UNIVERSIDAD SAN FRANCISCO DE QUITO

Colegio de Ciencias e Ingeniería

“Caja de seguridad electrónica biométrica”

Germán Eduardo Luzuriaga Hidalgo.

Omar Aguirre MSC., Director de Tesis

Tesis de grado presentada como requisito para la obtención del título de Ingeniero Electrónico

Quito, mayo de 2015

Universidad San Francisco de Quito

Colegio de Ciencias e Ingeniería

HOJA DE APROBACIÓN DE TESIS

“Caja de seguridad electrónica biométrica”

Germán Eduardo Luzuriaga Hidalgo

Omar Aguirre MSC.,
Director de Tesis
……

Nelson Herrera Ing.,
Miembro del Comité de Tesis ……

René Játiva, DEA.,
Miembro del Comité de Tesis ……

Ximena Córdova, Ph.D.,
Decana de la Escuela de Ingenierías ……

Quito, mayo de 2015

©DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído la Política de Propiedad Intelectual de la Universidad San Francisco de Quito y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo de investigación quedan sujetos a lo dispuesto en la Política.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo de investigación en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma:

Nombre: Germán Eduardo Luzuriaga Hidalgo

C. I.: 1711921492

Lugar y fecha: Quito, mayo de 2015

AGRADECIMIENTOS

A mis Director de Tesis Omar Aguirre por la paciencia en la dirección del presente trabajo y en toda mi carrera universitaria, a mi Institución por darme la oportunidad de ingresar a tan prestigiosa Universidad, a todos y cada uno de los docentes y personal administrativo de la Universidad San Francisco de Quito por sus valiosos conocimientos impartidos los que me han pulido mi saber cómo a un diamante y un agradecimiento muy especial a Cesar Cisneros por enseñarme a vender las cosas que imagino.

DEDICATORIA

A Dios por darme a mis Padres, a mis Padres por darme la vida y a la vida por darme la familia que tengo que ha sido mi inspiración para cumplir todas mis metas.

RESUMEN

El principal objetivo del presente trabajo de tesis consiste en realizar el diseño y construcción de una "**Caja de seguridad electrónica biométrica**" para guardar armas de fuego, que además de las características físicas de su blindaje resistente a las diferentes condiciones climáticas existentes en nuestro país, resista también el impacto de proyectiles calibre 9mm accionados por armas cortas y que las características del funcionamiento electrónico de los dispositivos seleccionados permitan el control absoluto del ingreso y salida de las pistolas individualizado a los usuarios y las armas designadas a cada uno de ellos con su respectiva munición. Cuando nos referimos a los usuarios del sistema se considera potencialmente a policías, militares y guardias de seguridad, es decir que el presente desarrollo tentativamente tiene el objetivo de ser implementado dentro de los cuarteles, unidades y repartos donde exista armamento con especial atención a las Unidades de Policía Comunitaria las que se han convertido en mini-cuarteles donde se almacena todo el equipo de dotación que dispone un policía para realizar su trabajo cotidiano y debe contener dispositivos de seguridad que resguarden el armamento en beneficio de la comunidad. Los componentes comerciales utilizados en la caja de seguridad además de los implementados por desarrollo propio deberán ser integrados en un solo circuito para que funcionen de manera óptima y permitan alcanzar un nuevo producto vanguardista capaz de satisfacer las necesidades de los organismos y cuerpos de seguridad nacional e internacional.

El presente desarrollo se ha dividido en cinco capítulos, en el primero se especifica el fundamento teórico en el cual se basa el diseño de la "**Caja de seguridad electrónica biométrica**". Luego de ello el capítulo segundo especifica los detalles y la elaboración del producto final donde se han establecido las condiciones de diseño considerando las características de la caja de seguridad y los sistemas utilizados.

En el tercer capítulo se analizan las especificaciones y detalles de ejecución donde constan de manera detallada su diseño electrónico, el diseño mecánico y la estructura operativa del proyecto con la finalidad de satisfacer las necesidades determinadas en el capítulo anterior.

En el capítulo cuarto se especifica el presupuesto asignado al desarrollo del sistema, recalcando la valoración individual de cada componente así como la inversión total del proyecto.

En el siguiente capítulo cinco consta de las conlcluisones y recomendaciones del funcionamiento del producto final donde se realiza una valoracióin de la importancia del desarrollo final.

Para finalizar se han incluido en los anexos las características de cada uno de los componentes seleccionados en el presente desarrollo.

ABSTRACT

The main objective of this thesis is to perform the design and construction of a "Safe Electronic biometric" to save fire guns, in addition to the physical characteristics of its tough can resist different climatic conditions that you can find in our country , also resist the impact of projectiles of 9mm hand weapon and the characteristics of the electronic operation of selected devices allow complete control of the entry and the exit of individual users guns and weapons designated, each with its respective ammunition. When we refer to the system's users is considered potentially police, soldiers and security guards, namely that this development tentatively have the objective to be implemented in the headquarters, units and distributions where the units there weapons with special attention to the community policing which have become mini-barracks where all the equipment available to a police officer staffing, to perform their daily work and should contain safety devices that protect the weapons for the benefit of the community. The commercial components used in the safe in addition to those implemented by own development must be integrated into a single circuit, to have a optimally function and to achieving a new breakthrough product able to meet the needs of agencies and persons of National and International security.

This development has been divided into five chapters, the first we show and specified the theoretical foundation on which the design of the "biometric electronic security box" is based. After that the second chapter specifies the details and preparation of the final product where they have established design conditions considering the characteristics of the safe and the systems we used.

In the third chapter details the specifications and implementation which consist in detail of electronic design, the mechanical design and operational structure of the project in order to meet the needs identified in the previous chapter.

In the fourth chapter the budget allocated to the development of the system is specified; show the individual valuation of each component and the total project investment.

In the next chapter consists in the conclusion and recommendations of the function of the final product where the importance of the final development is valuated.

Finally they have been included in the annexes the characteristics of each of the components selected in this development.

TABLA DE CONTENIDOS

INTRODUCCIÓN

En el Ecuador y Latinoamérica a través de la historia ha sido un factor común las dictaduras militares y la caída de gobiernos democráticos elegidos por elección popular por el retiro del apoyo de las Fuerzas Armadas y Policías por circunstancias políticas, sociales y económicas, lo que ha llevado a generar varias crisis que muchas veces las armas dotadas a uniformados, para el cumplimento de su deber constitucional de custodiar la soberanía nacional y precautelar el orden interno y la seguridad social, han sido utilizadas en contra de la población civil y el pueblo, quien eligió en su momento a las autoridades de gobierno en la que más de una vez han existido lamentables pérdidas humanas, las cuales han sido violentados sus derechos.

Los organismos estatales de seguridad se deben a la protección del pueblo y no pueden ser utilizados bajo ningún interés de grupos de poder u otras circunstancias en contra de quien deben servir. Es la sociedad civil a quien le compete el control y monitoreo del correcto uso de las armas de dotación entregadas a los uniformados para que cumplan su deber consagrado en la Constitución de la República.

Solo en nuestro país en los últimos 20 años se ha tenido el derrocamiento de tres presidentes y un sin número de hechos lamentables como el 30 de septiembre del 2010 en la que hubo un enfrentamiento entre militares y policías donde fallecieron ciudadanos uniformados y civiles.

En el Ecuador por su posición geográfica a nuestro vecino país del norte más de una se ha desviado de los cuarteles militares armamento bélico hacia fuerzas irregulares así también en el transcurso de la historia han existido varios asaltos de rastrillos donde han sido sustraídos gran cantidad de armamento como lo que ocurrió en el asalto y robo del Rastrillo General de la Policía en el sector del batán por miembros del grupo armado Alfaro Vive Carajo en el año 1985.

Todos estos hechos lamentables que de haber tenido el presente desarrollo y la debida tecnología de control y monitoreo permite habrían sido menor los daños y tal vez las páginas de nuestra historia no se habrían teñido de sangre ya que el poder ejecutivo no

debe ser un condicionante para gobernar el apoyo irrestricto de las FFAA y policía sino más bien al apoyo permanente de los mandantes quienes eligen a sus autoridades.

La Policía está en nuestra sociedad para servir y proteger a la ciudadanía, en este contexto, las personas y principalmente las instituciones públicas y privadas que manejan armas de fuego, se ven en la necesidad de resguardarlas de la delincuencia o eventos inesperados como una catástrofe natural o ya sea producida por el hombre.

Es por esto que se da la necesidad de crear un producto que llene las expectativas de seguridad de estas instituciones a través del manejo de una caja fuerte inteligente que sea abierta a través de un sistema digital biométrico y además que cumpla con características de seguridad.

CAPÍTULO I

FUNDAMENTOS TEÓRICOS

La "**Caja de seguridad electrónica biométrica**" consiste en una caja metálica que dispone de varios compartimentos asignados a diferentes usuarios que pueden ser policías, militares o guardias de seguridad para que guarden de forma individual sus armas de fuego mediante un manejo seguro y con un control sistematizado de registro de ingresos y egresos. El presente desarrollo utiliza un sistema biométrico de huella digital, dispositivos de tecnología ZIGBEE , internet inalámbrico y su monitoreo es permanente en tiempo real mediante cámaras de audio y video las cuales mediante una central de vigilancia que en caso de sabotaje, conmoción nacional o manifestaciones puedan ser bloqueados o inhabilitados emergentemente para su buen recaudo y ser habilitados nuevamente luego de que las condiciones de riesgo hayan pasado.

1.1 Caja fuerte

1.1.1 Definición

Una caja fuerte es un instrumento de varias formas que sirve para albergar objetos, joyas, dinero y cualquier artículo de valor para su propietario (Diccionario, 2013). Son muy difícil de abrirlas, el material que se utiliza para la fabricación es un metal extremadamente duro resistente al fuego, al agua y a balazos; además se ha utilizado materiales que resisten a pequeñas explosiones.

1.1.2 Huellas digitales

La huella digital está constituida por rugosidades que forman salientes y depresiones las mismas que son únicas para cada individuo, Las salientes se denominan crestas papilares y las depresiones surcos interpapilares.

Figura No. 1: Huella digital

Fuente: (González, 2011)

1.1.3 La dactiloscopia

"Es una ciencia que trata de la identificación de la persona humana por medio de las impresiones digitales. Es una ciencia de aplicación fundada en una verdad absoluta. Es la única rama del derecho que descansa en un fundamento analítico." (Vergara, 2011, pág. 1)

1.1.4 Imágenes digitales.

La digitalización de imágenes es el proceso por medio del cual se convierte una imagen en un formato interpretable por las computadoras. Una imagen digital se puede obtener utilizando cámaras fotográficas digitales, escáneres, periféricos biométricos, etc.

1.4.1.1 Resolución de las imágenes digitales.

La resolución es un factor que se utiliza para convertir las dimensiones de una imagen física a píxeles de una imagen digital y viceversa. Si por ejemplo una fotografía es digitalizada a 300 dpi (Dots Per Inch) o puntos por pulgada, significa que por cada pulgada de la fotografía física original se van a obtener 300 píxeles en la imagen digitalizada.

1.4.1.2 Proceso de reconocimiento de imágenes – algoritmos.

La función diferencia es la base del reconocimiento de imágenes; ya que indica la distancia entre dos imágenes.

Existen diversas estrategias para reconocimiento de imágenes digitales de acuerdo al tipo de aplicación y de los recursos del sistema:

Método lineal.

La manera más directa de comparar la imagen original con una colección de imágenes, es comparar cada píxel del cuadro de la imagen original con su correspondiente píxel en la imagen de la colección de imágenes y acumular las distancias entre cada pareja de píxeles para determinarla distancia general entre las dos imágenes. Aunque esta es una estrategia relativamente buena para comparar imágenes, la cantidad de comparaciones necesarias es muy grande. Por cada comparación debe calcularse la distancia entre los píxeles de las dos imágenes.

Método cuadrático.

Se puede acentuar el efecto de la diferencia de cada píxel utilizando una diferencia cuadrática o distancia euclidiana.

1.2 Biometría.

"La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas como es la huella digital. (Alegsa, 2010)"

Los sistemas Biométricos incluyen dispositivos de captación y un software biométrico que interpreta la muestra física y la transformada en una secuencia numérica, que en el reconocimiento de huella digital se deberá tomar en cuenta que en ningún caso se extrae la imagen de la huella, sino más bien una secuencia de números que la representan (patrón digital).

El uso de Biometría aplicada a Sistemas Informáticos da la ventaja de la seguridad ya que el uso de passwords va quedando de lado frente al uso de esta tecnología.

1.2.1 Biometría y seguridad

El concepto clásico de biometría denota la aplicación de técnicas matemáticas y estadísticas al análisis de datos en las ciencias biológicas. Dentro del contexto tecnológico, la biometría expresa la aplicación automatizada de técnicas biométricas a la certificación, autentificación e identificación de personas en sistemas de seguridad. Las técnicas biométricas se utilizan para medir características físicas o de comportamiento de las personas con el objetivo de establecer una identidad.

1.2.2 Características de los rasgos biométricos

Para que una característica física o de conducta sea considerada como una característica biométrica, esta debe cumplir con las siguientes propiedades:

Universalidad: todos los individuos deben tener la característica.

Unicidad: dos personas no pueden ser la misma en términos de la característica.

Permanencia: la característica debe ser invariante con el tiempo.

Cuantificable: la característica puede ser medida cualitativamente.

Realización: referido a si es posible la identificación exacta, los recursos requeridos y los factores del entorno y de trabajo que afectan a la identificación.

Aceptabilidad: referido a la extensión de población que estaría predispuesta a aceptar el sistema de identificación.

Engañable: referido a cuan fácil sería engañar al sistema con técnicas fraudulentas.

1.2.3 Ventajas

El sistema biométrico proporciona un mayor grado de seguridad en comparación con sistemas tradicionales ya que libera al usuario de la utilización de elementos externos auxiliares tales como, claves, tarjetas, llaves, etc.

1.2.4 Estructura general de un sistema biométrico

Un sistema biométrico esencialmente es un reconocedor de patrones que captura datos biométricos de un individuo, extrae un conjunto de características a partir de dichos datos y las compara con otros patrones previamente almacenados en el sistema

En la grafica se muestra la estructura general de un sistema biométrico.

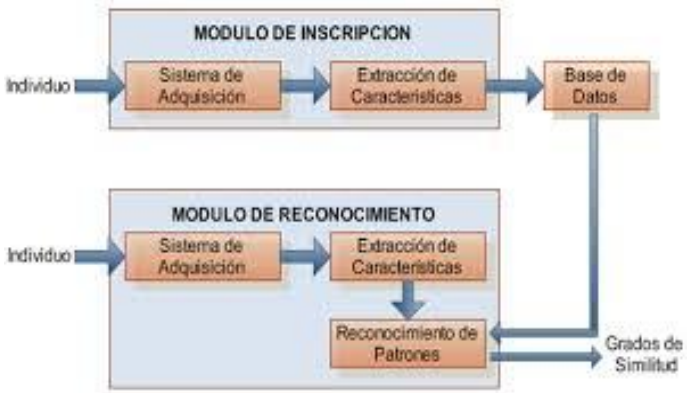


Figura No. 2: Estructura de un sistema biométrico

Fuente: (Werner, 2011, pág. 8)

A continuación se describe cada una de estas etapas:

Adquisición de datos:

A través de un sensor se escogen datos analógicos para luego ser transformados a un formato digital, este sensor debe tener características técnicas que garanticen la calidad y cantidad de datos, ya que son el pilar fundamental para los procesos siguientes.

Preprocesado:

La señal proveniente de la adquisición en ocasiones suele tener ruidos o distorsiones, así que se necesita una etapa de procesamiento de esta señal que elimine los mismos.

Extracción de características:

En esta etapa se extrae únicamente aquellas características que sean discriminantes entre distintos individuos y que al mismo tiempo permanezcan invariables

Generación de un modelo y comparación de patrones:

Una vez extraídas las características más significativas, se elabora un modelo que representa a cada individuo. Dichos modelos se almacenan en la base de datos del sistema y permiten, en la etapa operativa del sistema de reconocimiento, la comparación entre los datos que se capturen y el modelo de un individuo en particular.

Base de datos:

Es donde se almacenan los modelos que representan la identidad de cada usuario del sistema.

Umbral de decisión:

Es el comparador entre los datos de entrada y un modelo de identidad extraído de la base de datos.

1.2.5 Tecnologías Biométricas

En la actualidad existen varias tecnologías biométricas, debido a las características biométricas, algunas de estas son: voz, huellas dactilares, cara, iris, retina, venas de la mano, forma de la mano.

Reconocimiento facial

Este tipo de sistemas extrae los rasgos de la cara para la identificación de usuarios. Para realizar esta identificación se puede utilizar imágenes fotográficas o video, adicionalmente esta identificación puede hacer en 2D o en 3D o combinando las dos,

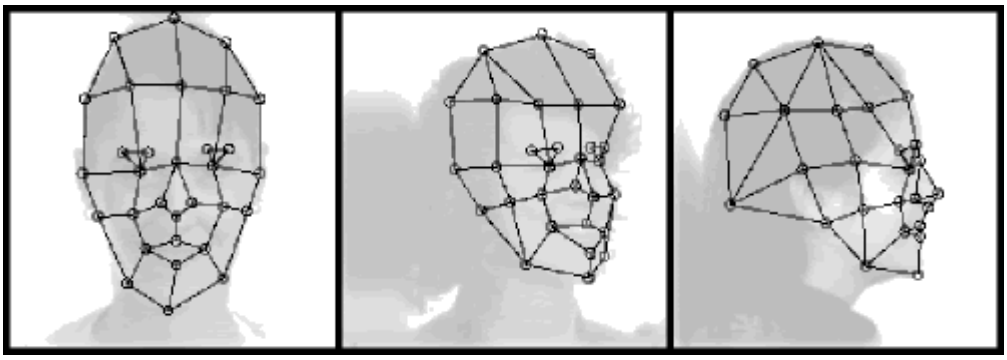


Figura No. 3: Reconocimiento Facial

Fuente: (biometría, 2006, pág. 14)

Reconocimiento de voz

La voz es una característica de identificación de una persona, la misma que es una combinación de características fisiológicas las mismas que vienen dadas por el tamaño de la cavidad del tracto vocal, y son comunes para cada individuo, sin embargo esta característica depende mucho de varios factores como el tiempo, la edad, el estado de ánimo, provocando una desventaja en comparación con otro tipo de característica biométrica

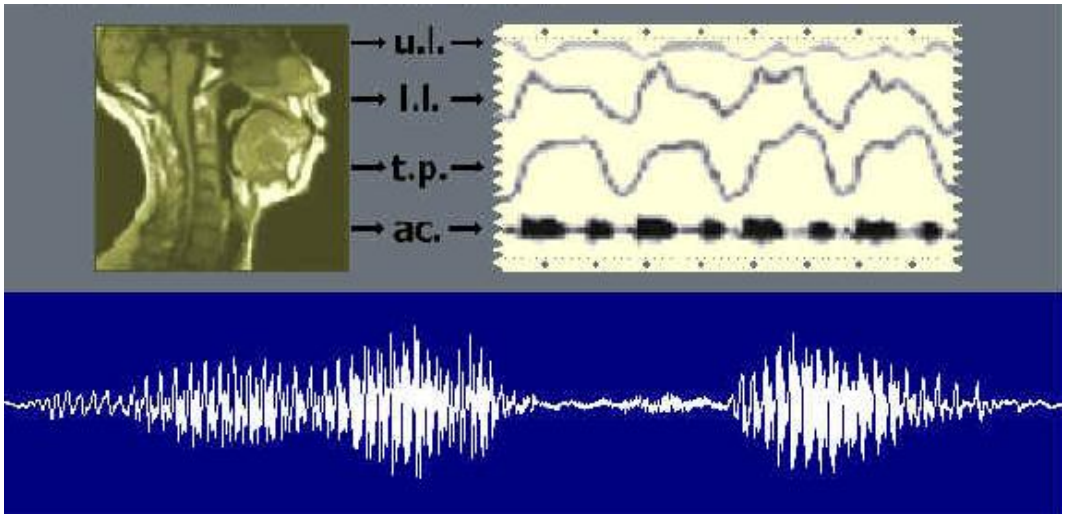


Figura No. 4: Reconocimiento de voz

Fuente: (Arrabales, 2002, pág. 1)

Reconocimiento de iris

El iris es una región anular en el ojo que se encuentra entra la pupila y la esclera, la textura que posee este permitirá obtener información compleja que es muy distintivo para cada individuo, El iris se presenta ante la comunidad científica como el rasgo biométrico más identificativo (a excepción del ADN, si bien éste no suele considerarse un rasgo biométrico en aplicaciones civiles, al no permitir el reconocimiento en tiempo real), si bien recientes evaluaciones competitivas han puesto en entredicho este presupuesto. Otra ventaja del iris es que su captura no precisa contacto físico con el sensor.

