recomendaciones que indica la guía ergonómica de diseño de interfaces de supervisión (GEDIS).

6.2. RECOMENDACIONES

- Un adecuado enrutamiento previo a la ejecución del cableado optimiza las distancias que se deberá recorrer para alcanzar los puntos de conexión de cada dispositivo.

- Antes de la energización de los dispositivos que comparten la alimentación desde una misma fuente, como las cámaras análogas, se deben verificar que todas tengan la misma polaridad en sus tomacorrientes ya que al compartir barras podrían producirse corto circuitos o daños en el artefacto.

- La correcta configuración horaria programada en el grabador digital de video, permite optimizar el espacio que vaya a ser ocupado del disco duro no teniendo que realizar grabaciones en la noche sin que un evento aparezca.

- Se deben tomar muy en cuenta los identificadores y los nombres que se coloque a cada uno de los nodos para evitar la vinculación errónea de los indicadores de la interfaz con variables de red del mismo nodo o de otros nodos.

- Si la interfaz no se la realiza directamente en el computador que va a realizar el control, se debe tomar en cuenta la resolución máxima con la que puede operar este computador para evitar el auto ajuste al instalar la interfaz ya que se pueden echar a perder los gráficos que contenga la interfaz.

- En el caso de que el cableado las cámaras análogas sea realizado con par trenzado y no con cable coaxial, debe tener en cuenta la calidad del adaptador balun ya que de éste dependerá la calidad de la imagen que presente el monitor.

- Un bien elaborado plan de trabajo con una adecuada difusión del mismo permite alcanzar los objetivos planteados en los tiempos estimados en el proceso de diseño.

- Es necesaria la capacitación sobre el uso del sistema de seguridad electrónica a una persona que sea responsable de discriminar por área la información del funcionamiento de este sistema ya que las herramientas de monitoreo y control no pueden ser utilizadas por cualquier personal de la empresa.

BIBLIOGRAFÍA

Control-Accesos. (7 de 3 de 2008). *Teoría de Protocolo de comunicaciones Wiegand*. Obtenido de http://control-accesos.es/protocolos/protocolo-wiegand

DAHUA. (2010). *Mobile Phone Monitor Software User´s Manual.* China: Dahua.

DAHUA. (2013). En DAHUA, *N56 Series DVR User´s Manual* (págs. 34-45). China.

ECHELON. (2002). *LNS DDE User´s Guide.* San Jose, California: ECHELON.

ECHELON. (2006). *U10/U20 USB Network Interface.* San José, California: Echelon.

Echelon. (2007). *Guía de Diseño de Redes LONWorks.* España: Aditel Sistemas.

ECHELON. (2012). *LONMaker® User´s Guide.* Silicon Valley: ECHELON.

ISDE-Ing. (2005). *Manual Técnico INM-050TX/V3.* Madrid: ISDE.

ISDE-Ing. (2005). *Manual Técnico INP-120X/V3.* Madrid: ISDE.

ISDE-Ing. (2005). *Manual Técnico INS-080X/V3.* Madrid: ISDE.

ISDE-Ing. (2005). *Manual Técnico INS-231TX/V3.* Madrid: ISDE.

ISDE-Ing. (2005). *Manual Técnico INS-460X/V3.* Madrid: ISDE.

José Manuel Huidobro, Ramón Jesús Millán Tejedor. (2010). Manual de Domótica. España: Creaciones Copyright

Pere Ponsa, A. G. (2009). Diseño de Pantalla. En P. Ponsa, *Diseño Industrial* (págs. 2-23). Madrid.

Roberto Mantiñan Ruanova.(29 de Octubre del 2012). Buses y protocolos en domótica e inmótica. Obtenido de http://www.slideshare.net/robertomantinanruanova/buses-y-protocolos-en-domotica-e-inmotica

SOYAL. (2008). *Access Control System.* Hong Kong: SOYAL.

SOYAL. (11 de 1 de 2008). *SOYAL*. Obtenido de http://www.soyal.com.hk/english/readers.htm

Wonderware®. (2007). *InTouch® HMI 10 Foundamentals of Application Development Course.* Lake Forest, California: Invensys.

Wonderware®. (2009). *Wonderware*. Obtenido de http://www.wonderware.es/