ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE MECÁNICA
ESCUELA DE INGENIERÍA INDUSTRIAL

"IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD Y CONTROL DE ASISTENCIA BIOMÉTRICO PARA EL LABORATORIO DE AUTOMATIZACIÓN DE PROCESOS INDUSTRIALES EN LA ESCUELA DE INGENIERÍA INDUSTRIAL-ESPOCH"

HURTADO CRIOLLO PAÚL MAURICIO
ORDOÑEZ VALAREZO EDINSON DANILO

TESIS DE GRADO

Previa a la obtención del Título de:

INGENIERO INDUSTRIAL

RIOBAMBA – ECUADOR
2016

ESPOCH

Facultad de Mecánica

CERTIFICADO DE APROBACIÓN DE LA TESIS

2014-02-03

Yo recomiendo que la Tesis preparada por:

HURTADO CRIOLLO PAÚL MAURICIO
ORDOÑEZ VALAREZO EDINSON DANILO

Titulada:

"IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD Y CONTROL DE ASISTENCIA BIOMÉTRICO PARA EL LABORATORIO DE AUTOMATIZACIÓN DE PROCESOS INDUSTRIALES EN LA ESCUELA DE INGENIERÍA INDUSTRIAL-ESPOCH"

Sea aceptada como parcial complementación de los requerimientos para el Título de:

INGENIERO INDUSTRIAL

Ing. Marco Santillán Gallegos
DECANO FAC. DE MECÁNICA

Nosotros coincidimos con esta recomendación:

Ing. Jhonny Orozco Ramos
DIRECTOR

Ing. Eduardo García Cabezas
ASESOR

ESPOCH

Facultad de Mecánica

CERTIFICADO DE EXAMINACIÓN DE TESIS

NOMBRE DEL ESTUDIANTE: HURTADO CRIOLLO PAÚL MAURICIO

TÍTULO DE LA TESIS: "IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD Y CONTROL DE ASISTENCIA BIOMÉTRICO PARA EL LABORATORIO DE AUTOMATIZACIÓN DE PROCESOS INDUSTRIALES EN LA ESCUELA DE INGENIERÍA INDUSTRIAL-ESPOCH"

Fecha de Examinación: 2016-06-08

RESULTADO DE LA EXAMINACIÓN:

COMITÉ DE EXAMINACIÓN	APRUEBA	NO APRUEBA	FIRMA
Ing. Ángel Guamán Mendoza P**RESIDENTE TRIB. DEFENSA**			
Ing. Jhonny Orozco Ramos **DIRECTOR**			
Ing. Eduardo García Cabezas **ASESOR**			

* Más que un voto de no aprobación es razón suficiente para la falla total.

RECOMENDACIONES:

El Presidente del Tribunal certifica que las condiciones de la defensa se han cumplido.

Ing. Ángel Guamán Mendoza
PRESIDENTE TRIB. DEFENSA

ESPOCH

Facultad de Mecánica

CERTIFICADO DE EXAMINACIÓN DE TESIS

NOMBRE DEL ESTUDIANTE: ORDOÑEZ VALAREZO EDINSON DANILO

TÍTULO DE LA TESIS: "IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD Y CONTROL DE ASISTENCIA BIOMÉTRICO PARA EL LABORATORIO DE AUTOMATIZACIÓN DE PROCESOS INDUSTRIALES EN LA ESCUELA DE INGENIERÍA INDUSTRIAL-ESPOCH"

Fecha de Examinación: 2016-06-08

RESULTADO DE LA EXAMINACIÓN:

COMITÉ DE EXAMINACIÓN	APRUEBA	NO APRUEBA	FIRMA
Ing. Ángel Guamán Mendoza P**RESIDENTE TRIB. DEFENSA**			
Ing. Jhonny Orozco Ramos **DIRECTOR**			
Ing. Eduardo García Cabezas **ASESOR**			

* Más que un voto de no aprobación es razón suficiente para la falla total.

RECOMENDACIONES:

El Presidente del Tribunal certifica que las condiciones de la defensa se han cumplido.

Ing. Ángel Guamán Mendoza
PRESIDENTE TRIB. DEFENSA

DERECHOS DE AUTORÍA

El trabajo de grado que presentamos, es original y basado en el proceso de investigación y/o adaptación tecnológica establecido en la Facultad de Mecánica de la Escuela Superior Politécnica de Chimborazo. En tal virtud, los fundamentos teóricos–científicos y los resultados son exclusiva responsabilidad de los autores. El patrimonio intelectual le pertenece a la Escuela Superior Politécnica de Chimborazo.

Hurtado Criollo Paul Mauricio

Ordoñez Valarezo Edinson Danilo

DECLARACION DE AUTENTICIDAD

Nosotros, Hurtado Criollo Paul Mauricio y Ordoñez Valarezo Edinson Danilo**,** declaramos que el presente trabajo de grado es de nuestra autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autores, asumimos la responsabilidad legal y académica de los contenidos de este trabajo de titulación.

Hurtado Criollo Paul Mauricio	**Ordoñez Valarezo Edinson Danilo**
Cédula de Identidad: 180402233-1	Cédula de Identidad: 070585720-9

DEDICATORIA

El presente trabajo se lo dedico a mis padres Mario Hurtado y Elvia Criollo; con su ayuda, paciencia y amor me ayudan en mi camino; a mis tías, tíos; a mi hermana, yo no soy tu ejemplo, tu eres el mío; a toda mi familia, y a mis queridos abuelitos José (+), Carmen, Gabriel (+), Zoila (+).