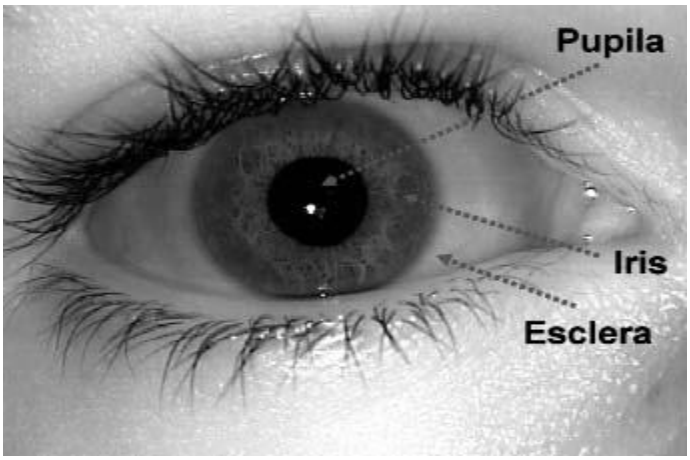


Figura No. 5: Reconocimiento de iris

Fuente: (Cipollone, 2000, pág. 2)

1.3 Tecnología RFID

La identificación por radiofrecuencia (RFID), permite cumplir tareas como almacenamiento, reconocimiento y recuperación de información, mediante la utilización de tarjetas electrónicas (tags)[1].

1.3.1 Ventajas

Para la obtención de la información no se necesita contacto físico con las denominadas tarjetas electrónicas (TAGS) permitiendo de este modo mediante la utilización de esta tecnología el control y captura de datos en entornos inadecuados para operarios. Esta tecnología posee una alta velocidad de lectura de datos a una alta precisión además que los datos asignados a una tarjeta electrónica (tag) pueden ser modificados repetidamente.

1.3.2. Funcionamiento de la tecnología RFID

Los elementos principales utilizados en este tipo de tecnología son: lectora, tarjeta electrónica, antena, host de almacenamiento de información

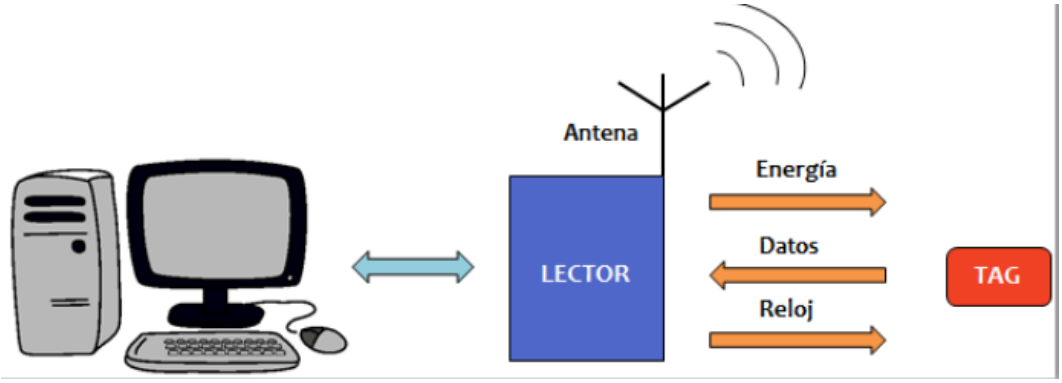


Figura No. 6: Componentes principales de un sistema de lectura RFID

Fuente: (Casero, 2012, pág. 20)

A continuación se realiza un detalle de cada uno de los componentes:

[1] http://www.telectronica.com/index.php/libro-rfid-telectronica/

Tag o etiqueta RFID

Una etiqueta RFID es el componente principal de todo el sistema RFID, tiene las principales funciones de recibir y transmitir señales, para este propósito cuenta con un chip montado sobre un sustrato flexible con una antena incorporada.

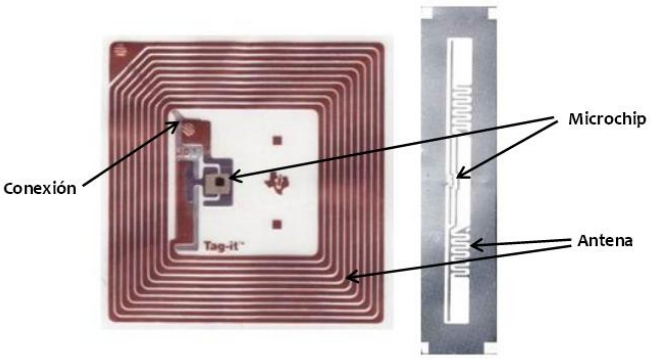


Figura No. 7: Etiqueta RFID

Fuente: (Casero, 2012, pág. 21)

Dispositivo lector

Mediante el uso de una antena es capaz de transmitir y recibir información vía radio proveniente de una etiqueta tag. Para una correcta adquisición de las señales provenientes de la etiqueta tag, un dispositivo lector necesitara más de una antena RF según el lugar de aplicación.

Figura No. 8: Lectoras RFID

Fuente: Manual digital Soyal

Tabla No. 1: Frecuencias de funcionamiento tecnología RFID

Banda de Frecuencias	Características del sistema
LF(de 100 a 500 KHz)	Corto alcance Poca velocidad de transmisión Relativamente económica Trabaja bien en la presencia de metales
HF. Típico 13.56Mhz	Corto/medio alcance Velocidad de transmisión media Puede leer a través de líquidos Problema junto a metales Moderadamente caro
UHF (400-01000 MHz)	Largo alcance Alta velocidad de transmisión Mecanismos de anticolisión Problemático con líquidos y metales En metal genera interferencias

1.4 Tecnología ZIGBEE

Es una nueva tecnología de comunicación inalámbrica de corto alcance y de un costo más bajo en comparación a otros tipos de tecnologías inalámbricas como lo es WiFi y Bluetooth.[2]. Este tipo de tecnología es utilizada en aplicaciones en las cuales se requiera de una comunicación a corto alcance tales como lo son domótica, automatización industrial, juguetes interactivos, etc

1.4.1 Características importantes

Tiene bajo consumo de energía además que son dispositivos con bajo costo de instalación y mantenimiento, pueden alcanzar una tasa de 20 a 250Kbps teniendo una cobertura de 10 a 75 metros su banda de operación es de 2.4GHz

[2] http://rua.ua.es/dspace/bitstream/10045/1109/1/InformeTecZB.pdf

CAPÍTULO II

2. ESPECIFICACIONES Y DETALLES DE LA LABORACIÓN DEL PRODUCTO FINAL

La Caja fuerte en su diseño mecánico cuenta con un blindaje proporcionado por el grosor y resistencia de las planchas de acero inoxidable seleccionadas de 3mm de espesor que permite soportar el impacto de proyectiles accionados por armas de 9 mm o de un menor calibre.

En su diseño electrónico cuenta con un lector biométrico que es el corazón de toda la aplicación, el lector posee un microprocesador en el cual almacena los usuarios que se van registrando asociándolos una huella dactilar, una clave numérica y lo más importante un tag que por su pequeña dimensión se coloca dentro del arma de fuego generando diferentes tipos de filtros de seguridad.

La lectora biométrica Soyal tiene la característica de registrar a una persona mediante estas tres opciones además que de fábrica tiene la opción de conectar una cerradura eléctrica o electromagnética a un relé que emite un pulso emitido por la lectora que a su vez asocia las huellas, pin y tag a una o varias personas habilitando la apertura de la cerradura eléctrica.

La presente configuración mediante una tarjeta expansora de 16 relees que se conecta a la lectora biométrica, que permite a su vez conectar hasta 3 tarjetas a modo de cascada para conectar 48 cerraduras, es decir que si el sistema necesita ser ampliado a un sinnúmero de usuarios es necesario conectar por cada 48 compartimentos una lectora biométrica.

Estas configuraciones comerciales son muy comunes en la instalación de ascensores, el usuario mediante una tag acerca a un lector esclavo instalado en el ascensor y este sube o baja al piso que se ha registrado previamente en el sistema. En este caso yo utilizo estas tarjetas expansoras para obtener un sinnúmero de pulsos diferentes para cada usuario con la finalidad de que única he individualmente aperture la cerradura de su compartimento pre designado mediante su huella digital y su tag colocado en el arma de fuego, garantizando un control exclusivo de que cada usuario abra su compartimento exclusivamente designado para el con su arma de fuego que se convierte en su llave electrónica del sistema.

Además la aplicación posee una cámara de audio y video que utiliza wifi y transmite en tiempo real por un Ip asignado que mediante un cloud privado puede ser monitoreado mediante una pc o celular desde cualquier lugar que tenga acceso a internet. Uno de los aportes más importantes del presente desarrollo es un circuito integrador de los diferentes componentes comerciales utilizados. Es aquí donde todas las cerraduras conectadas a la tarjeta expansora mediante una conexión en paralelo a un dispositivo de relees de 12 v que utiliza tecnología Zigbee que es muy utilizado para sistema de domótica permite realizar aperturas emergentes desde un computador, celular, Tablet ingresando al aplicativo de control (SCADA). Otro dispositivo Zigbee conectado en serie a uno de los polos que alimenta la corriente eléctrica a la lectora enciende o apaga la aplicación inhabilitando la lectora, impidiendo a los usuarios a sacar sus armas de fuego en caso de emergencia. Este sistema también tiene redundancia de generación eléctrica en caso de apagones de electricidad, el sistema seguirá funcionando normalmente a falta de fluido eléctrico mientras dure la carga de las baterías que permanentemente están siendo recargadas.

Una vez que vuelva el fluido eléctrico el sistema vuelve a cargar las baterías en caso de que se genere otro incidente. La lectora biométrica y los dispositivos Zigbee tienen sus propios aplicativo comerciales de monitore como cualquier software de control tipo SCADA el cual se puede programar y representar la apertura, encendido y apagado de todos los sistemas así como generar reportes según sea las necesidades del usuario generalmente al abrir o cerrar los compartimentos , bloquear usuarios o restringir las fechas de apertura esto para que en los días libres los uniformados no puedan disponer de las armas de fuego. Para todo esto se tiene una pc conectada a la lectora y los dispositivos zigbee para manipular el sistema como sea necesario y controlarlo remotamente mediante internet con esto se podrá llevar un control riguroso de las veces qué ha sido abierta la caja de seguridad y que usuario realizó esta operación.

La Caja fuerte se desarrollará con tecnología de última generación puesta a disposición de instituciones armadas que busquen mejorar la seguridad y resguardo de sus armas; ya que se cuenta con un sistema que reduce en gran medida la apertura de los compartimentos de la caja fuerte con la facilidades para llevar estadísticas y registros de los ingresos y egresos del armamento.

El desarrollo del presente sistema incluye las siguientes actividades:

- La fabricación de la parte mecánica de la caja de seguridad.
- El transporte.
- La instalación de los dispositivos electrónicos.
- La configuración.
- El Soporte Técnico.
- Mantenimiento Preventivo.
- Mantenimiento Correctivo.
- Garantía de equipos por daños de fábrica.

2.1Descripción de la Ingeniería del Proyecto

2.1.1 Dimensiones de la Caja fuerte

- Altura 1.05 metros.
- Ancho 64 cm.
- Profundidad 51 cm.

2.1.2 Características de las divisiones internas.

Cada compartimento tiene las siguientes dimensiones:

- Alto mide 16 cm
- Ancho es de 28 cm
- Profundidad es de 50 cm

Figura No. 9: Caja de seguridad biométrica

2.2 Sistema de bloqueo

El mecanismo para bloquear el sistema es mediante los dispositivos Zigbee. El bloqueo es electrónico vía internet normal o satelital para los lugares donde no exista cobertura de red esto depende del costo beneficio y las necesidades de los usuarios. En caso de emergencia desde el centro de monitoreo o una persona que tenga acceso a las claves del sistema

mediante un celular puede inhabilitar o habilitar el sistema las veces que genere necesario. El bloqueo puede ser selectivo para el conjunto de cajas que considere necesario.

2.3 Características de la caja fuerte

Materiales

La caja fuerte de seguridad está compuesta por los siguientes materiales:

Planchas de acero inoxidable

- Qnn/hg-5840/espesor: 3mm resistente a golpes, incendios, impacto de bala de 9mm; las mismas que serán soldadas con suelda de tipo plasma. Con estas planchas se arma toda la cubierta de la caja de seguridad biométrica.

Tubos cuadrados de 2pulgadas de acero inoxidable.

- Permite generar el esqueleto donde se sobreponen las planchas de acero además que le da más resistencia a la caja de seguridad.

Tag de radiofrecuencia:

- El tag seleccionado fue mandado a fabricar directamente a la China exclusivamente para este aplicativo. Trabaja a una frecuencia de 125 KHZ y tiene un recubrimiento plástico especial que le permite adaptarse a las condiciones de trabajo de los diferentes climas en especial al trópico selvático existente el Ecuador,s resistente a la humedad incluso golpes por lo habitual del trabajo cotidiano. La tecnología RFID o identificación por radiofrecuencia) es un sistema de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas, tarjetas, transponedores o tags RFID, transmite la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

Módulo Zigbee de 6 entradas y 6 salidas a relé de montaje riel DIN 12v.

- Monitorea seis entradas independientes, preparado para contactos secos o colectores abiertos y controla hasta seis cargas individuales (3A por canal) con relé incorporados, las entradas pueden ser configuradas para controlar directamente las salidas, dispara escenas, además su tiempo de desconexión es automático, configurable para todas las entradas, estos dispositivos utilizan

tecnología inalámbrica ZigBee y cada salida se puede configurar de forma independiente para participar en un máximo de 16 escenas diferentes.

Repetidor Built-in

- Dispositivo electrónico que recibe una señal débil o de bajo nivel y la retransmite a una potencia o nivel más alto, de tal modo que se puedan cubrir distancias más largas sin degradación o con una degradación tolerable. (Interviene en la comunicación de los dispositivos cercanos contribuyendo a elevar la señal de la red inalámbrica de los demás dispositivos), repiten todas las señales de un segmento a otro a nivel eléctrico.

Cerraduras eléctricas.

- La SD873 es una cerradura altamente resistente y compacta, diseñada para el mercado de las cajas fuertes tipo looker, como una alternativa de avanzada a las combinaciones u otras cerraduras electromecánicas.
- La energía de la cerradura la provee un Paquete de Poder PP901, operado por una batería de Litio 123A (incluida). El Indicador de Estado LP873 es opcional. Es usado para aplicaciones de monitoreo y el sistema de conexión es normalmente cerrado lo que permite que si hay un corte de corriente eléctrica permanezca los compartimientos cerrados aun cuando las baterías de redundancia se encuentren totalmente agotadas.

Lector biométrico Soyal AR-821ES-OS

- Consta de un lector de huellas DIGITAL/PROXIMIDAD/PIN OPT: AR-821ES-OS y este a su vez se conectó a un MAIN BOARD DUAL CORE 3GB que está conectado al DISCO DURO 500GB donde se guarda toda la información y registro de los ingresos y egresos de las armas, para que el procesador funcione a la perfección y realice los reportes y demás trabajos correctamente se utilizó MEMORIA RAM DDR3 2GB.

Fuente de poder

- Está formado por fuente para cámara 12V 1.5AMP ST-P150 las cuales dan el funcionamiento a las puertas de los gabinetes donde están guardadas las especies valoradas y con su fuente de alimentación 12V 3.5AMP CON/BAT ST-PB350 para su funcionamiento. Una tarjeta de red wireless 150 MB, que será la que permita transmitir la información a un computador donde se receptara la información del sistema de Caja fuerte, para ver los reportes que necesitemos.

2.4 Cámara de video D-Link

Las cámaras de video D-Link son sistemas de vigilancias compuestas por una amplia gama de cámaras IP para su uso en diversos entornos empresariales, desde tiendas y oficinas hasta almacenes e instalaciones más exigentes con la seguridad, para uso tanto en interiores como exteriores.

Las cámaras IP de D-Link abarcan un amplio portfolio con las prestaciones más avanzadas: alta definición Full HD, sensores progressive scan CCD y CMOS megapíxel de Sony, monitorización remota avanzada, certificaciones IP contra vandalismo y cambio de clima, infrarrojos para visión nocturna, amplio rango dinámico, visión panorámica y de ojo de pez, movimiento motorizado de la lente en giro, inclinación y zoom (PTZ), alimentación PoE, conexión Wireless, sonido bidireccional y amplia conectividad a sensores y alarmas.

Estos sistemas de vigilancia son los más evolucionados en cuanto a tecnología, pues su servicio que consiste en Videovigilancia IP unificada: cámaras IP, switches de red, grabadoras de vídeo en red (NVR), dispositivos de almacenamiento NAS/SAS y software de gestión de vídeo (VMS), permite que empresas y organismos oficiales pueden desplegar sistemas de Videovigilancia IP con un máximo de efectividad.

CAPÍTULO III:

3. ESPECIFICACIONES Y DETALLES DE EJECUCIÓN

El proceso de ejecución de este proyecto siguió la siguiente secuencia:

1. Formulación de la idea

   La idea nace al surgir la necesidad.
2. Investigación de la posibilidad de realizarla

   Se realiza una investigación para conocer la factibilidad de realizar del proyecto, para conocer si existen similares, materiales requeridos, presupuesto necesario, etc.
3. Búsqueda de equipos

   En el mercado se buscan los equipos y materiales necesarios para la elaboración del proyecto, se solicitan proformas con especificaciones y se elige la mejores.
4. Adquisición de equipos

   Después de analizar las cotizaciones y escoger la mejor, se adquieren los equipos elegidos.
5. Conexión de dispositivos

   Con los materiales y equipos en stock, se procede a la conexión de dispositivos que conforman la solución.
6. Desarrollo circuitos electrónicos de integración

   Se desarrollan los circuitos de integración.
7. Desarrollo de la estructura metálica de integración

   Se desarrolla la estructura metálica de acuerdo a las especificaciones, se cortan las láminas de acuerdo medidas especificadas, se hacen los orificios para el cableado, se suelda.
8. Pruebas de equipos.

   Se realizan las pruebas para comprobar el funcionamiento requerido. En caso de no hacerlo, se sustituyen componentes, se mejora el circuito.

3.1 Estructura operativa.

En la fase de diseño se realizó el bosquejo de cómo se quería que funcione la Caja fuerte, las partes que son necesarias para su realización y que los componentes a utilizarse en el presente desarrollo puedan integrarse mediante un solo circuito electrónico para que su funcionamiento sea el esperado y el proyecto pueda culminar con éxito.

En la fase de adquisición de los materiales se buscó proveedores que mantengan los estándares necesarios para el presente desarrollo y se escogió la mejor calidad.

En la etapa de designación del espacio, el dispositivo fue ensamblado y soldado en una metalmecánica de la ciudad de Quito en la Av. 6 de diciembre y Colón, y el montaje de los dispositivos electrónicos en una oficina ubicada en la avenida República del Salvador donde se pudo tener las facilidades que el proyecto necesitaba para su desarrollo.

En la fase montaje o armado de la Caja fuerte, se colocaron las piezas tal y como se estructuró en los bosquejos, reportándose algunos percances de quema de equipos zigbee ya que son sensibles a la diferencia de voltaje común en la generación eléctrica de 110 voltios por cual se utilizó de manera posterior un regulador de voltaje. La cámara de video también sufrió los mismos percances, sin embargo estas situaciones fueron solventadas.

En la fase de acoplamiento de los componentes lógicos y de monitoreo no hubo ningún inconveniente.

En la fase de pruebas, se procedió a realizar todos los procedimientos tanto de tipo físico como lógico, para verificar que todo el sistema funcione bien.

3.2 Diseño de la solución

En este capítulo se presenta la propuesta de hardware y software para la implementación y montaje de la Caja de Seguridad Electrónica Biométrica para el resguardo en forma segura de las armas de fuego de los diferentes repartos, unidades y cuarteles militares y policiales así como empresas de seguridad armada. Se han seleccionado los mejores fabricantes para cada componente del sistema con el propósito de implementar una solución técnica y económica idónea que cumpla con las normas y los estándares más elevados del mercado

nacional e internacional, que permitan integrar una caja fuerte con los sistemas electrónicos más actuales.

El proceso de protección de las armas de fuego en la caja fuerte tiene diferentes subprocesos que garantizarán que estas salgan de la caja de origen y sus compartimentos y regresen a su lugar de almacenamiento, indicando los eventos que puedan ocurrir durante todo el proceso y permitiendo resolver posibles controversias.

No existe en la actualidad un proceso para el almacenamiento de armas que utilice los componentes utilizados en el presente desarrollo y que funcione de la presente manera.

El presente sistema de seguridad debe poseer las siguientes características:

- Centralizar la información de control de las armas de fuego.
- Capacidad de acceder a la caja fuerte mediante tag, pin y huella digital.
- Permitir una auditoría y gestión personalizada los usuarios que guardan sus armas.

3.2.1 Definición del proceso de funcionamiento.

El sistema de resguardo de armas de fuego cumple con un protocolo que permite centralizar los datos, llevar a cabo un inventario, generar alarmas y controlar las armas desde la salida de la caja fuerte hasta su llegada o almacenamiento.

A continuación se indica las etapas y las condiciones que se debe cumplir para obtener un funcionamiento total del sistema.

3.2.2 Programación de los usuarios.

En esta primera etapa se programan los medios de acceso a las diferentes celdas de la caja fuerte con los datos de identificación de los usuarios autorizados para la manipulación de las armas de fuego a través del software de gestión en donde se encuentran las opciones más adecuadas para el ingreso de usuarios mediante tag de proximidad, pin y huella dactilar. Una vez generado el usuario se puede asignar diferentes modos de acceso aumentando la seguridad, los cuales se indican a continuación:

Tabla No. 2: Modo de Acceso

MODO DE ACCESO	TIPOS Y MODO DE ACCESO
1.- FP/TAG	Solo huella / Solo tarjeta / Huella + Tarjeta
2.- TAG OR PIN	Solo huella / Solo tarjeta / Solo Pin / Huella + Tarjeta / Pin + Huella
3.- & PIN	Pin + Tarjeta / Pin + Huella + Tarjeta
4.- PAUSE	Sin Acceso

3.2.3 Lectura de salida de las armas de fuego.

La lectura de salida de las armas con los respectivos medios de acceso RFID o huella, se realizará mediante una lectora biométrica que permita identificar el usuario y garantizar los siguientes parámetros:

- Identificación de usuario, fecha y hora del evento.
- Generación de alarmas en el caso de que se produzca una intrusión no deseada.
- Verificación de la celda autorizada mediante el módulo de salida de relés.

3.2.4 Lectura de llegada de las armas de fuego.

En esta etapa se tomará información mediante el software de control en el sitio a través del usuario que es el responsable de la devolución del arma de fuego, para garantizar que éstas lleguen a su lugar de destino. Cuando las armas no estén en uso se complementa su monitoreo con una cámara de video vigilancia. Dentro de esta etapa se realizara una identificación de los usuarios, de la hora y fecha de llegada.

3.2.5 Control domótico a través del teléfono celular.

Con el objetivo de aumentar la seguridad y lograr una opción de emergencia en el caso de no tener acceso a través de la lectora biométrica o requerir de un bloqueo total, se implementara un sistema domótico zigbee con aplicación para teléfono celular o sistema web desde donde se podrá tener el control inmediato en todo momento.

3.3 Componentes de la Solución

La propuesta para la caja fuerte electrónica se lo ha establecido en la parte del hardware, en base a la teoría del capítulo 1, como se indica en el diagrama de bloques de la Figura No. 11.:

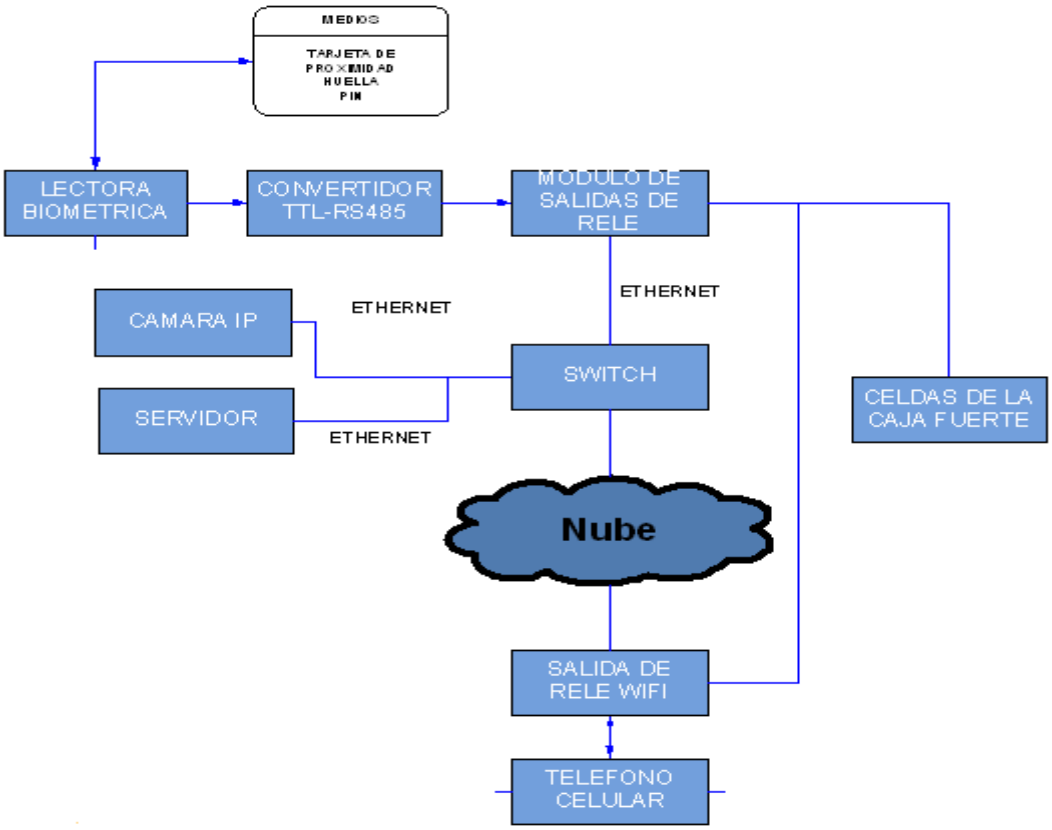


Figura No. 10: Componentes de solución

Elaborado: Germán Luzuriaga

Este diagrama está formado por los componentes necesarios y medios de transmisión que permiten obtener un sistema confiable y garantizado para controlar y monitorear las celdas de la caja fuerte. En base al diagrama de bloques del hardware del sistema se puede dimensionar y seleccionar cada uno de los componentes que se requiere para la implementación real y funcional de la solución. Estos elementos se detallan a continuación:

- Lectora biométrica
- Medios de acceso
- Módulo de salida de relés
- Módulo de salida de relés zigbee
- Router inalámbrico
- Servidor
- Fuentes de voltaje
- Cámara IP
- Regulador de voltaje
- Caja fuerte

Para la selección adecuada de los productos se analizó varios proveedores en el mercado que cumplan con los requerimientos de durabilidad y de la capacidad de transmisión y lectura de medios RFID y biométricos a la vez, así como los estándares ISO especificados para sistemas de RFID y ZIGBEE ya que actualmente en el mercado se encuentran disponibles un sin número de equipos.

Dado que en el mercado existen muchos productos, los criterios que se tomaron en cuenta para la selección de los equipos son los siguientes:

- Operacionales
- Técnicos
- Económicos

Estos parámetros permitirán implementar un sistema óptimo de alto desempeño en su funcionamiento. Los criterios técnicos son los más importantes para el desarrollo del sistema y se detallan a continuación:

- **Frecuencia de operación:** para esta aplicación de acceso, es común y recomendable, el uso de un sistema RFID que opera en frecuencias de 13.56 Hz. Su principal ventaja radica en una distancia de comunicación mayor que las tarjetas Mifare. Está tecnología fue la primera tecnología sin contacto, con una capacidad de flujo de datos reducida, por lo que se reserva a aplicaciones de control de accesos, en las que el intercambio de datos es mínimo: se trata de leer el número de serie del tag para reconocer el usuario preregistrado.

- **Tecnología zigbee:** para el control domótico se usará el estándar de comunicaciones inalámbricas diseñado por la ZigBee Alliance. Es un conjunto estandarizado de soluciones que pueden ser implementadas por cualquier fabricante. ZigBee está basado en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (wireless personal área Newark, WPAN) y tiene como objetivo las aplicaciones que requieren comunicaciones seguras con baja tasa de envío de datos y maximización de la vida útil de sus baterías. ZigBee es un sistema ideal para redes domóticas, específicamente diseñado para reemplazar actuadores individuales.

- **Tipo de cámara**: se deben considerar aspectos técnicos y de resolución para la selección de la cámara, de igual forma sus características de conexión POE

Selección de los medios de acceso.

Los medios seleccionadas son TAG +PIN+ HUELLA DIGITAL en diferentes combinaciones para aperturar o cerrar los compartimentos de la caja fuerte.

3.3.1 Diseño electrónico.

El diseño electrónico que se utiliza para la caja fuerte se base en el esquema de la figura 11. Componentes de la solución donde se describe en forma general el funcionamiento de los componentes sistema electrónico.

La conexión de los diferentes dispositivos o componentes de la marca Soyal se detalla continuación, donde se observa la interconexión y su lógica de funcionamiento.

El control de acceso biométrico AR-821-EF presenta en la figura No. 12 en la que se observa las terminales de conexión:

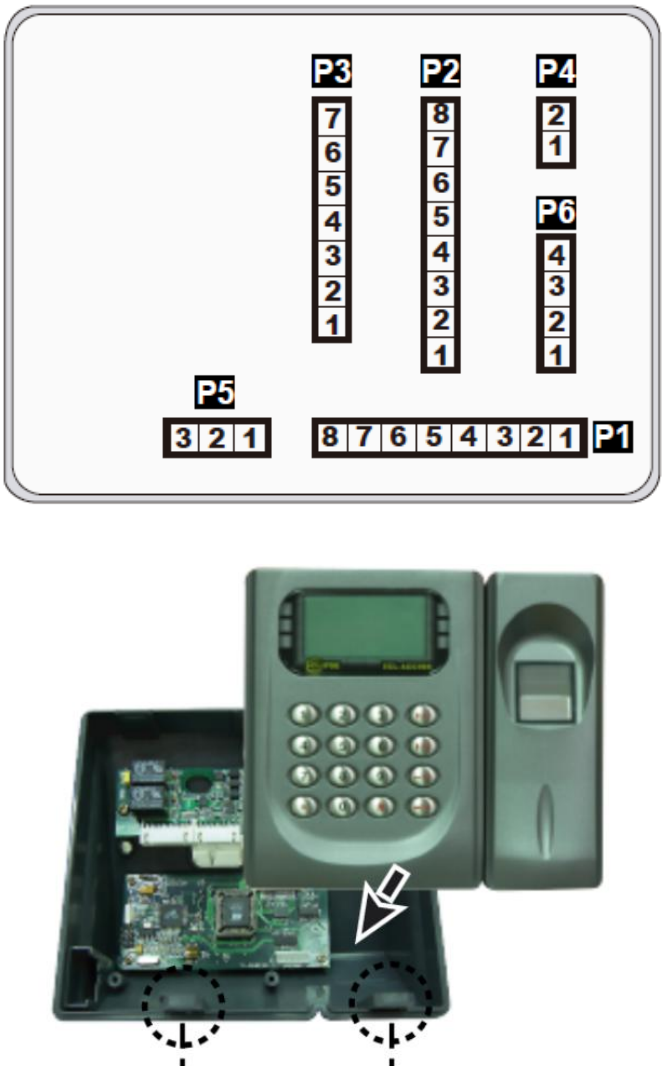


Figura 12. Distribución de terminales del controlador

Cada uno de los terminales, con distintos tipos de colores de conductores, que representan las diferentes prestaciones del controlador, se detalla a continuación:

Descripción de los conductores del terminal P1

Esta bornera se emplea para la conexión de alimentación del lector y la interfaz física con la cerradura eléctrica, los pulsadores de salida, alarmas y de las salidas programables.

Tabla No. 3 Disposición conductores del terminal P1 del terminal de control AR-B21-EF

Tabla No: 3 Conexiones de lector biométrico Soyal

Aplicación del Cable	Cable	Color	Descripción
Relé de Bloqueo	1	Azul Blanco	(N.O) DC24V 1Amp
	2	Morado Blanco	(N.C) DC24V 1Amp
Relé de Bloqueo COM	3	Blanco	(COM) DC24V 1Amp
Contacto de Puerta	4	Naranja	Entrada Activadora Negativa
Switch de Salida	5	Morado	Entrada Activadora Negativa
Relé de Alarma	6	Gris	Transistor de salida Max. 12V/100mA (Colector Abierto Activo Bajo)
Alimentación	7	Rojo Cable Grueso	DC 12V
	8	Negro Cable Grueso	DC 0V

En este proyecto se utiliza únicamente los conductor 7 y 8 para alimentación de la controladora, mediante una fuente de 12Vdc de 2 Amp.

Descripción de los conductores del terminal P2

Esta bornera se emplea para la conexión con una lectora Wiegand que contempla la visualización, sonido y salidas.

Tabla No. 4 Balta: disposición conductores terminal 4P2 del terminal de control AR-821-EF

Aplicación del Cable	Cable	Color	Descripción
Localizador	1	Rosado	Localizador de Salida 5V/100mA, Bajo
LED	2	Amarillo	LED Rojo de Salida 5V/20mA, Max.
	3	Marrón	LED Verde de Salida 5V/20mA, Max
Puerta de Salida	4	Azul Blanco	Transistor de Salida Max. 12V/100mA (Colector Abierto Activo Bajo)
Wiegand	5	Verde Cable Delgado	Wiegand DAT:0 Entrada
	6	Azul Cable Delgado	Wiegand DAT:1 Entrada
WG Contacto de Puerta	7	Naranja	Entrada Activadora Negativa
WG Switch De Salida	8	Morado	Entrada Activadora Negativa

Descripción de los conductores del terminal P3

Esta bornera se emplea para la comunicación TCP/IP utilizando un punto de red de 4 pares, a continuación se detalla que pines de terminal se asigna para la conexión:

Tabla No. 5. Disposición conductores del terminal P3 del terminal de control AR-821-EF.

Aplicación del Cable	Cable	Color	Descripción
	1	---	---
	2	---	---
Salida TCP/IP	3	Naranja Blanco	Net - TX +
	4	Naranja	Net - TX -
	5	Verde Blanco	Net - RX +
	6	Verde	Net - RX -
	7	---	---

En este proyecto se utiliza este terminal para conectarse a la red y poder gestionar y controlar el proceso con el software Server 701 y Client 701. Cada cable o patch cord de la red consta de dos puertos de red RJ-45 con 8 hilos, en la siguiente figura se muestra la distribución de los pines del puerto de red:

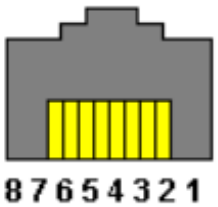


Figura No. 12: Líneas del puerto de red

Según la norma EIA/TIA 568 donde se reconoce dos asignaciones de puntos de conexión por pares, la T568A y la T568B, y de acuerdo a la aplicación la forma de conexión más usada es la asignación T568B, por lo tanto se van a utilizar los pines 3,4,5,6 de acuerdo a lo establecido por el fabricante.

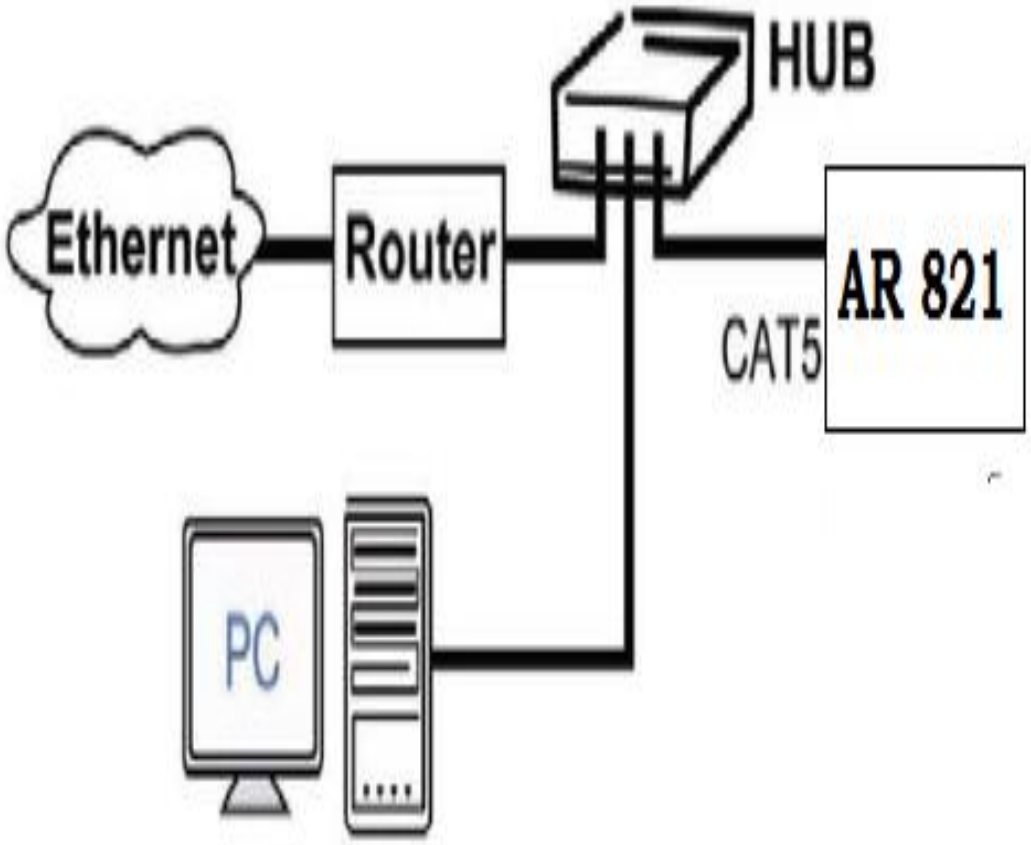


Figura No. 13: Configuración de red

De acuerdo al esquema de conexión todos los dispositivos se conectan a un hub mediante cable cat 5E y sus respectivos RJ 45 para formar una red que permita manejar los dispositivos soyal mediante la PC.

Descripción de los conductores del terminal P4

Este terminal se emplea para la conexión de la comunicación con el panel de control, bajo interfaz RS-485.