Paul Mauricio Hurtado Criollo

Dedico este trabajo a mis padres George Ordoñez y Julia Valarezo, ya que con su apoyo y esfuerzo me han ayudado a cumplir con una de mis metas, sabiendo formarme con buenos valores y hábitos los que ayudaron a seguir adelante.

A mi hermana Angelica Ordoñez por brindarme su confianza y apoyo que sirvieron de ejemplo de superación.

A mi familia en general, por brindarme su apoyo incondicional y compartir conmigo buenos y malos momentos, para lograr superarme.

Edinson Danilo Ordoñez Valarezo

AGRADECIMIENTO

A Dios por mi existencia, a San Isidro Labrador y a mi querida familia que han hecho muchos sacrificios para que yo pueda lograr este trascendental logro en mi vida; papá, mamá, hermana, tíos, tías, primos, primas, abuelitos (+), abuelita, y todos quienes alguna vez me brindaron su apoyo, su consejo, su amistad.

De manera efusiva agradezco a la Escuela Superior Politécnica de Chimborazo, Escuela de Ingeniería Industrial, el personal docente, administrativo de tan distinguida institución. Al Ing. Jhonny Orozco, Ing Eduardo García; director y asesor del presente trabajo respectivamente. ¡ GRACIAS !

Paul Mauricio Hurtado Criollo

Agradezco a Dios por darme la fuerza para lograr mis metas, a mi querida familia por brindarme todo el cariño y confianza para poder ver cumplida una meta más de mi vida.

El más sincero agradecimiento a la Escuela Superior Politécnica de Chimborazo, en especial a la Escuela de Ingeniería Industrial, por brindarme la oportunidad de obtener una profesión y ser personas útiles a la sociedad.

Agradezco al Ing. Jhonny Orozco e Ing. Eduardo García, por brindarme su amistad y asesoramiento en la tesis, quienes con la ayuda de su conocimiento y experiencia se logró elaborar el presente documento.

Edinson Danilo Ordoñez Valarezo

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ABREVIACIONES

TI	Tecnologías de la información
TIC	Tecnologías de la información y comunicación
PL	Línea eléctrica (Power Line)
CEBus	Bus Consumidor Electrónico
EIAJ	Asociación de Industrias Electrónicas de Japón (Electronic Industries Association of Japan)
OCR	Reconocimiento Óptico de Caracteres (Optical Caracter Recongnition)
ADN	Ácido Desoxirribonucleico
NIST	Normas del Instituto Nacional de Tecnología (National Institute Standards and Technology)
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers)
AFIS	Sistema Automático de Identificación Dactilar (Automatic Fingerprint Identification System)
JPEG	Grupo Conjunto de Expertos en Fotografía (Joint Photographic Experts Group)
CCTV	Circuito Cerrado de Television
NTSC	Comisión Nacional de Sistemas de Televisión (National Television System Committee)
PAL	Línea Alternada en Fase (Phase Alternating Line)
DVR	Grabador de Vídeo Digital (Digital Video Recorder)
NVR	Grabador de Vídeo en Red (network video recorder)
POE	Alimentación Eléctrica a Través de Ethernet (Power Over Ethernet)
DSP	Procesador Digital de Señal
PTZ	(Pan / Tilt / Zoom)
CMOS	Semiconductor Complementario de Oxido Metálico (Complementary Metal Oxide Semiconductor)
CCD	Dispositivo con carga acoplada (Charge Coupled Device)
TVL	Líneas de Resolución
BLC	La Compensación de Contraluz (Back light compensation)
STP	Cable de par trenzado protegido (Shielded twisted pair)
UTP	Cable de par trenzado no protegido (Unshielded Twisted Pair)
LAN	Red de Área Local (Local Area Network)
FTP	Con pantalla global También llamado FUTP
BNC	Bayoneta, Neill-Concelman (Bayonet Neill-Concelman)
ONVIF	Foro Abierto de Interfaz de Red de Vídeo (Open Network Video Interface Forum)
UPS	Sistema de Alimentación Ininterrumpida (Uninterruptible Power Supply)
IP	Protocolo de Internet (Internet Protocol)

LISTA DE ANEXOS

RESUMEN

La implementación del sistema de seguridad y control de acceso biométrico para el laboratorio Automatización de Procesos Industriales en la Escuela de Ingeniería Industrial – ESPOCH, con el objeto de resguardar los bienes y precautelar la integridad de las personas al interior del laboratorio.

Se determinó que los elementos electrónicos, eléctricos, electro-magnéticos, mecánicos que se utilizan al instalar el sistema, se elabora un análisis de los dispositivos a seleccionar para su posterior adquisición. El conjunto consta de un dispositivo de acceso biométrico que permite el ingreso de los usuarios autorizados, (un cerrojo eletro-mecanico, cerrojo electro-magnetico), dos cámaras IP provistas de sistema de imágenes infrarrojo, un dispositivo NVR (Net Video Recording), pulsador de salida, unidad UPS (Unit Power Supply) y una puerta metálica.

Se instaló un UPS que permite la distribución de energía uniformemente a todos los dispositivos; conexionar los cables de datos desde las cámaras al router y por ultimo al NVR, logrando la comunicación entre los dispositivos; los cerrojos se instaló en la puerta teniendo en cuenta la conexión en paralelo y el pulsador de salida para la apertura de la puerta desde el interior del establecimiento, las pruebas se realizan coordinando los ciclos de acceso, registro de personal y video-grabacion de las actividades.