Tabla No. 6. Disposición conductores terminal P4 controlador AR-821-EF

Aplicación del Cable	Cable	Color	Descripción
RS-485 Para Controlador	1	Verde Cable Grueso	RS-485(B-)
De Ascensor	2	Azul Cable Grueso	RS-485(A+)

.

Descripción de los conductores del terminal P5 del controlador AR-821-EF

Este terminal se emplea para la usar en modo de anti sabotaje.

Tabla No. 7. Disposición conductores terminal P5.

Aplicación del Cable	Cable	Color	Descripción
Interruptor Anti-Sabotaje	1	Rojo	N.C.
	2	Naranja	COM
	3	Amarillo	N.O.

Descripción de los conductores del terminal P6

Este terminal se emplea para la conexión de salidas y seguridad

Cuadro No. 8 Disposición conductores terminal P6 del controlador AR-821-EF.

Aplicación del Cable	Cable	Color	Descripción
Alimentación	1	Rojo	Salida DC 12V
Señal de Seguridad	2	Morado	Activador de Señal de Seguridad De Salida
Armamento	3	Rojo Blanco	Armamento de Salida
Coacción	4	Amarillo Blanco	Coacción de Salida

El módulo de control de ascensores o de salidas AR-401R presenta la distribución de borneras como indica la Figura No. 17:

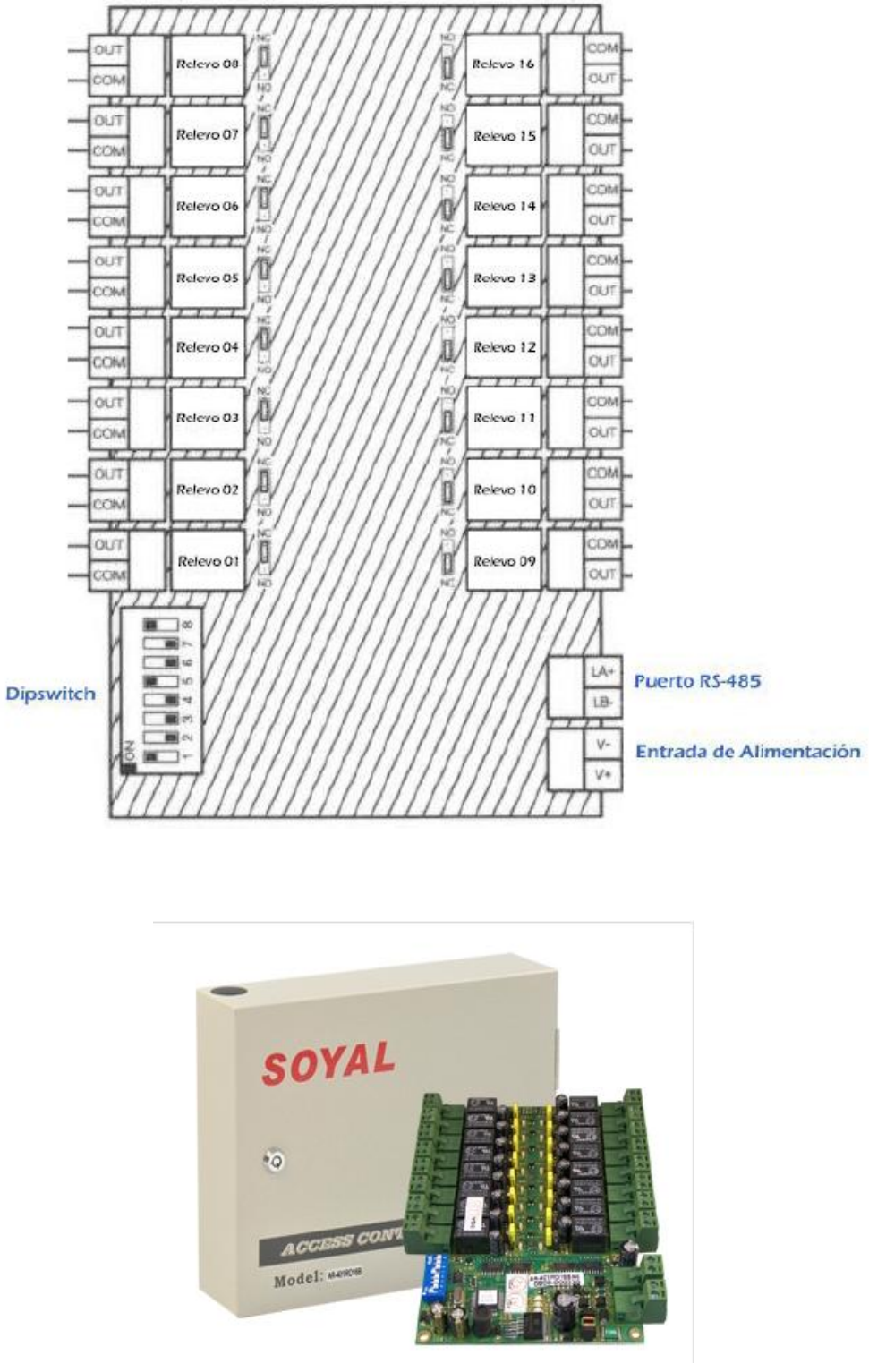


Figura No. 11: Conexiones del módulo de salidas

Configuración del nodo ID.

Esta configuración se realiza mediante un DIP SWITCH de 8 pines, para este proyecto se colocan los 5 primeros pines en modo on lógico para determinar la dirección del nodo, el rango de nodos es de 1 a 32 dispositivos a una velocidad de 19200, el pin 6 se coloca en alto y el 7 y 8 en bajo para poder comunicarse con la lectora AR821 pero también permite seguir implementado tarjetas en cascada para aumentar el número de pulsos pesarios para instalar más cerraduras como se puede apreciar en el siguiente gráfico.

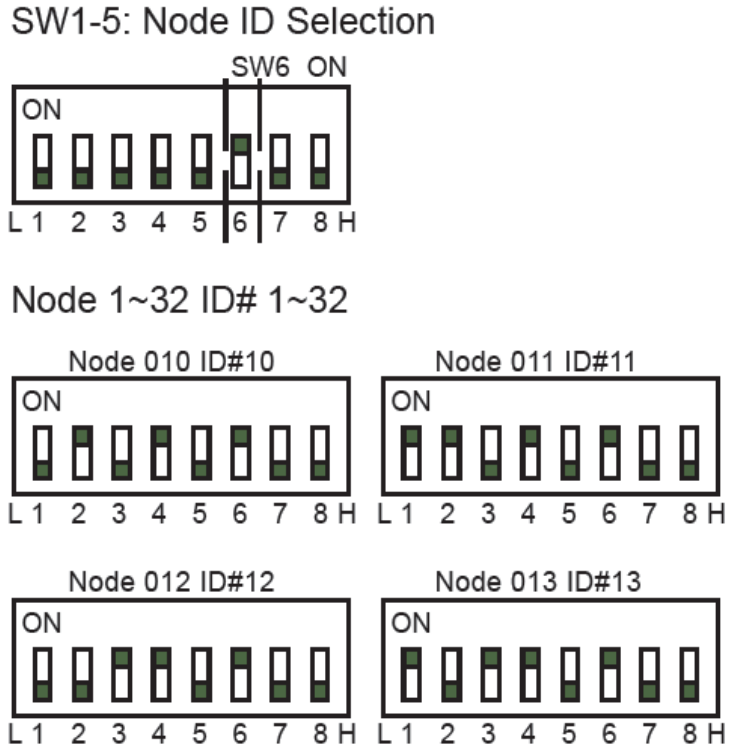


Figura. 18 Configuración del nodo ID.

Conexión de la lectora y módulo de salidas de relé mediante el convertidor.

Para que el lector biométrico pueda controlar el módulo de salidas de relé se debe utilizar el terminal RS 485, el esquema de conexión se detalla en la figura No.19:

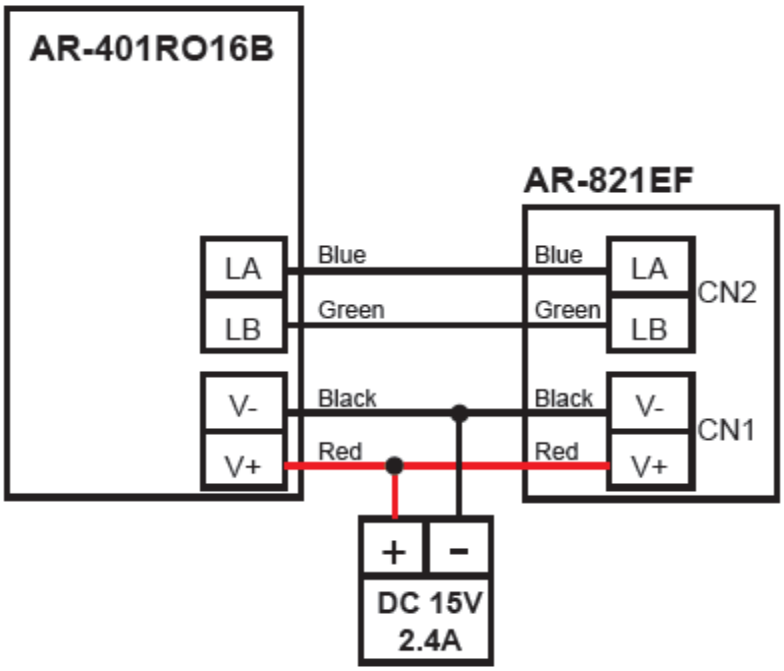


Figura No. 19. Conexión Lectora-Modulo de salida.

Como se puede observar en la figura la conexión de comunicación entre la lectora biométrica y el módulo de salidas se realiza directamente por medio de dos hilos (LA y LB) del terminal P4.

El método de funcionamiento para contralar las salidas de relé (cerraduras eléctricas) mediante la lectora biométrica se detalla a continuación:

1.- Se asigna las huellas y las claves necesarias de acuerdo al número de celdas de caja fuerte y personal autorizado, creando una base de datos del personal autorizado por el supervisor del sistema.

2.- Para ingresar del arma o la especie valorada a la caja fuerte, se debe colocar el dedo pulgar y al mismo tiempo el arma que contienen un tag único introducido en la especie valorada, este es el método para que el sistema permita la apertura de la celda autorizada y programada con anterioridad, después de verificar en la base datos.

3.- Para extraer un arma o especie valorada se coloca el dedo índice y una clave de seguridad.

En el caso de que una persona no autorizada o no identificada en el sistema trate de abrir las celdas, la lectora emite una alarma sonora y al tercer intento proceda a bloquear la caja fuerte.

Las fuentes utilizadas son de 2 Amp - 12 Vdc y 5 Amp - 12 Vdc, una para la lectura y modulo y la otra para las cerraduras eléctricas. Las cerraduras eléctricas tienen un consumo de 400mA a 12 VDC cuando se encuentran operando en modo individual, por lo que se usa una fuente de 5 amperios con el negativo en modo común. En el caso de lectores de proximidad, cada uno consume 80 mA en Stand By, y 150 mA en Lectura, por lo que se conectarán la lectora y el módulo de salidas a una sola fuente

Descripción Modulo Zig bee

Finalmente el diseño electrónico contempla un control domótica wifi, para esto existe un control de salidas relé wifi que se controla mediante la interface desde el celular o desde una PC, este módulo se conecta en paralelo al módulo de salida Soyal para poder controlar y gestionar de un forma remota las diferentes celdas de la caja fuerte. A continuación se presenta en la figura No. 20 el módulo de salida wifi:

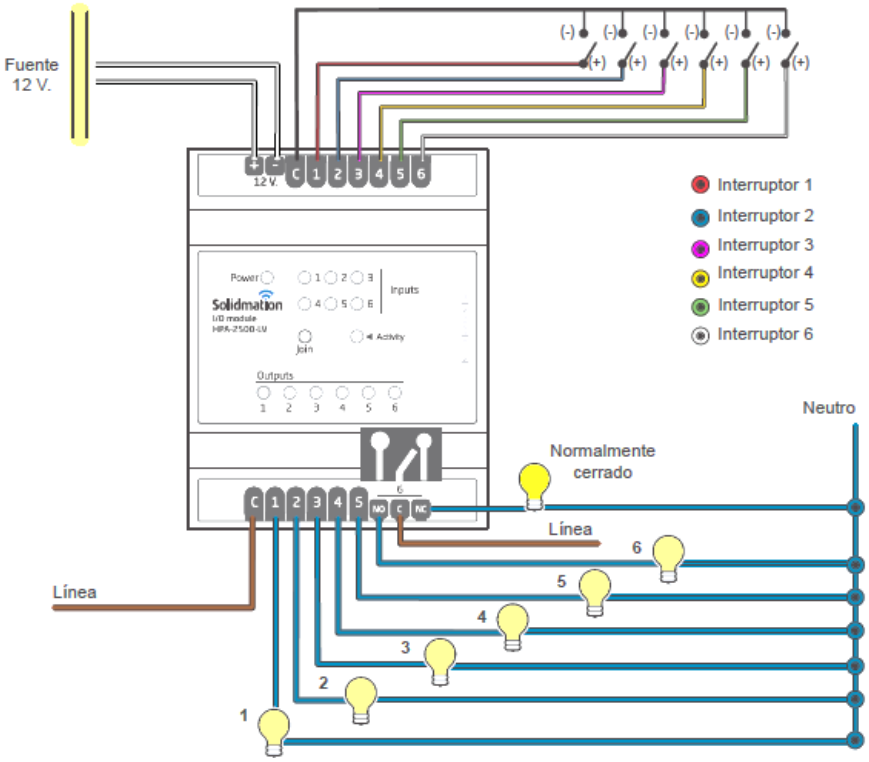


Figura. 20 Modulo Salida wifi.

Todos los datos se almacenan en una PC (servidor) que a su vez se comunica mediante protocolo Ethernet a un Access point en donde se interconectan los elementos de video vigilancia y acceso. De esta forma se tiene una configuración tipo estrella donde todos los dispositivos que forman parte de la caja fuerte están conectados y pueden comunicarse entres si, mediante sus programa.

La cámara de la marca D-link IP permite una grabación en forma continua tanto audio y video. Cuando se presenta una emergencia o denuncia procede a verificar la cámara IP y con el aplicativo zig bee se puede cortar la alimentación de la lectora con lo cual se eliminan el terminal de alimentación y pasa a un control remoto por wifi en el caso que se requiera abrir las celdas. El sistema también posee un respaldo de batería para el sistema en el caso de falla de alimentación.

Se realizó la simulación del sistema electrónico utilizando un diseño de circuito electrónico integrador que se detalla a continuación;

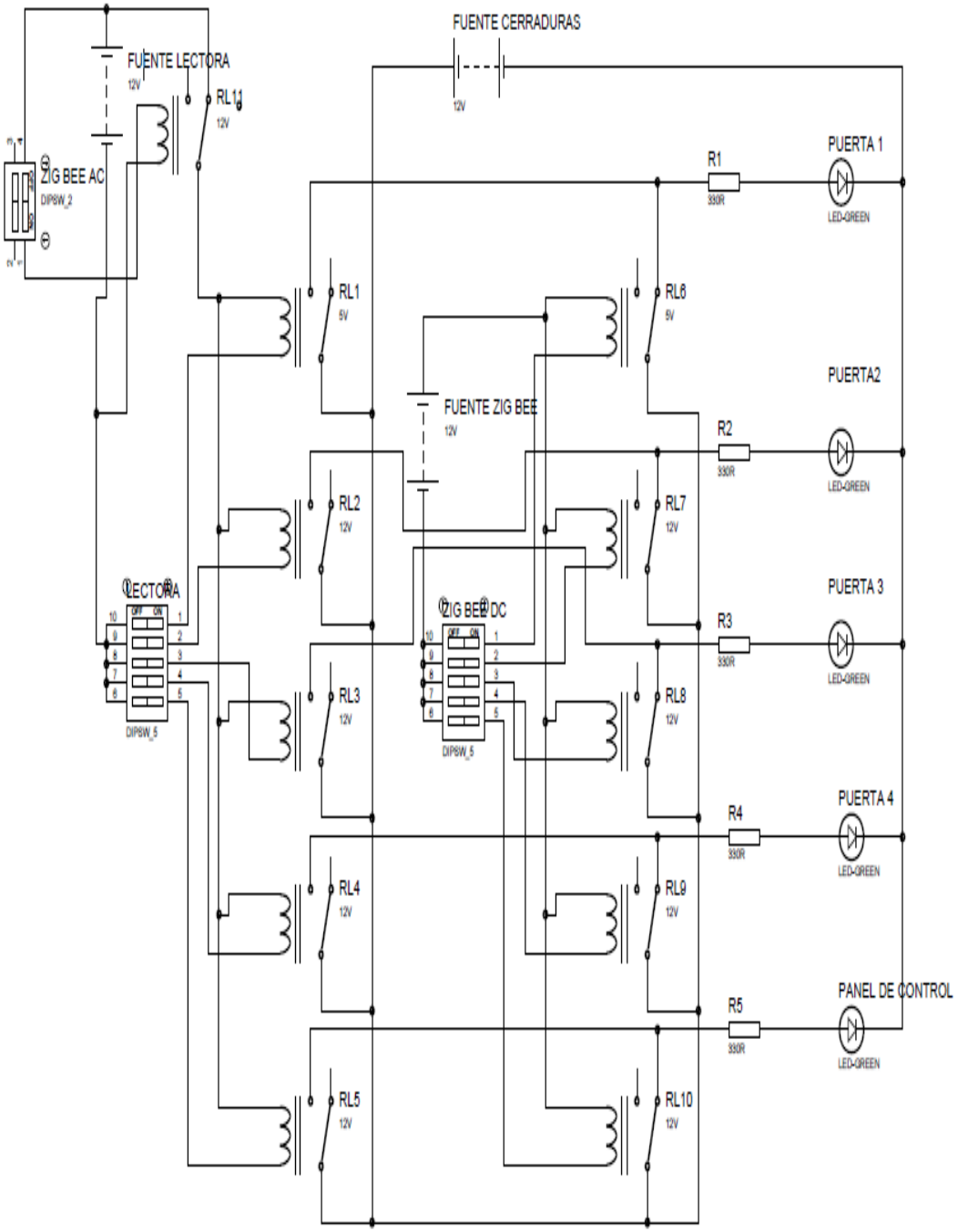
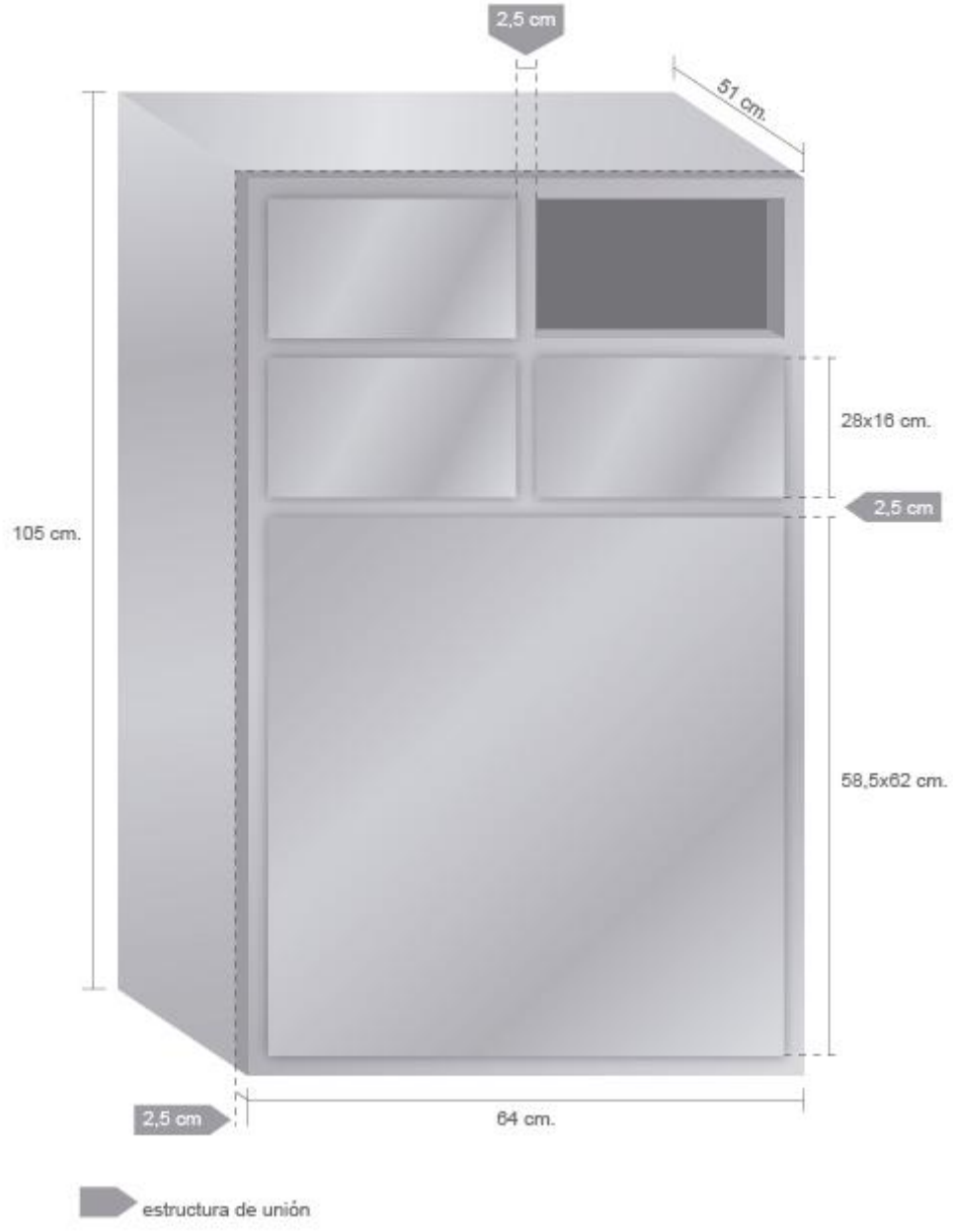


Figura No. 21 Diseño del circuito electrónico de integración.