Al automatizar la vigilancia y el control de accesos, disminuye los conflictos psicológicos que a veces presenta el ser humano; se optimiza los periodos de guardianía y finalmente se resguarda de mejor manera los materiales, herramientas, enseres, maquinas didácticas pertenecientes al sistema.

ABSTRACT

The implementation of a security system and biometric access control for the Automation of Processes Laboratory in the School of Industrial Engineering – ESPOCH was carried out with the objective of protecting property and safeguard the integrity of persons within the laboratory.

An analysis was carried out to determine the appropriate electronic, electrical, electro-magnetic elements and mechanical devices to install in the system and these were subsequently acquired. The set consists of a biometric access device which permits the entry of authorized users (an electro-mechanical lock and an electro-magnetic lock), two IP cameras equipped with infrared imaging systems, an NVR device (Net Video Recording) an exit button, UPS unit (Unit Power Supply) and a metal door.

A UPS unit was installed which allows energy to be distributed evenly to all installed devices; data cables were connected from the cameras to the router and finally the NVR, creating integrated communication between security devices; the locks were installed on the door taking into account the parallel connection and exit button for opening the door from inside the establishment, tests were carried out coordinating access cycles, the personnel record and video-recording of activities.

By automating security monitoring and access control, the psychological conflicts that the human condition sometimes presents are reduced; optimizing the surveillance and better protecting the materials, tools, equipment and teaching machines belonging to the laboratory.

CAPÍTULO I

1. INTRODUCCIÓN

1.1 Antecedentes

En un mundo globalizado, con el desarrollo creciente de la tecnología los procesos de automatización se manifiestan en mayor actividad. Cada día se utiliza nueva y mejorada ciencia con la finalidad de agilizar nuestras labores cotidianas. En el caso de las industrias estos avances permiten producir a mayor velocidad y con más precisión.

La tecnología está al servicio de la humanidad, actualmente existen sistemas capaces de automatizar la vivienda, los edificios, los lugares de trabajo; y de reconocer a los usuarios previamente programados para el acceso al recinto.

A lo largo del tiempo la seguridad de los bienes ha sido una gran interrogante; vigilar continuamente necesitaba de personal específico para la tarea. De la misma forma conocer quienes visitan las instalaciones y llevar un registro de accesos, fue un proceso específicamente manual.

Actualmente varios edificios e instalaciones gubernamentales, públicos y privados, cuentan con esta tecnología; los mencionados dispositivos se usan para monitoreo-control de sus empleados, video vigilancia de los bienes, resguardo y seguridad de las personas.

La Escuela Superior Politécnica de Chimborazo, Escuela de Ingeniería Industrial; no posee en su infraestructura, dispositivos biométricos destinados para el control del acceso de los estudiantes, la vigilancia externa está a cargo de la guardianía y al interior del Laboratorio de Automatización no se custodian los bienes.

Se tiene acceso al aula de prácticas solo cuando el profesor o el conserje pueden disponer de ella; la instalación de los mencionados dispositivos permite al acceso de las personas autorizadas (profesores, estudiantes, tutores, ayudantes de cátedra propende a la mejor comprensión de la enseñanza a través de la práctica en el laboratorio.

1.2 Justificación

Los conocimientos se afianzan mejor si podemos poner en práctica lo aprendido. Partiendo de esta premisa se analizó la posibilidad de tener mayor acceso a los laboratorios de prácticas sin la necesidad de que el encargado del laboratorio se halle en las cercanías del lugar.

El comportamiento humano, la disponibilidad de las instalaciones, la ausencia de control, monitoreo y vigilancia a toda hora ponen en riesgo las pertenecías institucionales

La presente tesis nace de la necesidad de resguardar las instalaciones del Laboratorio de Automatización de Procesos de la Escuela de Ingeniería Industrial perteneciente a la Escuela Superior Politécnica de Chimborazo; además de controlar, monitorear, y vigilar el ingreso; junto con el uso que se dé por parte de las personas que ingresan a la misma.

La implementación permitirá visualizar de manera práctica la aplicación de la automatización (considerando a la domótica y la biometría); motivando el aprendizaje.

Dado que la Escuela de Ingeniería Industrial no dispone de un sistema de seguridad biométrica para el laboratorio de Automatización de Procesos, resulta conveniente que, por medio de trabajos de investigación y aporte de los estudiantes, adquirir e instalar estos equipos para salvaguardar los módulos de aprendizaje que se encuentran dentro del laboratorio, los mismos servirán para el desarrollo de la Escuela.

La tecnología biométrica en sus inicios representaba costos elevados para su adquisición, pero a medida que ha avanzado la ciencia estos precios se han flexibilizado. Tal es el caso que los ingresos generados por ésta industrian representan 8152 millones de dólares para el año 2016y el dispositivo mayormente utilizado es el biométrico de huellas dactilares.

En términos económicos se visibiliza la rentabilidad de este tipo de sistemas, la automatización de la seguridad, monitoreo y control, reduce el aspecto de falla por parte del ser humano en los aspectos psicológico y físico, por lo tanto, el servicio requerido por parte del usuario se hace eficiente.

1.3 Objetivos

1.3.1 *Objetivo general.* Implementar el sistema de seguridad y control de asistencia biométrico para el Laboratorio de Automatización de Procesos en la Escuela de Ingeniería Industrial-ESPOCH.

1.3.2 *Objetivos específicos:*

- Implementar el sistema biométrico que permita el acceso de personas autorizadas al laboratorio de Automatización de Procesos.

- Determinar la secuencia de programación correcta para el acceso hacia el laboratorio.

- Elaborar las guías de manejo y mantenimiento del sistema biométrico.

CAPÍTULO II

2. MARCO TEORICO

2.1 Domótica

La Domótica es una disciplina técnica que introduce infotecnología (Tecnologías de la Información y Comunicación TIC) en los hogares; para mejorar la calidad de vida de sus habitantes y ampliar las posibilidades de comunicación, gestión energética, seguridad, bienestar; automatizando los procesos domésticos e intercomunicando (por medio de redes interiores y exteriores, cableadas o inalámbricas) dichos procesos con los residentes del hogar y con el exterior (DOMINGUEZ, y otros, 2006).

2.1.1 *La Domótica como solución futura.* En lo que a tecnología se refiere en los últimos años se están produciendo algunos cambios muy significativos e interesantes; estas modificaciones afectan sobre todo a los lugares en los que residimos, pero también a aquellos en los que trabajamos o pasamos nuestros ratos de ocio.

La tecnología aplicada al hogar conocida como Domótica; integra automatización, informática y nuevas tecnologías de comunicación; todas ellas dirigidas a mejorar la comodidad, seguridad, y el bienestar del usuario.

Por estas razones se precisa que los constructores, proyectistas, arquitectos y demás involucrados, adquieran una rápida familiarización con las posibilidades de los nuevos dispositivos y su conocimiento, que les proporcione la capacidad suficiente para incorporarlos a sus productos y servicios; incrementando así su competitividad en el mercado (DOMINGUEZ, y otros, 2006).

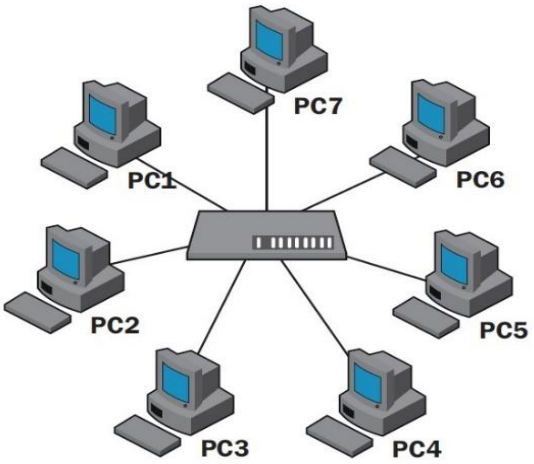
2.1.2 *Topología de las redes.* Los diversos componentes de las redes de datos poseen distintas formas de interconectarse, cada una con sus propias características; existen cuatro tipos de redes, como se describirán a continuación.

2.1.2.1 *Red tipo estrella.* En este tipo de redes todos los componentes se conectan a una unidad central. Si un dispositivo necesita comunicarse con otro primero debe

informarlo a la unidad central, que es la que toma las decisiones y gestiona la comunicación.

Las ventajas que encontramos en este tipo de red es que se pueden agregar dispositivos fácilmente y en caso de que alguno sufra un desperfecto no afectará al resto de la red; incluso se lo puede reemplazar sin que el trabajo de la red sea interrumpido. Como aspecto negativo encontramos que si la unidad central falla, toda la red se cae. La característica principal de las redes en estrella es el nodo central de gestión por el que pasan todos los mensajes (REDOLFI, 2013).

Figura 1. Red Tipo Estrella

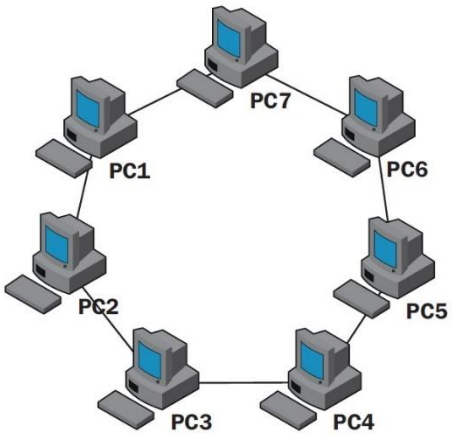


Fuente: Domótica 1ra. Ed. Redolfi Luciano

2.1.2.2 *Red tipo anillo.* En esta red de distribución comunicamos cada elemento de la red por una conexión de entrada y una de salida. Cada uno recibe el mensaje, analiza si le pertenece o no, de ser necesario lo modifica y lo transmite al siguiente. Como ventaja de esta topología podemos mencionar que todos los componentes tienen el mismo nivel de acceso y que sin importar la cantidad de usuarios, la capacidad de la red no decaerá, es una red muy fiable.

Las desventajas de esta red son que el dato o mensaje que se transmite es más largo debido a que el mismo mensaje debe destinarse “bytes” de información para identificar el origen y el destino. Además, si un dispositivo falla, toda la red se paraliza; y a medida que la red crece se ralentiza y nos es muy difícil encontrar el punto exacto en que la red falla. En las redes de anillo todos los componentes tienen el mismo nivel de jerarquía y los mensajes son analizados por todos (REDOLFI, 2013).