Diseño mecánico de la caja fuerte

Para la caja fuerte se ha utilizado acero inoxidable de 3mm con nivel de resistencia de hasta proyectiles de 9mm. La construcción se ha realizado siguiendo las normas de seguridad necesaria y protocolos que corresponden al manejo de armas de fuego.



3.4.1 Configuración del sistema de control 701server

En la aplicación 701Server, se configura la manera en que están conectados los equipos, con sus identificadores (ID) y la forma de comunicación con el Servidor.

Primero se configura la comunicación entre equipos y servidor utilizando el botón "Com", como se muestra en la figura No. 24:

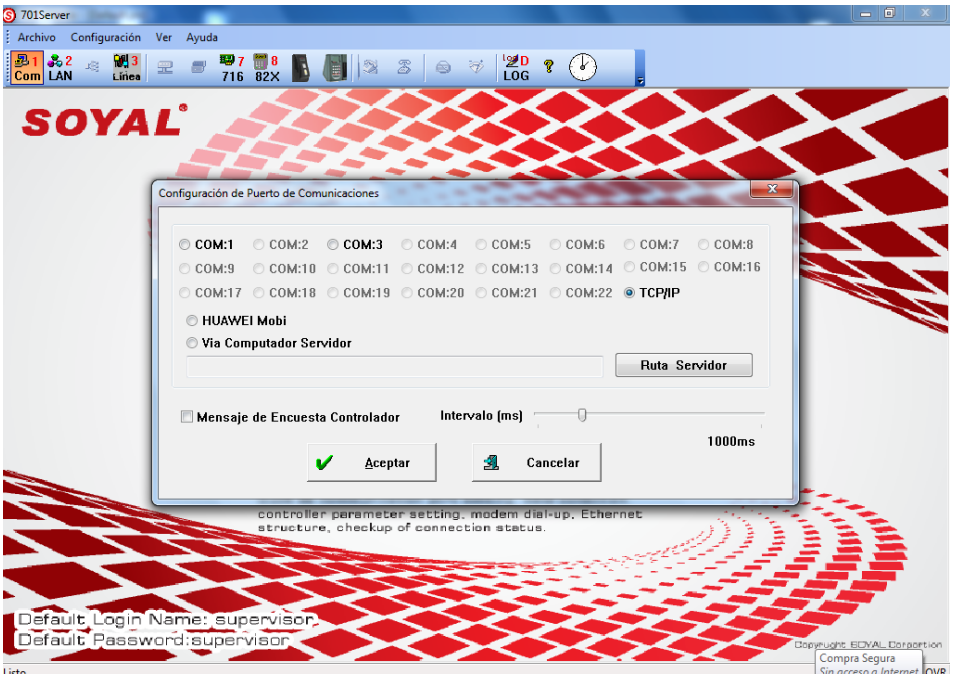


Figura No. 12: Configuración aplicación 701 server

En esta opción se selecciona el puerto de comunicación al que esta conectado directamente el sistema, mediante el conversor de RS485 a RS232, o TCP/IP (No Comm Port) si la comunicación se va a realizar por medio de la red. Si el computador en el que está siendo instalada la aplicación es un cliente que va a acceder a un servidor, se escoge la opción Via Server Computer, y en el botón Server Computer Path se busca en la red la carpeta compartida 701Server en el computador servidor. De igual forma se debe asegurar de seleccionar la opción Polling Message From Controller y seleccionar un intervalo de tiempo entre 200ms y 500ms. Si el sistema es conectado mediante red, debe ser de 1000ms.

Luego se debe configurar los equipos conectados a la estructura del sistema, en el botón "LAN", como se puede ver en la siguiente figura No. 25:

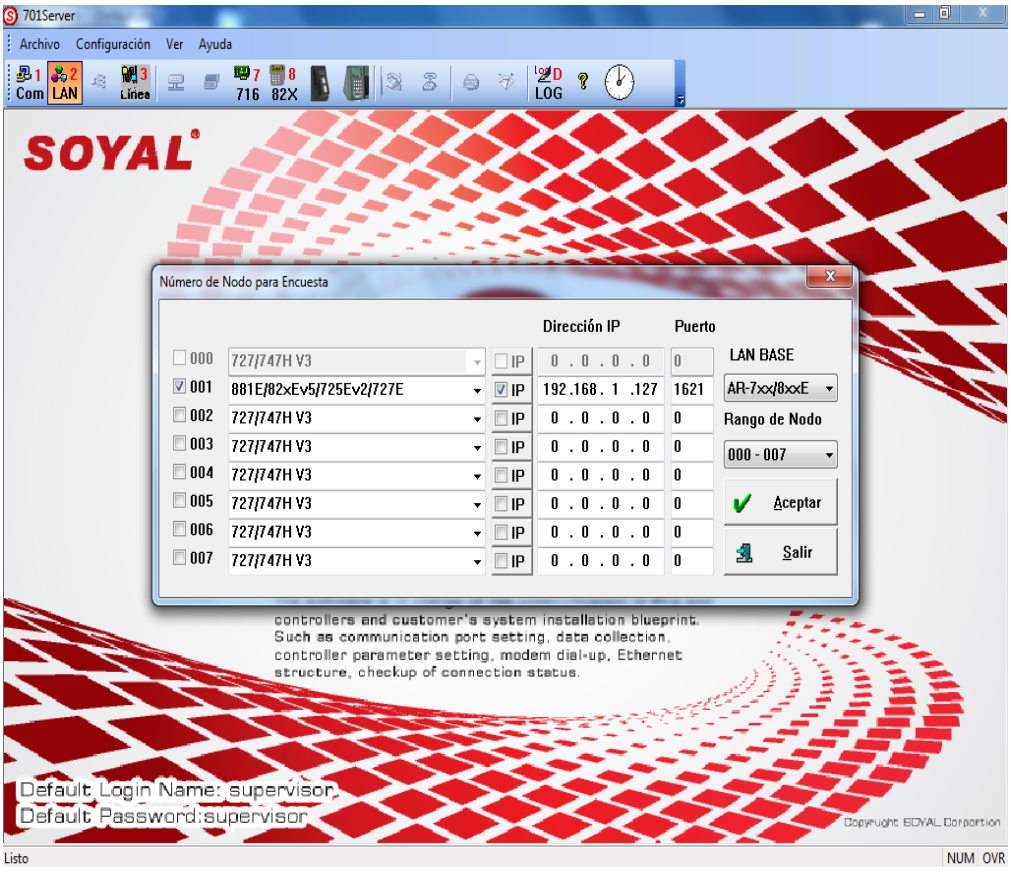


Figura No. 13: Configuración equipos

Los dispositivos que se incluyen en el sistema debe tener un ID diferente. Solamente se configuran en este punto las controladoras y las lectoras que no estén conectadas a una controladora, es decir, las que trabajen como autónomas. Para cada dispositivo, se debe indicar el tipo de equipo. En el caso de monitoreo de equipos mediante la red, seleccione en la casilla IP de la controladora y digite la dirección IP asignada a ella. Adicionalmente se debe colocar el número de puerto que tiene la controladora. De fábrica, la dirección IP de las controladoras es 192.168.1.127 y el puerto 1621.

Finalmente en el estado de los equipos en la pestaña "Botón Line" se puede verificar el cuadro de conexiones donde aparece el árbol con los equipos conectados al sistema. Los

equipos que estén bien configurados y conectados aparecerán con un símbolo al lado del dispositivo en verde; si el equipo está mal configurado o desconectado, aparecerá el símbolo al lado del dispositivo en rojo como se puede ver en la figura No. 26.

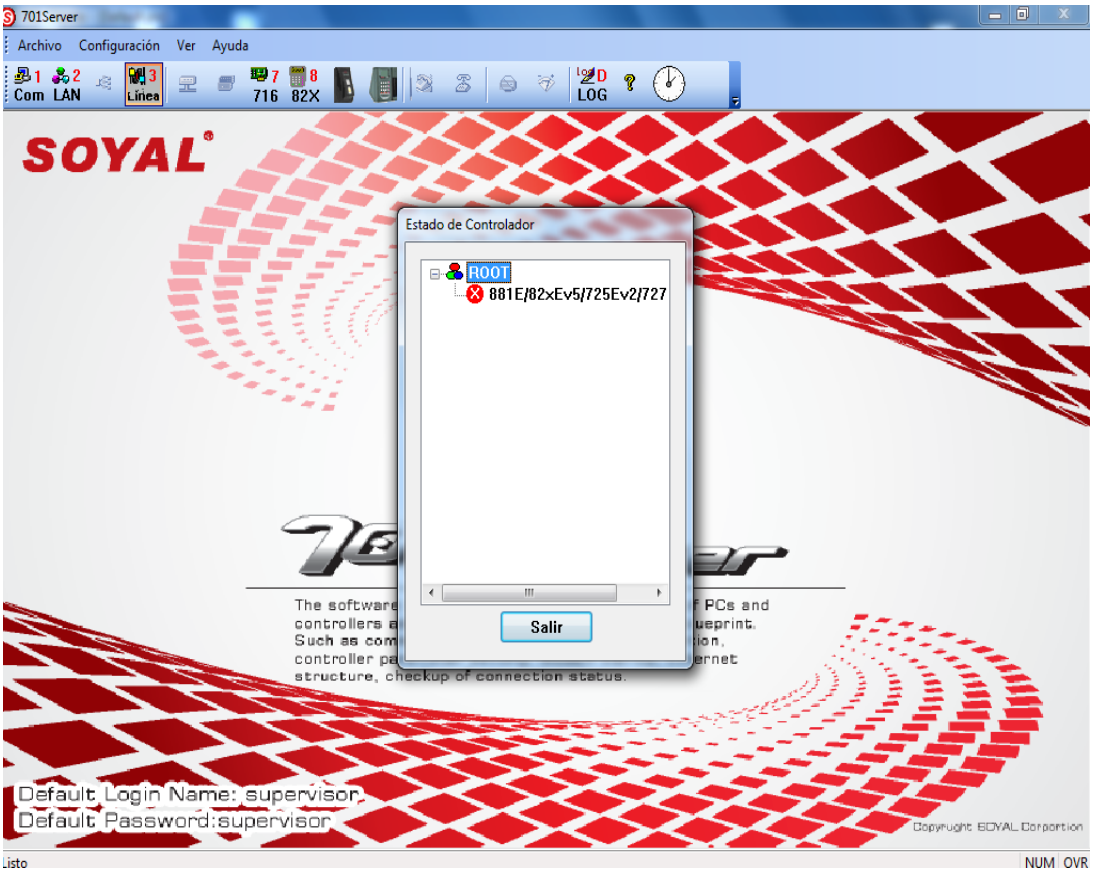


Figura No. 14: Estado de equipos

3.4.2 Configuración de la aplicación de control 701client.

Para garantizar el correcto funcionamiento del software se debe programar el 701 Server; parámetros que son parte del proceso de gestión y monitoreo de los usuarios deben ir en el siguiente orden:

- Puertas (Areas)
- Grupos de Puertas (Group)
- Zonas horarias (Zone)
- Usuarios (User)

La configuración de puertas, grupos de puertas, zonas horarias, se configuran sencillamente en las pestañas del programa. La opción más importante es de usuarios la cual se muestra en la figura No. 27:

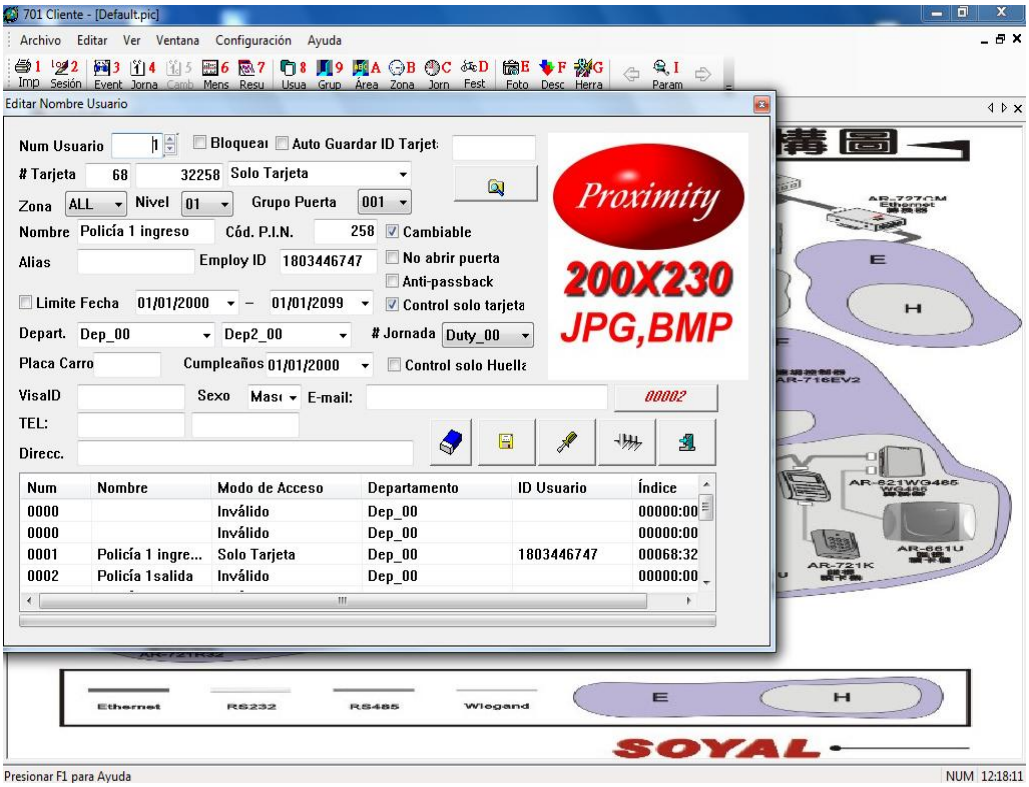


Figura No. 15: Configuración de la aplicación 701client

La configuración de esta opción empieza con la selección del número de usuario que desea editar. El usuario 0 (CERO) no se puede utilizar. En el campo CARD ID, se colocan el número impreso en la tarjeta. Son los dos últimos números de 5 dígitos de la tarjeta. Este programa permite bloquear la interfaz de usuario para evitar que durante el proceso de edición de usuarios, si algún usuario pasa la tarjeta por alguna lectora, la interfaz no cambie mostrando los datos del usuario.

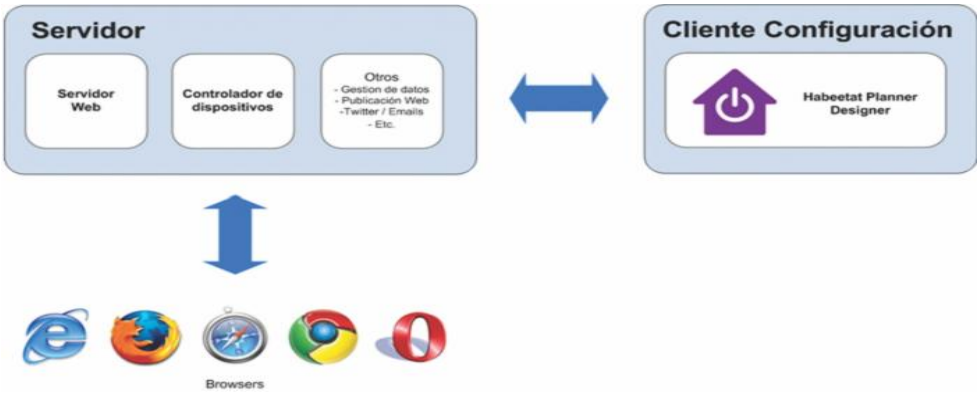
Luego escoja el número de usuario que desea editar, habilite esta opción y pase la tarjeta por alguna de las lectoras para guardar el número de la tarjeta de forma automática. Escriba el dato y presione el botón ubicado debajo para buscar cualquier dato (número de tarjeta,

nombre, cédula, etc.) en la base de datos de usuarios. (hace diferencia entre mayúsculas y minúsculas). También se puede mostrar la foto del usuario.

Finalmente se selecciona el modo de acceso para este usuario. Se puede escoger entre Solo Tarjeta (CARD ONLY), tarjeta o Clave (CARD OR PIN) o tarjeta y Clave (CARD AND PIN). Se escoge la Zona horaria en la que este usuario tendrá acceso. Se escoge el grupo de puertas al que este usuario podrá tener acceso. Como ítem opcional, pero siempre recomendado, se escribe el nombre del tarjeta-habiente. Si el usuario va a tener acceso mediante tarjeta Y clave, en este campo se digita la clave que usará el usuario. Una vez se termina de ingresar la información del usuario, se presiona el botón guardar (SAVE) para agregar este usuario a la base de datos del PROGRAMA 701client.

3.5 Sistema de monitoreo de dispositivos zigbee Habeetat Planner

Es el software de automatización compatible con toda la línea de productos Habeetat, y con una amplia variedad de productos de terceros. Permite crear planos / pantallas que son accesibles y operables desde teléfonos móviles, PC y Tablets a través de Internet (mediante una conexión segura HTTPS) o directamente desde la red local de su casa.[3]



[3] http://support.solidmation.com/HabeetatPlanner/Help/es/que_es_habeetat_planner.ht

Figura No. 16: Arquitectura del software

Sus principales características son:

- Funciona en cualquier PC estándar con Windows (Windows Server 2008 recomendado).
- Simplifica el proceso de adición, sustitución y configuración de Dispositivos en el entorno de Habeetat.
- Le permite crear sus propios planos y que sean accesibles desde Internet con una intuitiva interfaz de arrastrar y soltar.
- Permite la creación de Macros de gran alcance con una interfaz de usuario muy simple.
- Permite definir Escenas programadas en el tiempo u otras basados en la activación de Dispositivos específicos, por lo que se pueden automatizar tareas repetitivas, tales como el riego o el filtrado de la piscina.
- Permite integración nativa con el sistema de audio multi-room de Sonos.
- Incluye un motor para crear Scripts que le permite construir sus propios programas complejos en su lenguaje de programación preferido (JScript, VBScript o Pascal).
- Está basado en una arquitectura abierta que está permanentemente actualizándose para incluir los Dispositivos de otros fabricantes.
- Permite asociar una cuenta de Twitter y configurar qué eventos serán informados mediante un e-mail.
- Permite integrar controladores con PLC Bus.