Figura 2. Red Tipo Anillo



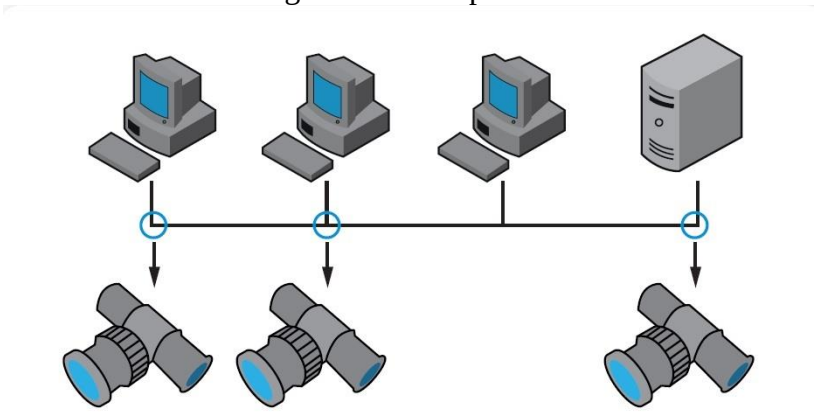
Fuente: Domótica 1ra. Ed. Redolfi Luciano

2.1.2.3 *Red tipo Bus.* Estas redes poseen una canal central de comunicación o "bus", por el que circula toda la información, y al que están conectados todos los dispositivos. Cuando un dispositivo quiere comunicarse con otro, coloca el mensaje en el bus, indicando el origen y el destino; los otros dispositivos lo leen y lo procesan si es para ellos, caso contrario lo eliminan.

Este es el tipo de red que más fácil se construye y es amplia; por otra parte, si queremos mantener una señal de calidad, nos veremos limitados en su extensión, ya que la red suele ocupar mucho espacio y no tenemos control sobre si hay un mensaje en el bus antes de enviar el nuestro, lo que ocasiona problemas.

En la topología de redes en bus, todos los componentes colocan mensajes en él y todos los leen y recogen según la necesidad (REDOLFI, 2013).

Figura 3. Red Tipo Bus



Fuente: Domótica 1ra. Ed. Redolfi Luciano

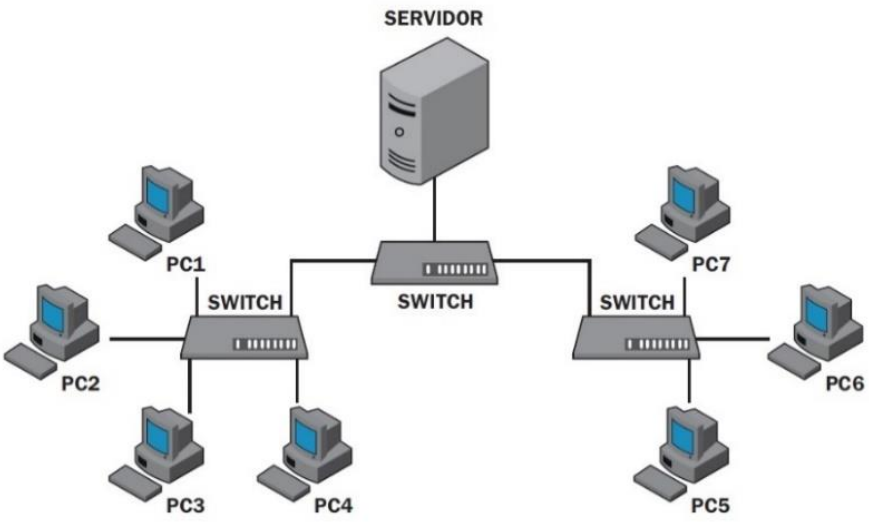
2.1.2.4 *Red Tipo Árbol.* Podemos considerarla como una red de redes estrella. Aquí no tenemos un nodo central, cada subred se comunica y gestiona localmente, y se conecta con el resto de la red mediante un punto de conexión con ella.

En cada nodo que conecta una estrella con otra encontraremos lógicas que identifican al destinatario del mensaje, para así dirigirlo a la estrella del destinatario.

Posee las ventajas de la red estrella, y además esta topología cuneta con el hecho de ser soportada por varios fabricantes.

Como desventajas podemos decir que su configuración es difícil de realizar y por consiguiente más cara. Las redes en árbol deben su nombre a que desde un punto troncal parten varias ramas, y éstas a su vez se dividen (REDOLFI, 2013).

Figura 4. Red Tipo Árbol



Fuente: Domótica 1ra. Ed. Redolfi Luciano

2.2 Biometría

2.2.1 *Concepto de Biometría.* "Biometría es el conjunto de características fisiológicas y de comportamiento que pueden ser utilizadas para verificar la identidad del individuo".

La medición biométrica se ha venido estudiando desde tiempo atrás y es considerada en la actualidad como el método ideal de identificación humana (BORJA, y otros, 2009).

2.2.2 *Biometría y seguridad.* El campo de la seguridad utiliza tres tipos distintos de autenticación:

- Algo que el usuario sabe, por ejemplo, una clave secreta.
- Algo que el usuario tiene, por ejemplo, una tarjeta de identificación o una llave.
- Algo que el usuario es, por ejemplo, un dato personal biométrico (GARCÍA, 2009).

2.2.3 *Tipos de Biometría.* En función de las características que se usan en la identificación se distinguen dos áreas:

2.2.3.1 *Biometría estática*. Es el estudio de las características físicas del ser humano a la cual pertenecen las siguientes características:

- *Huella dactilar*. El uso de huellas dactilares es uno de los métodos más antiguos y más usados en la actualidad. La huella dactilar constituye una de las características humanas más singulares, no existen dos personas con las mismas huellas dactilares (incluyendo a gemelos idénticos). La medición automatizada de la huella dactilar requiere un gran poder de procesamiento y alta capacidad de almacenamiento, por esto los sistemas biométricos de huella dactilar se basan en rasgos parciales. Los sistemas biométricos de huella dactilar son considerados seguros, fáciles de usar y económicos.