3.5.1 Procedimiento de instalación[4]:

Los requisitos mínimos para realizar una instalación de Habeetat Planner son:

Un HPA-6200, Unidad de Control más una computadora para visualizar el Habeetat Planner o cualquier ordenador con Windows NT/200/XP/Vista, en donde instalar el Habeetat Planner más una Interface USB, HPA-2400.

[4] http://support.solidmation.com/HabeetatPlanner/Help/es/procedimiento_de_instalacion.htm

Una conexión a internet de banda ancha en el lugar a realizarse la instalación. Esto le permitirá controlar los Dispositivos de la línea Habeetat desde cualquier lugar, previamente configurados en el software.

Uno o más Dispositivos Habeetat.

Descargar e instalación

Los pasos utilizados en esta etapa son los siguientes:

- Descargar la versión Full del software Habeetat Planner desde la página web de Solidmation,

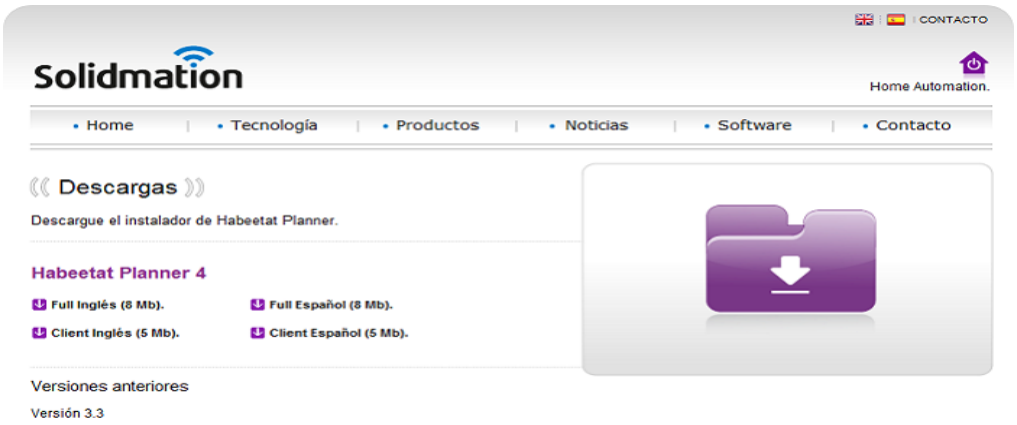


Figura No. 17: Descargar e instalación

- Instalar el Software Habeetat Planner en la PC que se utilizará para la configuración de la instalación a realizar.
- Instalar la "Unidad de Control": HPA-6200, o en su defecto la "Interfaz USB": HPA-2400, para lo cual necesitara también descargar los drivers del Dispositivo desde la página web de Solidmation,
- Instalar los equipos Habeetat que requiera la instalación: controladores de iluminación, cortinas, on/off, contadores de pulso, emisores-receptores IR, etc. Para realizar la correcta instalación de los dispositivos se recomienda leer atentamente el manual de usuario de cada uno de ellos.

Configuración del programa[5]:

Para asegurar el correcto funcionamiento del Habeetat Planner, se deben configurar todas las variables del cuadro de diálogo Preferencias, accediendo desde Menú Principal / Herramientas / Preferencias como se indica en la figura No. 26.

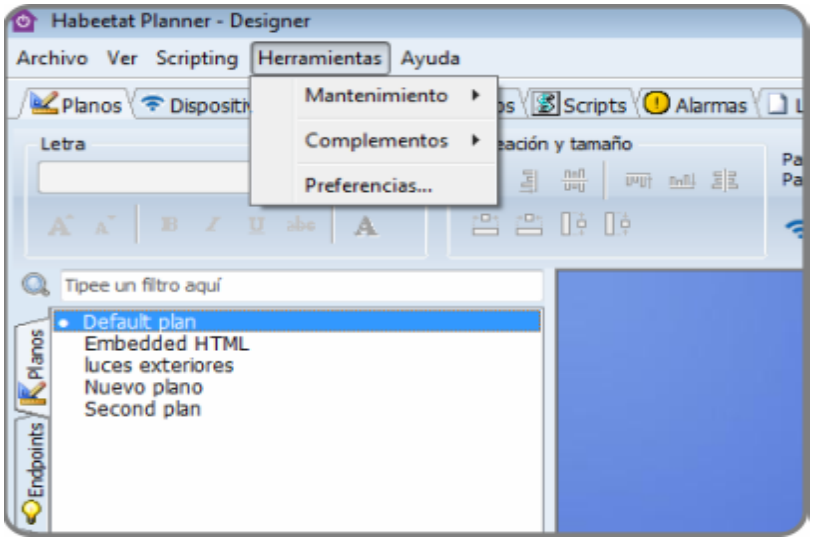


Figura No. 18: selección de preferencias para configuración del software

Web server:

Desde aquí configurará el servidor web incorporado.

- **Configuración de red:** el servidor web incorporado le permite acceder a los planos previamente definidos en el Habeetat Planner, desde cualquier navegador de PC, Smartphone, Tablet, etc. Al elegir el navegador web, debe seleccionar un puerto en el que se escuche (normalmente el puerto 80).
- **Autenticación:** el servidor web compatible con la autenticación, le permite restringir el acceso a ciertos usuarios que usted defina. Por defecto, Habeetat Planner define el usuario admin, con la contraseña que Ud. seleccione en la instalación. No se puede eliminar este usuario, pero puede cambiar su contraseña.

[5] http://support.solidmation.com/HabeetatPlanner/Help/es/configuracion-del-programa.htm

También se pueden crear otros usuarios, y protegerlos con las contraseñas correspondientes.

Autenticación:

La Autenticación es controlada por los siguientes parámetros:

- **Habilitar autenticación de usuarios:** activa o desactiva la autenticación del Habeetat Planner. Si se desactiva, todos los usuarios tendrán acceso a los planos que se definan, sin la necesidad de introducir un nombre de usuario o contraseña.
- **Saltear para redes locales:** le permite eludir la autenticación para las redes locales, definidas en el cuadro de texto debajo de esta opción. Ud. puede instruir al Habeetat Planner para eludir la autenticación en las redes que son "de confianza". Un ejemplo típico es "127.0.0", que representa a todas las conexiones procedentes de la computadora en la que el software está instalado. Puede añadir otras redes separándolas con comas o punto y coma.

Lista de usuarios:

La lista de Usuarios le permite crear usuarios adicionales a los que Habeetat Planner permitirá el acceso. Puede crear tantos usuarios como desee y especificar una contraseña para cada uno de ellos, ver en la figura No. 31

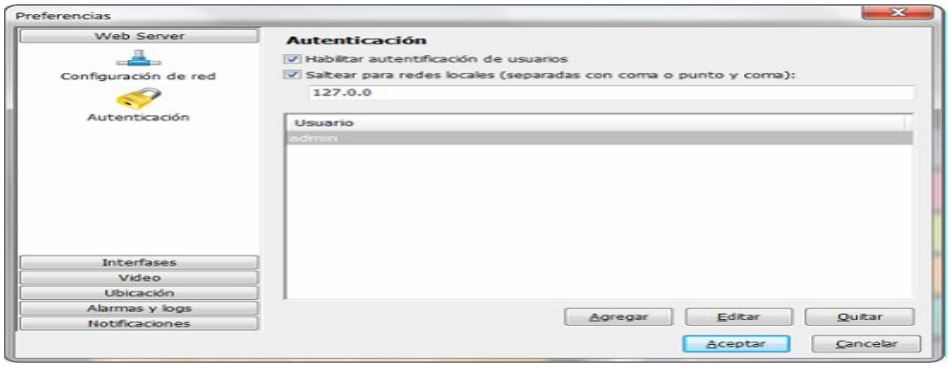


Figura No. 19: Pantalla de autenticación. Lista de usuarios

Interfaces:

Aquí debe configurar con qué tipo de Dispositivos desea trabajar, ver figura No. 33.

El Habeetat Planner le permite integrar Dispositivos Solidmation para redes ZigBee, así como también dispositivos de la línea Habeetat y dispositivos con tecnología PLCBus.

Para instalar los Dispositivos de Solidmation, debe Habilitar la interfaz Habeetat ZB

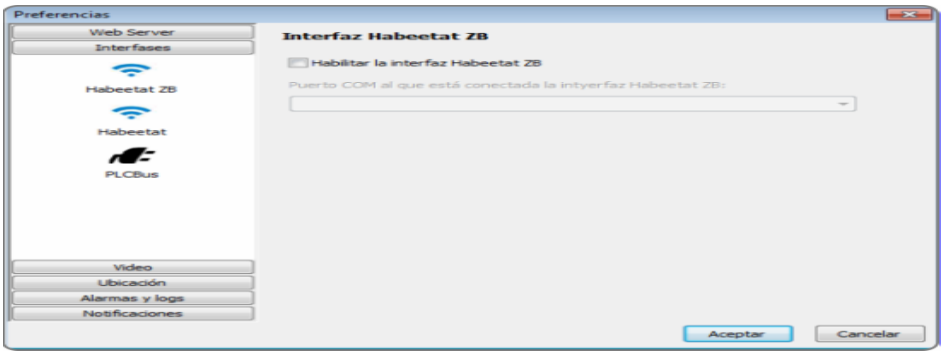


Figura No. 20: selección del tipo de interfaz, según el dispositivo a utilizar

Video:

Le permite administrar las cámaras de video IP de diferentes fabricantes. Desde esta pestaña Ud. podrá agregar o quitar equipos así como también configurar el puerto IP de cada uno de ellos y establecer una clave de acceso si lo cree necesario para la instalación que está diseñando, ver figura No. 33.

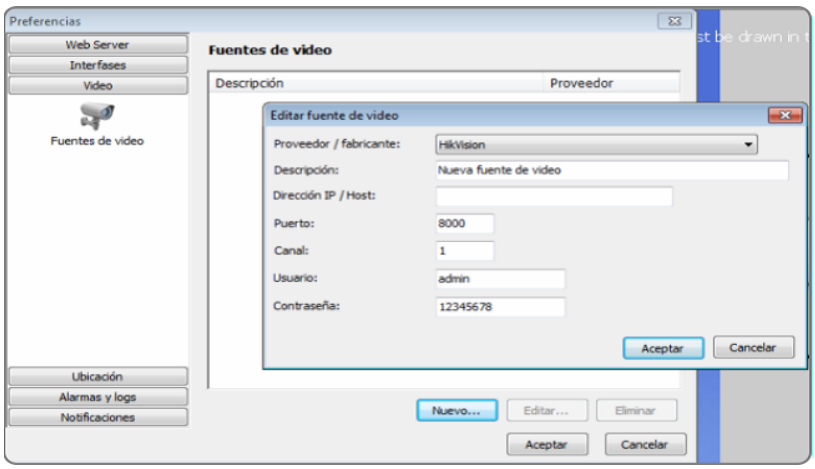


Figura No. 21: Integración de cámaras ip

Ubicación:

Con el fin de configurar su ubicación geográfica, especifique su país, región y ciudad, o introduzca directamente coordenadas de su ubicación en latitud y longitud, ver figura No. 34.

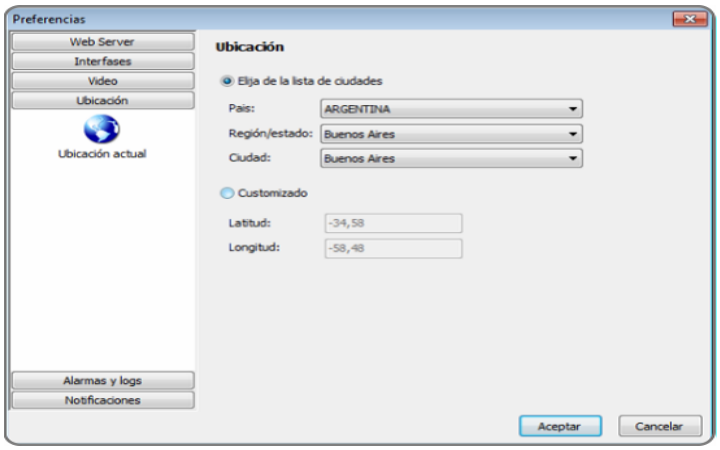


Figura No. 22: Configuración de ubicación geográfica

Alarmas y Logs:

Aquí podrá configurar las notificaciones para alarmas y la cantidad de días que desee guardar los Logs del Server.

- **Alarmas:** configure el tipo de notificación (mail, twitt o macro) que desee que se ejecute para cada Tipo de alarma que se active desde el Servidor o desde los Dispositivos.
- **Depuración:** se puede especificar un número de días (entre 1 y 180) para que las alarmas se mantengan dentro de la base de datos de Habeetat Planner. Alarmas mayores a este parámetro se eliminarán de la base de datos de forma automática, ver figura No. 35.

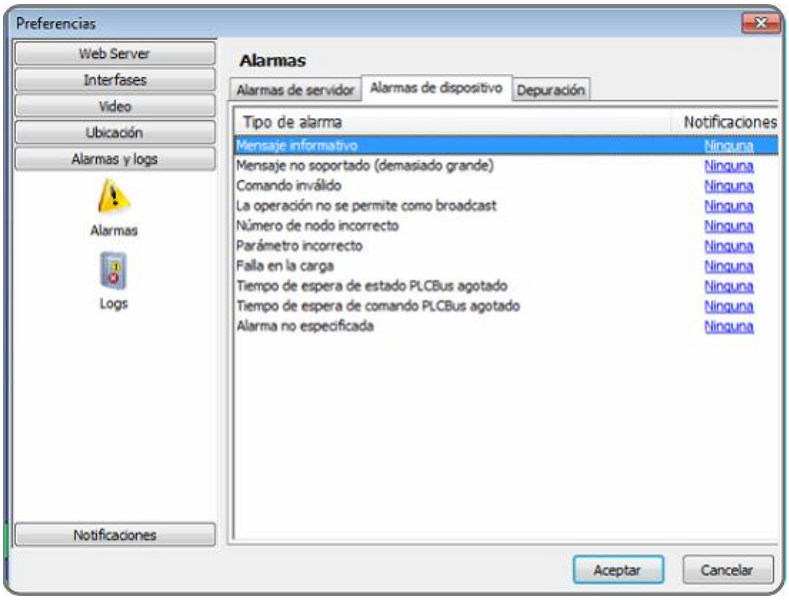


Figura No. 23: Configuración de alarmas

Logs:

Esta opción le permite especificar el número de días (entre 1 y 180) que los archivos de registro se almacenan en el Servidor carpeta. Estos registros contienen un detalle de actividades del servidor de Habeetat Planner.

Notificaciones:

Son mensajes que puede enviar de manera automática el sistema a una cuenta de Twitter. Estas notificaciones deberán ser configuradas posteriormente, en este paso solo se deberá vincular una cuenta de Twitter existente a la instalación de Habeetat Planner

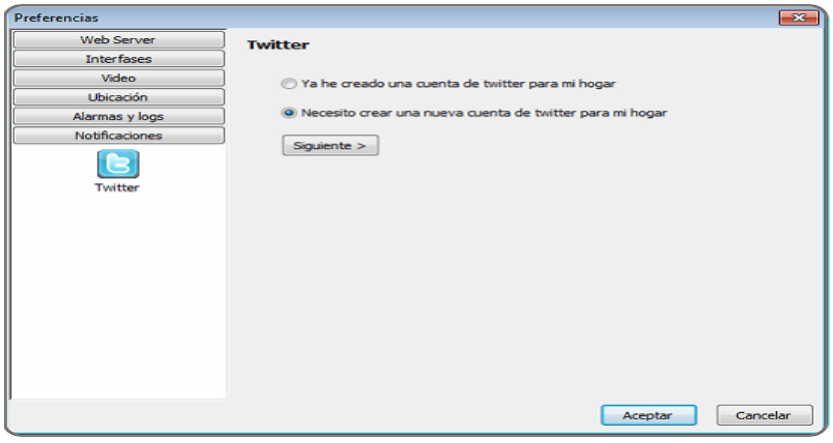


Figura No. 24: Configuración de notificaciones

Diseño de la aplicación:

A continuación en la figura No. 33, se presenta la interfaz gráfica de la solución planteada para mediante acceso web poder tener control de cada una de las cerraduras del prototipo diseñado

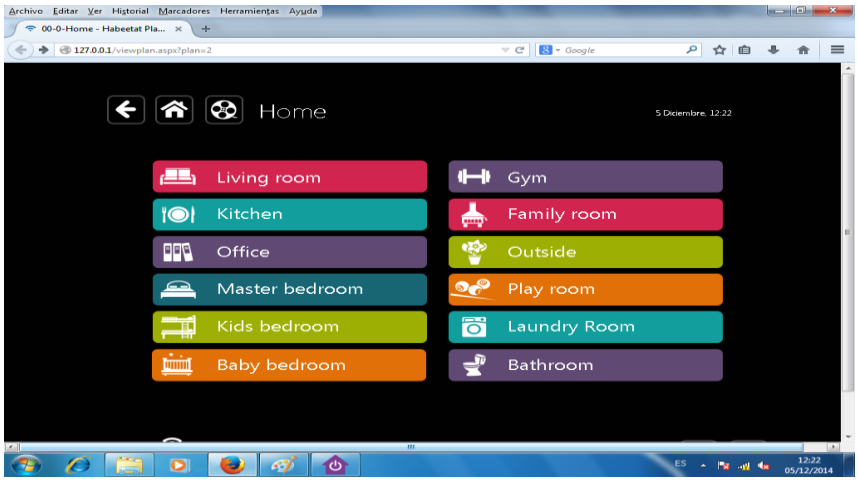


Figura No. 25: solución de control vía web.

Planos

Es en esta pantalla figura No. 37, en donde se realiza la elección del número de ventanas que aparecerán en la interfaz gráfica, así como los botones que enlazan mediante la comunicación y la correspondiente programación con cada una de las salidas del relé vía zegbee

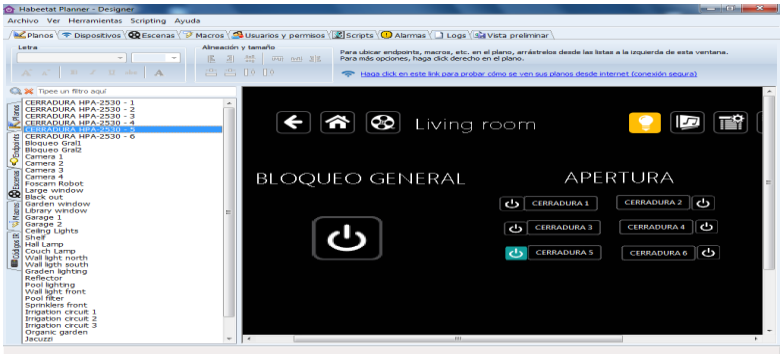


Figura No. 26: Planos para la aplicación para bloqueos y aperturas emergentes

Dispositivos:

En la figura No. 35 donde se encuentran todos los dispositivos conectados a nuestra aplicación en este caso los dispositivos zigbee y las cámaras ip, además es aquí en donde se puede realizar la configuración e incorporación de nuevos dispositivos

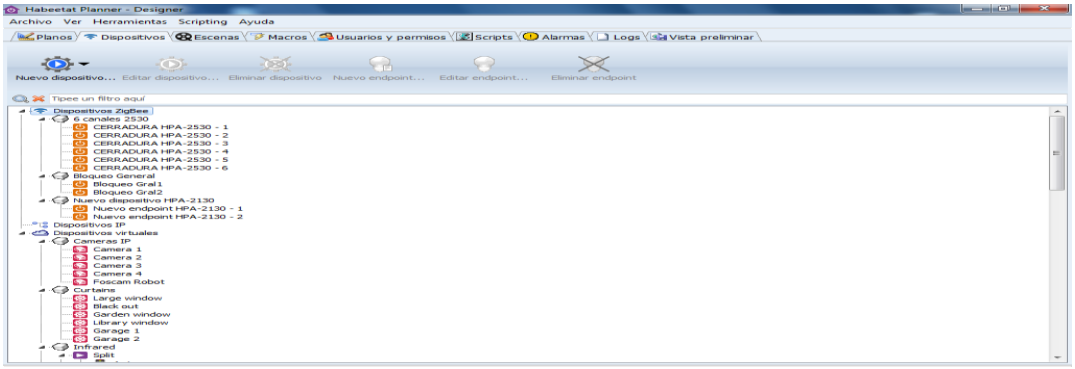


Figura No. 27: Dispositivos utilizados en la aplicación

Macros:

A continuación en la figura No. 40se presenta la lista de asignación de macros enlazada con cada uno de los botones utilizados en la pantalla plana.