- *Reconocimiento del iris.* El iris es la parte pigmentada del ojo que rodea la pupila. Este método utiliza las características del iris humano con el fin de verificar la identidad de un individuo. Los patrones de iris vienen marcados desde el nacimiento y rara vez cambian. Son extremadamente complejos, contienen una gran cantidad de información y tienen más de doscientas propiedades únicas. El escaneado de iris se lleva a cabo mediante una cámara de infrarrojos especializada (situada por lo general muy cerca de la persona) que ilumina el ojo realizando una fotografía de alta resolución. Este proceso dura sólo uno o dos segundos y proporciona los detalles del iris. Es importante señalar que no existe ningún riesgo para la salud, ya que, al obtenerse la muestra mediante una cámara de infrarrojos, no hay peligro de que el ojo resulte dañado en el proceso (PÉREZ, y otros, 2011).

- *Reconocimiento de retina.* El escáner biométrico de la retina se basa en la utilización del patrón de los vasos sanguíneos. El hecho de que cada patrón sea único (incluso en gemelos idénticos, al ser independiente de factores genéticos) y que se mantenga invariable a lo largo del tiempo, la convierten en una técnica idónea para entornos de alta seguridad (PÉREZ, y otros, 2011).

- *Reconocimiento de la geometría de las venas.* Esta tecnología se basa en la estructura de las venas de la mano o del dedo. De forma similar al iris o a la retina, la geometría de las venas se define antes del nacimiento y es diferente incluso en gemelos idénticos.

  En el proceso de captura de la muestra, el sensor infrarrojo obtiene una imagen del patrón de las venas, a partir del cual se genera una plantilla biométrica. Adicionalmente, al tratarse de un órgano interno, resulta más complejo realizar cualquier variación sobre el mismo (PÉREZ, y otros, 2011).

- *Reconocimiento de la geometría de la mano.* Esta tecnología utiliza la forma de la mano para confirmar la identidad del individuo. Su aceptación por parte de los usuarios es muy elevada, ya que no requiere información detallada de los individuos. Para la captura de la muestra, se debe colocar la mano sobre la superficie de un lector (PÉREZ, y otros, 2011).

- *Reconocimiento facial.* El reconocimiento facial es una técnica mediante la cual se reconoce a una persona a partir de su cara. Para ello, se utilizan programas de cálculo que analizan imágenes de rostros humanos. El proceso de registro dura entre veinte y treinta segundos, tiempo en el cual se toman varias fotografías de la cara. Idealmente, la serie de imágenes debería incluir diferentes ángulos y expresiones faciales, para permitir una búsqueda de coincidencias más precisa (PÉREZ, y otros, 2011).

- *Reconocimiento espectroscópico de la piel.* Se toma una imagen de la superficie de la piel. Esta imagen se clasifica usando el algoritmo de análisis de la textura de la superficie de la piel que tiene en cuenta una serie de características aleatorias y genera una plantilla (PÉREZ, y otros, 2011).

- *Reconocimiento del A.D.N. (acido desoxirribonucleico).* Se toma una muestra de tejido de un individuo para la extracción del A.D.N. (Ácido Desoxirribonucleico) del núcleo de una célula. Esta técnica resulta adecuada para el uso forense, pero no para la identificación en tiempo real debido a la complejidad del proceso y al tiempo necesario para extraer una huella genética a partir de una muestra de tejido (PÉREZ, y otros, 2011).

2.2.3.2 *Biometría dinámica.* Estudia las características de la conducta del ser humano a las cual pertenecen las siguientes características:

- *Reconocimiento de la dinámica del tecleo.* Esta técnica se basa en la existencia de un patrón de escritura en teclado que es permanente y propio de cada individuo. De este modo, se mide la fuerza de tecleo, la duración de la pulsación y el periodo de tiempo que pasa entre que se presiona una tecla y otra. La principal ventaja de esta técnica es que la inversión necesaria en sensores es prácticamente nula, ya que los teclados de ordenador están presentes en múltiples aspectos de nuestra vida cotidiana; y además están altamente aceptados por la población que hace uso de ellos a diario. De este modo los costos de implantación se centrarían en el software (PÉREZ, y otros, 2011).

- *Reconocimiento de firma.* Esta técnica analiza la firma manuscrita para confirmar la identidad del usuario. Cabe la posibilidad de que existan ligeras variaciones en la firma de una persona, pero la consistencia creada por el movimiento natural y la práctica a lo largo del tiempo crea un patrón reconocible que hace que pueda usarse para la identificación biométrica (PÉREZ, y otros, 2011).

- *Reconocimiento de voz.* Junto con el reconocimiento facial, el reconocimiento locutor es un método natural de identificación. Es un proceso realizado a diario por los individuos para reconocer a un conocido en una llamada telefónica o al oír una voz. Estas aplicaciones usan redes neuronales para aprender a identificar voces. Los algoritmos deben medir y estimar la similitud para devolver un resultado o una lista de posibles candidatos. La autenticación se complica debido a factores como el ruido de fondo, la calidad de la muestra y su duración, por lo que siempre es necesario considerar un margen de error (PÉREZ, y otros, 2011).

- *Reconocimiento de la cadencia del paso (forma de andar***).** Este método se basa en la forma de caminar de una persona, este acto se graba y se somete a un proceso analítico que genera una plantilla biométrica derivada de dicho comportamiento. El dispositivo de captura es una cámara, y el sistema permite el emparejamiento de los datos mediante el uso del software con su respectivo algoritmo; permitiendo la identificación a distancia (PÉREZ, y otros, 2011).

2.2.4 *Elección del rasgo biométrico adecuado*. La elección de un rasgo biométrico para una aplicación no se basa solamente en su posible capacidad discriminativa. A la hora de elegir, concurren muchos factores adicionales como el coste, el nivel de seguridad requerido, el tiempo de respuesta necesario, entre otros.