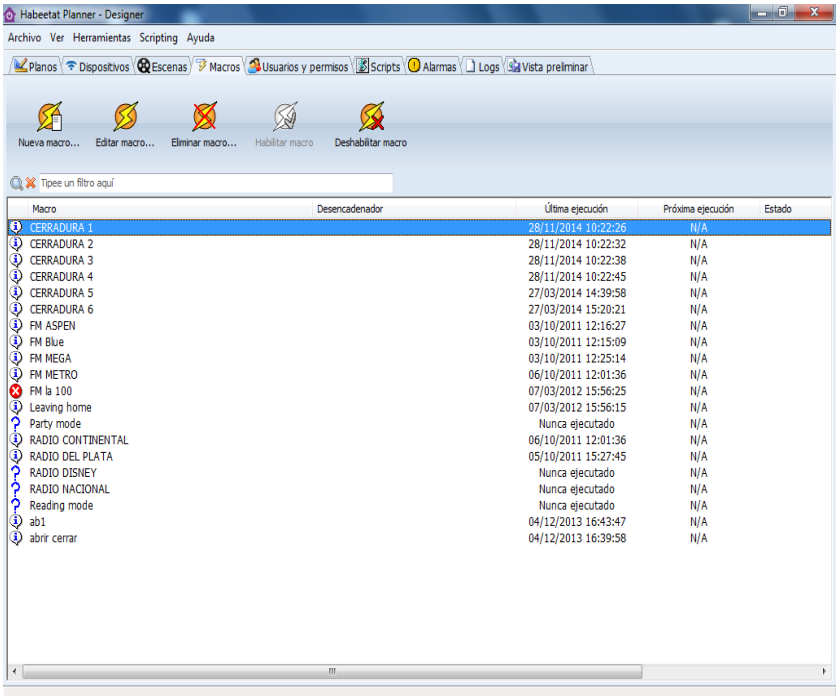


Figura No. 28: Lista de asignación de macros

3.6 Arreglos institucionales y modalidad de ejecución

Este proyecto se lo realizó de forma independiente y está dirigido a cuarteles, repartos, unidades militares, policiales y dependencias de empresas de seguridad con especial atención a los nuevos UPC y en adelante a cualquier institución ya sea pública o privada, que requiera el sistema.

Tabla No.9 : Arreglos institucionales

ARREGLOS INSTITUCIONALES		
Tipo de ejecución		**Personas involucradas**
Directa (D) o Indirecta (I)	**Tipo de arreglo**	
D	Desarrollo del sistema de la caja de seguridad.	ESTUDIANTE - ELECTROMECÁNICOS
D	Compra de equipos	ESTUDIANTE -PROVEEDORES
D	Integración de todos los componentes	ESTUDIANTE-TUTOR

3.6.1 Cronogramas valorados por componentes y actividades.

Para el cronograma valorado se tomara las etapas del proyecto para las fuentes de financiamiento.

Tabla No.10: Fuentes de Financiamiento

	FUENTES DE FINANCIAMIENTO			
Componentes/Rubros	**TOTAL**			
	Crédito		**R. Propios**	
	Periodo 1	**Periodo 2**	**Periodo 1**	**Periodo 2**
Diseño del Caja fuerte	-	-	-	30
Compra de Material.	-	-	2693,55	2693.55
Armado del Caja fuerte componentes físicos.	-	-	800	800
Montaje de los componentes lógicos.	-	-	45	45
Ensamblar los componentes tanto físicos como lógicos del Caja fuerte.	-	-	50	50
Desarrollo del sistema	-	-	300	300
Mantenimiento del Sistema	-	-	30	30
Servicios Básicos	-	-	50	50
Total	-	-	5.133.29	5.133.29

3.6.2 Origen de los insumos

Para el origen de los insumos se tomara las etapas del proyecto para describir su origen.

Cuadro No. 3: Orígen de insumos

Componentes/Rubros	Tipo de bien	ORIGEN DE LOS INSUMOS		TOTAL
		Nacional	Importado	
TAG DE SEGURIDAD	Final	0%	100%	100%
LECTOR HUELLA DIGITAL/PROXIMIDAD/PIN OPT: AR-821ES-OS	Final	0%	100%	100%
MODULO CONTROL DE ASCENSORES AR-401R	Final	0%	100%	100%
FUENTE PARA CAMARA 12V 1.5AMP ST-P150	Intermedios	0%	100%	100%
FUENTE ALIMENTACION 12V 3.5AMP CON/BAT ST-PB350.	Intermedios	0%	100%	100%
DISCO DURO 500GB	Final	0%	100%	100%
MAIN BOARD DUAL CORE 3GB	Intermedio	0%	100%	100%
MEMORIA RAM DDR3 2GB	Intermedio	0%	100%	100%
PLANCHA DE ACERO INOXIDABLE	Intermedio	0%	100%	100%
CERRADURAS ELECTRICAS	Final	0%	100%	100%
TARJETA DE RED WIRELESS 150 MB	Intermedio	0%	100%	100%
Total		0%	100%	100%

Todos los componentes y materiales que se utiliza en este proyecto son importados, debidos a que se utiliza tecnología de punta y los suministros no se los produce en el país.

3.7 Estrategia de seguimiento y evacuación

3.7.1 Monitoreo de la ejecución

Cuadro No. 12: Monitoreo de ejecución

Etapas	Acciones	% de Avance	Número de Personas
Diseño del Caja fuerte	Bosquejo del Caja fuerte	100%	En esta etapa interviene 1 persona.
Compra de Material.	Designar a que proveedores se le comprara los suministros	100%	En esta etapa interviene 1 persona.
Designación de espacio en la empresa.	Modificar el espacio	100%	1 personas
Armado del Caja fuerte componentes físicos.	Ensamblar los componentes físicos	100%	3 personas
Montaje de los componentes lógicos.	Acoplar los componentes	100%	2 personas
Ensamblar los componentes tanto físicos como lógicos del Caja fuerte.	Unir todos los componentes y ver q funciones correctamente como fue diseñado	100%	2 personas
Implementación de los diferentes software de control.	Aplicativos comerciales de fábrica del producto.	100%	2 personas
Pruebas	Realizar pruebas.	100%	2 personas
Mantenimiento del Sistema	Revisión componentes	0%	1 personas.

3.7.2 Evaluación de resultados e impactos.

Definir el proceso a realizar después de finalizado el proyecto, con el propósito de determinar los productos o metas alcanzadas.

- Agregar usuarios para que el sistema tenga todos sus registros con todos los usuarios que utilizan la caja fuerte.
- Desarrollar el sistema.
- Realizar controles de mantenimiento preventivo.
- Realizar una evaluación del sistema al cabo de 1 año para ver los resultados del sistema.

3.7.3 Actualización de línea base.

Una vez que se obtenga el financiamiento y se vaya a ejecutar el proyecto, la institución, de ser necesario, deberá actualizar la línea base.

CAPÍTULO IV

4. PRESUPUESTOS

Para el cálculo de los costos de operación y mantenimiento se tomaron en cuenta el tiempo que nos tomará desplazarnos a las entidades que adquieran el sistema.

También se sumaran el material utilizados en todo el proceso del desarrollo del proyecto y todo lo concerniente en el proyecto, tanto material como humano.

Tabla No. 13: Presupuesto de equipos

LISTA DE MATERIALES							
NUMERO	DISPOSITIVO	MARCA	PROVEEDOR	CANTIDAD	CARACTERISTICAS TECNICAS	PRECIO UNITARIO	PRECIO FINAL
1	TAG	GENERICO	COMERCIALIZADOR INDEPENDIENTE	30		1,20	40,32
2	Lector huella digital/proximidad/ pin opt: ar-821es-os	SOYAL	SEGUTELEC	1	Frecuencia: No RF o banda 125 kHz o 13,56 o doble. Estándar: ISO 15693 Fuente de alimentación: 10-24 VDC. Consumo de energía: 5W.	353,220	353,22
3	Modulo control de ascensores ar-401r	DIGIKEY	SEGUTELEC	1	Velocidad de transmisión: 4800bps/9600bps/19200bps(N, 8, 1). Fuente de alimentación: +9 ~ +24VC. Capacidad de los contactos: AC: 110V@0.6A DC: 24V@2A Peso: 1,780g±10g. Canales: 1. 16 Form C Relay Output	121,225	121,23
4	Fuente para camara 12v 1.5amp st-p150		SEGUTELEC	1	Fuente de alimentación: 12.5v 3.5 AMP. Voltaje de entrada: 100-120V / 200-240V 50~60Hz Intensidad de salida (trabajo): 5 A Potencia de salida (trabajo): 60 W Potencia de salida (pico): 90 W	3,890	3,89
5	Fuente alimentacion 12v 3.5amp con/bat st-pb350.		SEGUTELEC	2	Fuente de alimentación: 12.5v 3.5 AMP. Voltaje de entrada: 100-120V Intensidad de salida (trabajo): 5 A Intensidad de salida (pico): 7,5 A	33,330	66,66
6	Fuente de poder	DELUX	BIOCENTER	1	Conexiones: 24 pins, 3x4 pins, 2 SATA.	12,900	14,49
7	Cámara	DELINK		1		56.50	56.50
8	Disco duro 500gb	SEAGATE	BIOCENTER	1	ANCHURA: 10.2 CM. PROFUNDIDAD: 14.7 CM. ALTURA: 2.6 CM. PESO: 0.72 KG. CAPACIDAD: 500 GB.	63,980	71,66

9	Main board dual core 3gb	BIOSTAR	BIOCENTER	1	Socket LGA 775 Supported Intel Core 2 Quad/Core 2 Duo/Pentium Dual-Core/Celeron Dual-Core/Celeron 400 Series Processor Supported FSB 533/800/1066/1333MHz	70,430	78,88
10	Memoria ram ddr3 2gb	KINGSTON	BIOCENTER	1	Capacidad: 2Gb Tipo: DDR3 Velocidad: 1333 Mhz Latencia: 9 Voltaje: 1,5 Volts Requerimientos: Motherboard con soporte para DDR3 1333Mhz	19,350	21,67
11	Cerraduras electricas			17		44,63	1829,03
12	Tarjeta de red wireless 150 mb	D-LINK	BIOCENTER	1	Tecnología Wireless N 150: hasta 150Mbps de velocidad Wireless. Compatible con la nueva tecnología Wireless N y tecnología ampliada Wireless G Certificado WiFiProtectedSetup™ (WPS)	14,440	16,17
13	Planchas de acero inoxidable		IMPORT.COM	1	Plancha inoxidable de 3mm	325,89	715,4
						SUB-TOTAL	3.389.08
						IVA	406.69
						TOTAL	3.795.77

.

1. Para el diseño de la Caja fuerte se invertirá la cantidad de $ 30 dólares americanos.
2. El presupuesto para contratar la compra del material es de $ 2693,55 dólares americanos incluido IVA.
3. En esta etapa de armar los componentes físicos de la caja de seguridad electrónica biométrica se invertirá un valor de $800 dólares americanos incluidos IVA.
4. En el montaje de los componentes lógicos se tiene un presupuesto de $ 45 dólares americanos incluidos IVA.
5. Para esta etapa de unir los componentes tanto físicos como lógicos el presupuesto es de $ 50 dólares americanos incluidos IVA.
6. Desarrollo del sistema una cantidad de 300 dólares americanos incluido IVA.
7. Mantenimiento del sistema 30 dólares americanos incluido IVA.
8. Servicios básicos 50 dólares americanos incluido IVA.

4.1 Identificación y valoración de la inversión total, costos de operación y mantenimiento, ingresos y beneficios.

Inversión:

La inversión es de $4.478.38 dólares americanos incluido el IVA, como se lo detalla en la tabla anterior y en la siguiente tabla se incrementó los rubros de mantenimiento del sistema.

4.2 Presupuesto

El presupuesto correrá a cargo del Estudiante con capital propio.

Tabla No. 14: Presupuesto total

Número	Acción	Precio
1	Diseño del Caja fuerte	30,00
2	Materiales	2.693.55
3	Armado de la caja de seguridad, componentes físicos	800,00
4	Montaje de los componentes lógicos	45,00
5	Ensamblado de los componentes tanto físicos como lógicos de la caja de seguridad	50,00
6	Desarrollo del Sistema	300,00
7	Mantenimiento del Sistema	30,00
8	Servicios Básicos	50,00
	SUB-TOTAL	3.998.55
	IVA	479.83
	TOTAL	4.478.38

CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Se cumplió con el objetivo general que fue el Diseño del nuevo producto "**Caja de seguridad electrónica biométrica**" que consiste en una caja fuerte para guardar armas de fuego para policías, miembros de las Fuerzas Armadas y Guardias de seguridad.
- El nuevo producto cumple, con los requerimientos actuales para seguridad de especies valoradas y armamento para empresas públicas y privadas.
- Los sistemas biométricos de seguridad, asegurarán un correcto control del uso de la caja fuerte, disminuyendo en gran porcentaje su vulnerabilidad por adulteración de documentos de identidad.
- La utilización de la caja de seguridad que utiliza sistemas biométricos de identificación, asegurará que las armas de fuego sean ingresadas y extraídas por sus verdaderos usuarios el momento que vaya a realizar su servicio.

RECOMENDACIONES

- Fomentar la utilización de la caja de seguridad, para evitar el uso de métodos tradicionales de control de identidad, lo que provoca pérdida de valores y crea desconfianza en los usuarios.
- Al diseñar un software biométrico de seguridad, se debe considerar que dichos programas cumplan con los estándares internacionales.
- Se recomienda para futuras ampliaciones utilizar análisis de imágenes para aumentar la seguridad del sistema.
- Se recomienda usar una base de datos estándar para que la ampliación sea posible.

Bibliografía

Alegsa. (3 de 5 de 2010). *Diccionario informático*. Recuperado el 20 de 11 de 2013, de http://www.alegsa.com

David. (27 de mayo de 2012). *Historia de la caja fuerte*. Recuperado el 16 de 11 de 2013, de Cuaderno de David: http://cuadernodeldavid.blogspot.com

Diccionario. (2013). *definición de caja fuerte*. Recuperado el 26 de 11 de 2013, de http://www.wordreference.com/definicion/caja%20fuerte

eHow. (s/d). *Caja fuerte de pared*. Recuperado el 17 de 11 de 2013, de eHow en español: http://www.ehowenespanol.com

González, V. (11 de 08 de 2011). *ElDiario*. Recuperado el 25 de 11 de 2013, de http://eldiario.com

imágenes, g. (s/d). *Imágenes de bóvedas de bancos*. Recuperado el 16 de 11 de 2013, de http://www.bancafacil.com

moofmonster. (s/d). *www.moofmonster.com*. Recuperado el 15 de 11 de 2013, de http://www.google.com.ec

WebAcademia. (s/d). *Seguro, historia, especificaciones, bóbedas a prueba de fuego*. Recuperado el 16 de 11 de 2013, de http://centrodeartigos.com

ANEXOS

Anexo 1

Selección de los medios de acceso.

Los medios seleccionadas son de dos clases la una es un TAG de marca genérica compatibles con lector Soyal que trabaja en una frecuencia de 13.56 HMZ que cumple con las características técnicas necesarias para este tipo de aplicación ya que permite configurar al dispositivo también con pin o clave y la huella dactilar.

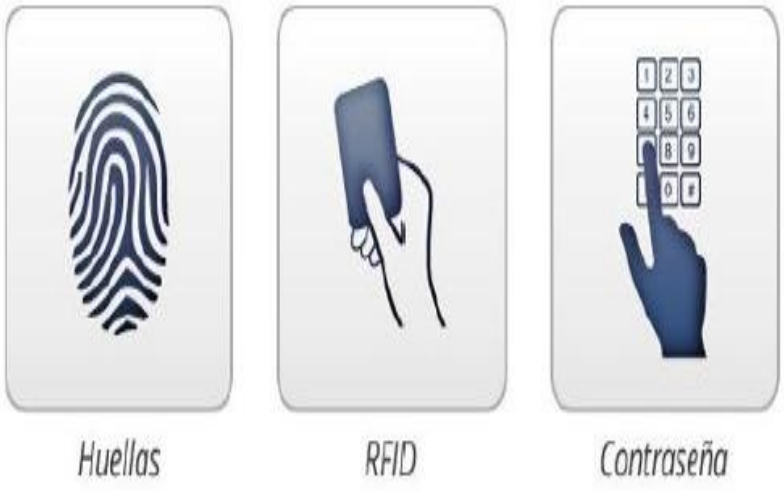


Figura No. 29: Medios de acceso

Fuente: (ZKSoftware, 1995, pág. 1)

Anexo 2.

Características técnicas de cada uno de los medios de acceso:

Tabla No. 15: Características de los tags

Dimensiones (mm):	3cmx0,57 cm
Frecuencia de Trabajo:	13,56 Mhz
Velocidad de Inicio:	Dependiendo de la Memoria del Ordenador
Material:	Plástico
Temperatura de Operación:	-25 to 55°C
Ensamblaje:	Molde de Inyección
Color:	Negro / Banco
Peso:	3 g
IP:	IP68
RoHS:	Amigable
Tamaño de Almacenamiento:	2000 pcs

Anexo 2.

Características de la lectora biométrica.

La lectora se ha seleccionado de acuerdo a la aplicación de acceso con la capacidad de funcionar con tarjeta, pin o huella. Es un controlador de acceso de la marca SOYAL modelo AR-821EF con lector de huella digital tipo inductivo, además tiene lector de proximidad incorporado y teclado para ser programado de forma Stand Alone (independiente) o mediante software propio de SOYAL que se detallara en el capítulo III.

Figura No. 30L Lectora biométrica

Fuente: (Criminalística, 2012, pág. 4).

Dispone de una pantalla lcd, donde muestra la fecha, hora, código de tarjeta o tag (ya sea autorizado o no), de igual forma la huella incorrecta o autorizada, todo el menú de su programación y el nombre de usuario (con un máximo de 11 caracteres).