2.2.5 *Valoración comparativa de las distintas técnicas biométricas.* El objetivo de usar características biométricas es poseer un conjunto de herramientas que permitan obtener la identificación y verificación de la identidad de una persona.

Tabla 1. Cuadro comparativo de las propiedades de diferentes técnicas biométricas.

	Grado de aceptación	Resistencia al fraude	Medible	Rendimiento	Permanencia	Singularidad	Universalidad
Huella dactilar	M	A	M	A	A	A	M
Reconocimiento facial	A	B	A	B	M	B	A
Reconocimiento del iris	B	A	M	A	A	A	A
Geometría de la mano	M	M	A	M	M	M	M
Reconocimiento de retina	B	A	B	A	A	A	A
Geometría de las venas de la mano	M	A	M	M	M	M	M
Reconocimiento de voz	A	B	M	B	B	B	M
Reconocimiento de firma	A	B	A	B	B	B	B
Reconocimiento de escritura de teclado	M	M	M	B	B	B	B
Forma, modo de caminar, andar	A	M	A	B	B	B	M
ADN	B	B	B	A	A	A	A
Termograma facial	A	B	A	M	B	A	A
Nomenclatura: A: Alto, M: Medio, B: Bajo.							

Fuente: Estudio sobre las tecnologías biométricas aplicadas a la seguridad

2.3 Papiloscopia

Es la ciencia que estudia la morfología papilar con fines de identificación personal. Esta morfología se presenta con iguales características en: yema de los dedos, palma de las manos y planta de los pies.

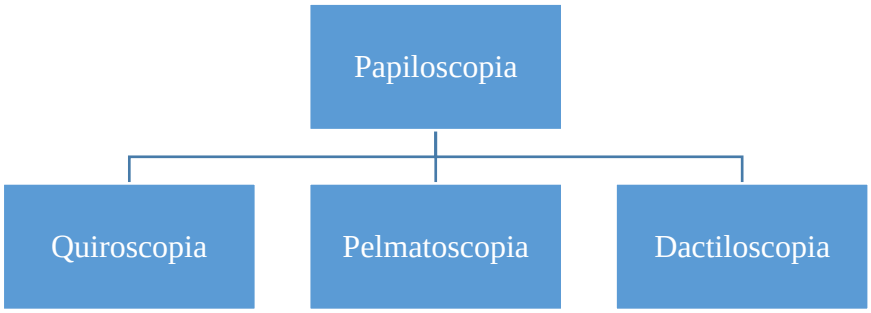
2.3.1 *Identidad humana.* Es el conjunto de caracteres físicos que individualizan a una persona, haciéndola distinta de todas las demás. Si aplicamos este concepto, "identificar" será comprobar si una persona es la misma que se supone o se busca (GARCÍA, 2009).

En nuestras relaciones diarias, basta generalmente con el propio testimonio del interesado para que lo consideremos como la persona que dice ser, el recuerdo que conservamos de su aspecto general, sus rasgos fisonómicos y su voz nos permitirá identificarlo en adelante. Pero hay ocasiones en que se sabe o sospecha que un determinado individuo, no puede (incapaz) o no quiere (delincuente) identificarse por sí mismo.

Para lograr su identificación será necesario entonces comparar una o varias de sus características actuales con otras debidamente fichadas que le correspondieron anteriormente (GARCÍA, y otros, 2008).

2.3.2 *Clasificación de la papiloscopia.* La papailoscopia se clasifica en:

Figura 5. Clasificación Papiloscopia



Fuente: Pailoscopia. Crnl. Torres Casimiro Rolando

Se divide en las disciplinas que estudian otras áreas morfológicas:

2.3.2.1 *Quiroscopia:* Es la parte de la papiloscopia, que estudia los dibujos de las crestas papilares de la palma de las manos, con fines de identificación personal, estos dibujos son denominados quirogramas (TORRES CASIMIRO, 2013).

2.3.2.2 *Pelmatoscopia:* Es la parte de la papiloscopía que estudia los dibujos de las crestas papilares de la planta de los pies, con fines de identificación personal, estos dibujos son denominados pelmatogramas (TORRES CASIMIRO, 2013).

2.3.2.3 *Dactiloscopia:* Es la parte de la papiloscopía que estudia los dibujos formados por las crestas papilares en la yema de los dedos con fines de identificación personal, estos dibujos son conocidos como dactilogramas.

2.3.2 *Origen del vocablo dactiloscopia.* La palabra dactiloscopia se deriva de dos voces griegas “daktilos” (dedo) y “skopen” (examen-examinador).

2.3.3 *Principios de la dactiloscopia.* La dactiloscopia propone la identificación de la persona, por medio de las impresiones producidas por las crestas papilares que se encuentran en las yemas de los dedos de las manos.

2.3.3.1 *Perennidad:* Porque las crestas del dibujo dactilar se forman desde el tercer mes de vida intrauterina, participan en el crecimiento de la persona y continúan hasta ciertos procesos avanzados de putrefacción (algunos han resistido al transcurso del tiempo gracias a los procesos de momificación).

2.3.3.2 *Inmutabilidad:* Porque no cambian. Si se toman la impresión de todos los dedos a tomarla en su vejez, observaremos que los dibujos dactilares participan del crecimiento general del individuo, pero sin variar en sus características que los individualizan. Excepto cuando se producen alguna lesión profunda que dejen cicatriz, y ésta pasa a ser considerada como otra característica identificativa.