Cuadro No. 16: Especificaciones lectora biométrica

Las especificaciones técnicas se detallan en la tabla 3 donde se puede verificar los modos de comunicación RS-485 o TCP/IP, así:Frecuencia:	No RF or 125kHz or 13.56MHz or Dual Band
Estándar:	125kHz:EMStandard 13.56MHz:ISO14443A DESFire (opcion) PSAM (opcion) NFC (opcional)
Rango de Lectura:	125kHz 3.56 5 15cm: 2-5cm
Fuente de Alimentación:	10-24VDC
Consumo de Energía: Interfaz de Comunicación:	<5W RS-485 Ethernet
Velocidad de Transferencia de Datos:	9600bps (N,8,1) 10 / 100M Base T
Temperatura de Funcionamiento:	0°C a +60°C
Entrada Digital:	Contacto de Salida (RTE) x 2 / Puerta x 2
Salida de Relé:	Relé de alarma / Rele de bloqueo
Bloqueo Hora Relay:	Toggle, 0.1 ˜ 600sec.
Hora de Alarma:	Toggle, 1 ˜ 600sec.
Interruptor anti sabotaje:	Final de Carrera (Modelo C)
Capacidad de Usuarios:	16000
Registro de Eventos:	32000
Lector Externo:	1WG Puerto
Anti-pass-back:	Si
Teclado de Materiales:	Caucho
Material de la Cubierta:	ABS
Uso Horario:	63
Peso (g):	Sensor Optico (DO): 470±10 Capacidad Sensor (MT): 420±10
Lejos:	<0.001%
FRR:	<1%
Capacidad de registro de Huellas:	9000
Aut. Velocidad:	0.8sec.

Anexo 3

Selección del módulo de Salidas de relé.

El modulo se ha determinado con el objetivo de controlar las salidas de relé seco para el acceso a las diferentes celdas de la caja fuerte de manera digital atreves de la lectora biométrica mediante la activación de chapas o cerraduras electromagnéticas, el modulo utilizado es de la marca Soyal, modelo AR-401R, que corresponde a una tarjeta de 16 salidas de relé NC/NA cada uno con soporta una corriente de 2A, que permite manjar cargas de esta potencia.

Figura No. 31: Módulo de salidas de relé
Fuente: (soyal, s/d, pág. 2)

A continuación se presentan las características de este módulo y las conexiones eléctricas entre la lectora biométrica y el módulo de salidas mediante el convertidor:

Tabla No. 17: Características del módulo de salidas

Fuente de Alimentación:	10-24VDC
Consumo de Energía:	8W
Interfaz de Comunicación:	RS-485
Velocidad de Transferencia de Datos:	9600bps (N,8,1)
Canal:	Salida 16 Formulario C Relay
Indicador:	Potencia: Tx / Rx; Relay (ON/OFF)
Reloj de Tiempo Real:	No
Material de la Cubierta:	Metal
Dimensiones (mm):	180(L) x 231(W) x 62(H)
Peso (g):	1780±10

Anexo 4.

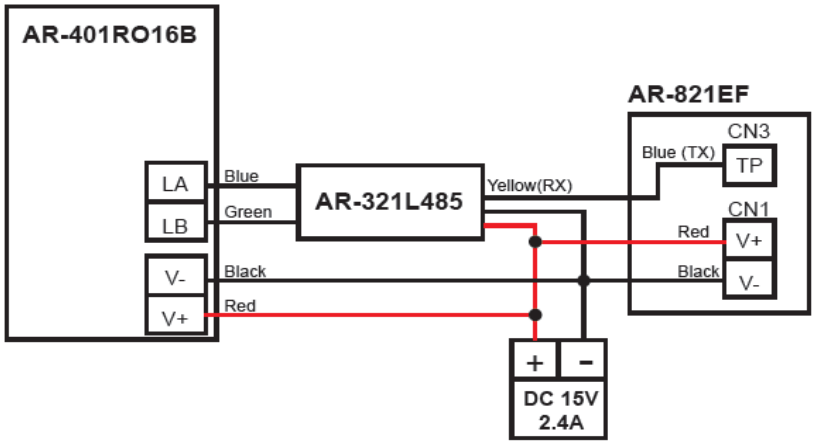


Figura No. 32: Conexión eléctrica entre lectora biométrica y módulo de salidas

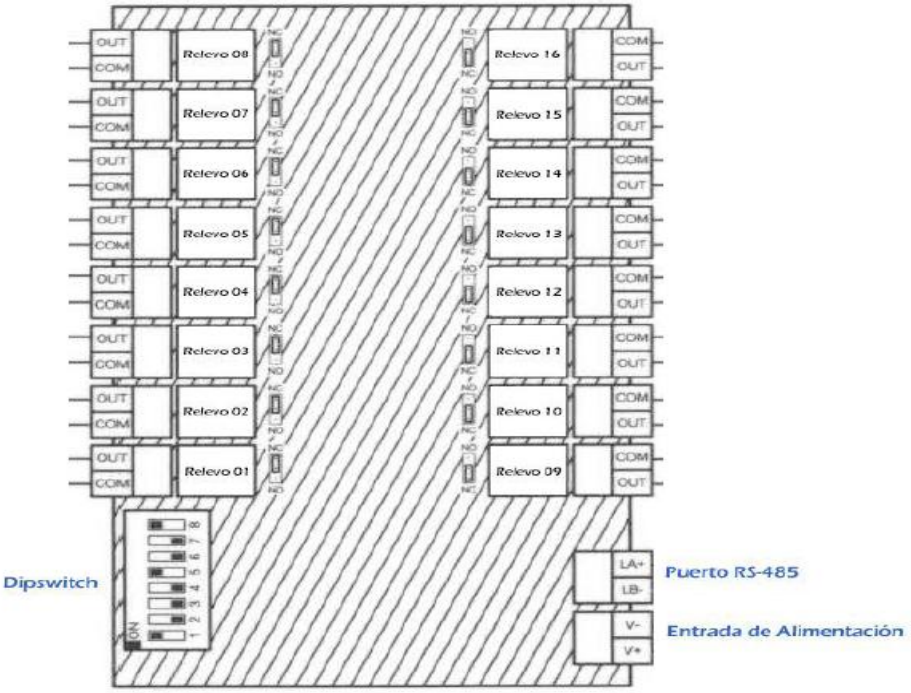


Figura No. 33: Conexiones del módulo de salidas

Elaborado: Germán Luzuriaga

Anexo 5

Selección del módulo de Salidas de relé Zigbee.

El modulo se ha determinado como modo de seguridad para controlar las salidas de relé seco para el acceso a las diferentes celdas de la caja fuerte de manera inalámbrica a través del software instalado en el servidor o una aplicación para el móvil. Mediante este módulo de tecnología Zigbee se puede controlar de manera paralela la activación de chapas o cerraduras electromagnéticas o si el caso restringir o dar apertura total o parcial a las celdas de la caja fuerte. El modulo utilizado es de la marca SOLIDMATION, modelo HPA-2500-LV que es un módulo de 6 entradas y 6 salidas a relay de montaje riel DIN, integrado al software mediante el dispositivo HPA-2400 que es una interfaz USB para domótica, que permite a la infraestructura Solidmation-Habeetat comunicarse con una PC o un servidor que esté ejecutando el software.

El modelo HPA-2500-LV es un dispositivo que permite interactuar con hardware externo, tales como sistemas de alarma, sistemas de control remoto, controles de acceso, etc. Es capaz de controlar cargas pequeñas (de hasta 3A), así como leer entradas de contacto seco o de colector abierto.

Figura No. 34: Módulo de salidas Zigbee

Fuente: (Santiago, 2008, pág. 15)

El modelo HPA-2500-LV cumple con las Normas de emisión electromagnética, garantizando no interferir en otros equipos.

Características Técnicas

- Tensión: 12 VDC.
- Sección máxima de los cables para la instalación: 1,5 mm2.
- Consumo de energía: < 1 W.
- Carga: 3 A por canal.
- Torque máximo sobre los bornes (tornillos de conexión): 0.5 Nm.
- Antena mono polar reemplazable, con conector estándar RPSMA.

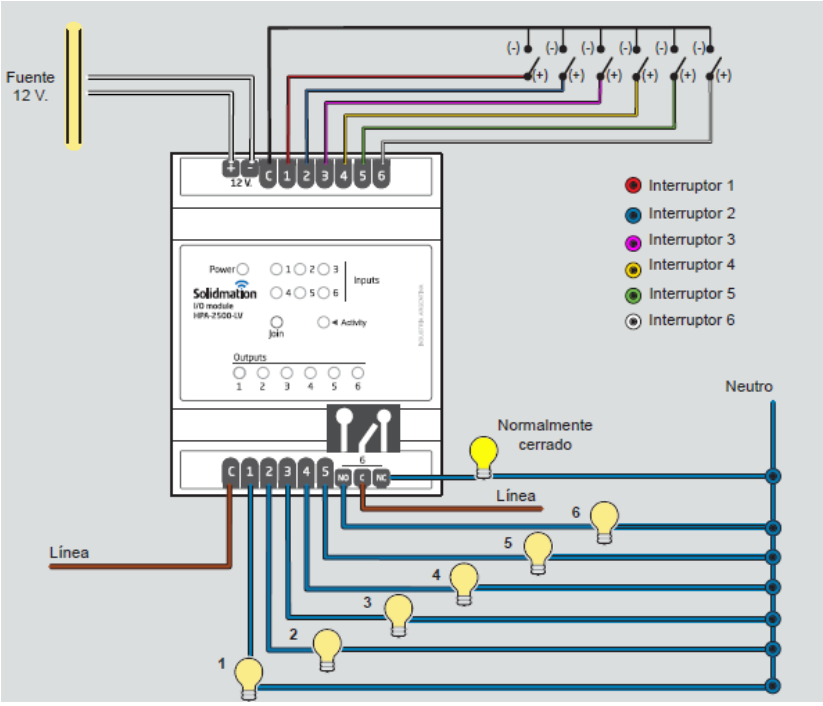


Figura No. 35: Diagrama de conexiones del Módulo de salidas Zigbee.

Fuente: (Santiago, 2008, pág. 15)

Por otro lado el HPA-2400 permite la integración de una red de dispositivos Habeetat con el software Habeetat Planner. Debe ser combinado con otros productos de la familia Habeetat como los controladores de escena.

Conectada con el software Habeetat Planner permite controlar sus dispositivos desde una variedad de plataformas tales como ordenadores, teléfonos inteligentes, tablets, etc .

Figura No. 36: Módulo interfaz USB

Tabla No:18 Características técnicas Modulo interfaz USB

Físicas	Dimensiones: 40 x 70 x 22 mm. Caja: Plástica Color: Blanco
Eléctricas	Potencia Eléctrica: Alimentada Directamente desde el Host USB Consumo de Energía: 85mA en reposo, 250 mA durante la transmisión
Comunicación	Velocidad de Datos: 250kbps Rango Inalámbrico: Hasta 50 metros sin repetidores, 50 metros adicionales por repetidor. Canales Inalámbricos: 16 Frecuencia de radio: 2.4Mhz Protocolo de Comunicación: ZigBee
Operación	LED testigo de actividad, enlace y encendido
Condiciones Ambientales	Temperatura de Funcionamiento: -5 a 60°C Humedad de Funcionamiento: hasta un 80% sin Condensación
Aplicaciones	Automatización de Casas Automatización de Edificios

Anexo 6

Router inalámbrico

El router se ha seleccionado específicamente por la aplicación y los requisitos de un Router inalámbrico a 300Mbps. La marca del dispositivo es TP Link y el modelo es el TL-WR841N. Con la tecnología MIMO 2T2R, el TL-WR841N crea un rendimiento inalámbrico excepcional y avanzada, lo que es ideal para la difusión de vídeo de alta definición, realizar llamadas VoIP y camaras IP. Además, la configuración rápida de Seguridad (QSS), asegura el encriptado WPA2, la prevención de la red de intrusiones externas cumple con la norma IEEE 802.11N, el TL-WR841N puede establecer una red inalámbrica y obtener hasta 15 veces la velocidad y 5 veces el alcance comparado con las otras marcas Además, con velocidades de transmisión de hasta 300Mbps. En cuanto a la seguridad de la conexión WI-FI, el encriptado WEP ha dejado de ser el más fuerte y más seguro como protección de las amenazas externas. TL-WR841N ofrece encriptación WPA/WPA2 (personal y empresas) que son creados por el grupo de la industria Wi-Fi Alliance, la promoción de interpretaciones y la seguridad de WLAN.

Figura No. 37: Router Wireless

Las características principales de este router se indican a continuación y resaltan las prestaciones que nos brinda para facilitar la transmisión de datos de los equipos conectados a red.

- Velocidad inalámbrica de hasta 300 Mbps es ideal para el consumo de ancho de banda y aplicaciones sensibles.
- 2T2R MIMO ™ proporciona un mayor rendimiento en la gama convencional versus 1T1R
- Configurar fácilmente una conexión segura WPA encriptado al presionar un botón de QSS
- Puente WDS inalámbrico ofrece una interconexión para ampliar su red inalámbrica
- La función QoS asegura la calidad de VoIP y difusión de multimedia.
- Es compatible con servidor virtual, aplicaciones especiales y DMZ host ideal para la creación de un sitio web dentro de su LAN
- Ofrece la función automática de correo de registro del sistema, adecuado para gestionar el router.
- Compatible con los productos 802.11b / g.
- Antenas desmontables externas permiten una mejor alineación y fuerte mejoras antena
- Elegante exterior, se puede colocar en una pared o en posición horizontal sobre una mesa o escritorio

Las especificaciones técnicas que han determinado la selección de del router se presentan en la siguiente tabla.

Tabla No.19: Especificaciones técnicas TP Link TL-WR841N.

Interface	4 puertos LAN de 10/100Mbps 1 Puerto WAN de 10/100Mbps
Botón	Botón de WPS/ Reinicio(Reset) Botón de encendido y apagado de WiFi (On/Off) Botón de Encendido / Apagado (On/Off)
Suministro de Energía Externa	9VDC / 0.6A
Estándares Inalámbrico	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
Antena	2 antenas Fijas Omnidireccional de 5dBi
Dimensiones (Largo x Ancho x Alto)	7.6 x 5.1 x 1.3 in.(192 x 130 x 33 mm)
Frecuencia	2.4-2.4835GHz
Velocidad de Señal	11n: Hasta 300Mbps (dinámico) 11g: hasta 54Mbps (dinámico) 11b: hasta 11Mbps (dinámico)
EIRP	<20dBm(EIRP)
Sensibilidad de Recepción	270M: -68dBm@10% PER 130M: -68dBm@10% PER 108M: -68dBm@10% PER 54M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Funciones Inalámbricas	Activar / Desactivar radio inalámbrica, WDS Bridge, WMM, estadísticas inalámbricas
Seguridad Inalámbrica	64/128/152-bit WEP / WPA / WPA2,WPA-PSK / WPA2-PSK
Inalámbrico	64/128/152-bit WEP / WPA / WPA2,WPA-PSK / WPA2-PSK
Tipo WAN	IP dinámico / IP estático / PPPoE / PPTP/L2TP/BigPond
DHCP	Servidor, cliente, lista de cliente DHCP, Reserva de dirección
Calidad de Servicio	WMM, Control de Ancho de Banda

Anexo7

Selección del Servidor

El servidor para gestionar los diferentes programas se ha seleccionado en base a los requerimientos de cada fabricante dando como resultado una PC de las siguientes características:

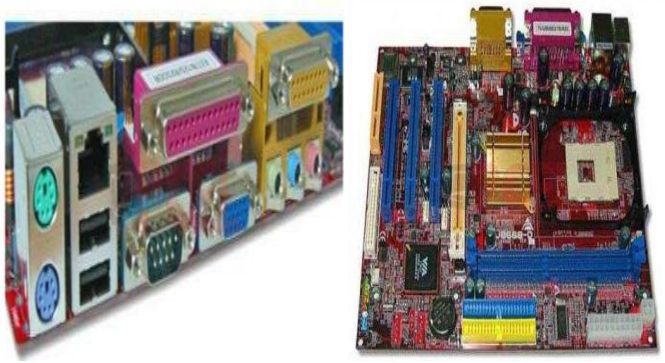


Figura No. 38: Servidor diferentes programas

Tabla No. 4: Componentes servidor

MAIN BOARD DUAL CORE (BIOCENTER) 3GB	
Procesador:	Intel® Pentium® 4
Velocidad de transferencia de Datos:	533MHz
Chipset:	VIA P4M266A / VT8237 (VT8235)
Memoria:	2 x 184-pin DDR SDRAM DIMM PC2100 DDR SDRAM Maximum 2GB
Ranuras de Expansión:	3 x PCI, 1 x AGP, 1 x CNR, 1 x PS/2 mouse, 1 x PS/2 keyboard 2 x Rear USB 2.0 ,2 x Front USB 2.0 Header(For 4 USB 2.0 Ports), 1 x VGA 1 x RJ45 port, 1 x Parallel ,1 x Serial, 1 x Lin-out/Lin-in/Mic, 1 x IrDA, 1 x Front Audio 1 x CD in, 1 x S/PDIF Out Connector, 1 x Floppy, 4 x IDE Hard Disk Devices Support Ultra DMA 66/100/133 Bus Master Modes, 1 x Chassis Intrusion Connetcor 1 x WOL Connector.
Video:	S3 ProSavage 8 up to 32MB shared video memory
Funciones de monitoreo de Hardware:	CPU/Sistema Fan Rápido, CPU Temperatura
Voltaje del Sistema:	Vcore,+3.3V,+5V,+12V
Dimensiones:	24.4cm x 19.5cm (W x L)

Anexo 8

Fuentes de voltaje

Las fuentes de voltaje DC que se han utilizado para polarizar los diferentes módulos y lectoras se indican a continuación con sus características técnicas:

Figura No. 39: Fuentes de 12 V dc

Tabla No. 5: Fuente de alimentación (DIGIKEY)

Fuente de Alimentación:	10-24VDC
Amperaje:	3,5 A
Voltaje de Entrada:	100-120V
Intensidad de Salida (trabajo):	5 Amp
Intensidad de Salida (pico):	7,5 Amp

Anexo 9

Baterías

Batería Risttone con gel libre de mantenimiento Universal, posee autonomía sin energía con carga plena de 72 horas totalmente recargable.

Figura 24 Bateria Risttone

Fuente: catálogo de productos comerciales Risttone.

Anexo 10

Cerraduras.

La cerradura eléctrica utilizada es marca eboxlock, modelo: SD873

Figura 25 cerradura eléctrica para looker

Fuente: Catálogo de productos comerciales Made In China

Contiene un embalaje de 145mmx80mmx70mm fabricada en China ideal para para cabinas y armarios de acero ya que su montaje permite un bloqueo eléctrico compatible con el sistema de Acceso Soyal , permite también la invalidación mecánica para la emergencia abierta en caso de cortes de fluido eléctrico ya que permite realizar conectar la cerradura de modo normalmente cerrado o abierto.

Tabla No. 22 de especificaciones técnicas eboxlock, modelo: SD873

Voltaje de la operación	12/24VDC el ±10% intermitente
Consumo de energía	C.C. 12V 1500mA
Modo de operación	Fall bloqueado
Resistencia	150KG
Temperatura de trabajo	~ +60ºC de -20ºC
Dimensiones LxWxH	72mm*56mm*13.8m m
Peso bruto	250g
Clase de la protección	IP20

Anexo 11

Cámara de video.

La cámara de red DCS-932L Wireless permite realizar una perfecta de vigilancia 24 horas ya que dispone de un sistema de leds infrarojo para captar imágenes en la noche, posee de un aplicativo de control comercial gratuito mydlink que permite visualizar desde un celular o computador con acceso a internet las 24 horas del día, los 7 días de la semana.

Características técnicas

- Antena inalámbrica integrada
- Tamaño compacto
- LEDs infrarrojos para visión nocturna (hasta 5 m)
- Tecnología Wireless N
- Sensor CMOS de 1,0 lux para condiciones de poca luz
- Avisos por correo electrónico al detectar movimiento
- Micrófono integrado
- Soporte de DNS dinámico para acceder fácilmente a la cámara desde cualquier punto de internet

Este tipo de cámara no necesita conectarse a un ordenador y transmite vídeo y audio de para la vigilancia remota en la más completa oscuridad ya que dispone de LEDs infrarrojos, su configuración no es compleja, la distancia de iluminación es de 5 metros perfecta para el uso del presente desarrollo ya que el contacto de los usuarios con la caja de seguridad es de muy corto alcance menor a 1 metro de distancia.

Figura 25. Cámara de video D-LINK IP WiFi-N mydlink DCS-932L
Fuente: Catalogo comercial D-Link