2.3.3.3 *Diversidad de características.* Son diversiformes, por el sinnúmero de dibujos que adquieren las crestas papilares y por los puntos característicos que se distribuyen. Hasta el momento no se han encontrado dos sujetos con la misma huella

dactilar, se incluyen los gemelos monocigóticos (es decir que proceden del mismo óvulo y por tanto presentan la misma información genética) y los clones (a pesar de que comparten el mismo ADN).

2.3.3.4 *Los dedos del homo sapiens.* Cada uno tiene tres falanges, excepto el pulgar que sólo tiene dos, son órganos esenciales de la aprehensión y del tacto.

En los casos normales son cinco: pulgar, índice o indicador, medio, anular y meñique.

Todos estos dedos están constituidos bajo un mismo tipo excepto el pulgar que presenta algunas particularidades anatómicas. Cada dedo está formado por tres columnas óseas llamadas falanges y que son sucesivamente decrecientes.

- *Las falanges se cuentan desde el borde inferior de la mano hacia la extremidad libre.* La falange donde está la uña es la tercera. También pueden llamarse falange, falangina y falangeta, en lugar de primera, segunda y tercera. Al pulgar le falta la segunda falange o falangina.

- *El volumen de los dedos, así como su longitud varía en cada uno de ellos.* El pulgar es el más grueso, el auricular es el más delgado; el del medio, llamado también cordial o del corazón, es el más largo. Este orden longitudinal decreciente resulta muy ventajoso para el examen de las impresiones planas, lo que nos sirve para comprobar si ha habido fraude. Tienen, como las manos, dos caras: una palmar o anterior y otra dorsal o posterior.

- *Los dedos presentan tres eminencias separadas por depresiones.* Las depresiones están situadas entre las eminencias y señalan las articulaciones o sean las uniones de las falanges que conocemos vulgarmente con el nombre de coyunturas. Las llaman superior o dígito palmar, media e inferior. Las eminencias son los cuerpos de las falanges.

  El pliegue superior o dígito-palmar es el límite de la palma de la mano y la cara palmar de los dedos. El inferior es el límite de la región que llamamos del dactilograma.

Figura 6. Palma de la Mano

Fuente. Google. Hand

- *Crestas papilares.* Las crestas papilares son glándulas de secreción de sudor, situadas en la dermis, llamada glándulas sudoríparas.

  Constan de un tubo situado en el tejido celular subcutáneo, formado por un glomérulo glandular con un canal rectilíneo que atraviesa la dermis, y termina en la capa córnea de la epidermis, concretamente en el poro; que es un orificio situado en los lomos de las crestas papilares.

  Una vez el sudor sale, se derrama por todas las crestas y se mezcla con la grasa natural de la piel, lo que da lugar a que cuando se toque o manipule un objeto apto para la retención de huellas, las crestas dejen una impresión en él.

Figura 7. Dedos de la Mano

Fuente: Google. Huellas dactilares

2.4 Huellas digitales

La biometría dactilar ha venido tomando cada vez mayor importancia en la identificación de personas. Esta tecnología ha madurado lo suficiente como para constituirse en una opción importante dentro de la identificación de personas, tanto en aplicaciones civiles como en forenses/policiales.

De los sistemas biométricos uno de los más populares es el reconocimiento mediante la "huella dactilar"; esta forma para identificar a las personas no es novedosa pues se aplica desde el siglo XIX; este proceso en sus inicios se lo realizaba visualmente y en la actualidad existen sistemas que lo realizan de forma automática.

Al hablar de "huella digital" nos referimos también al "rastro" dejado por las personas al momento de usar las comunicaciones digitales e internet. En el presente documento, utilizaremos el mencionado término para referirnos al proceso de adquisición de datos proporcionados por la huella humana, y posteriormente digitalizados con el fin de usarlos para su identificación.

Como concepto de huella dactilar tenemos que es la impresión visible o moldeada que produce el contacto de las crestas papilares de un dedo de la mano sobre una superficie. Es una característica individual que se utiliza como medio de identificación de las personas (LACIE, 2013).

Figura 8. Huella Dactilar, Dedo

Fuente: https://es.wikipedia.org/wiki/Huella_dactilar

2.4.1 *Huella Latente.* El vocablo latín “latens” significa oculto, escondido, que no se manifiesta exteriormente.

Por tanto, las huellas latentes son figuras invisibles que se producen al contacto sobre una superficie debido al sudor que emana por los poros sudoríparos de las papilas dactilares.

2.4.2 *Huella dactilar positiva.* Es la impresión artificial de la figura dactilar de alguno de los dedos de las manos sobre alguna superficie utilizando cualquier substancia colorante (tinta negra para huellas, grasa, aceite, sangre, etc.)

2.4.3 *Huella dactilar negativa.* Es la impresión artificial de la figura dactilar de alguno de los dedos de las manos, sobre materias blandas (plastilina, masa, yeso fresco, pintura fresca, jabón suave) y que registran su relieve.

Puntos característicos de las huellas dactilares (minucias). Se designa con ese nombre a las particularidades papilares que en detalle ofrecen las crestas en su curso por el dactilograma natural y su impresión. Es decir, son las convergencias, desviaciones, empalmes, interrupciones, fragmentos, de las crestas y de sus surcos (islote, bifurcación, punto, cortada, horquilla, empalme, encierro)

Cuando se cotejan dos huellas dactilares como mínimo se buscan doce puntos característicos, aunque la obtención de al menos ocho ya tiene validez jurídica (LACIE, 2013).

Figura 9. Minucias

Fuente: Papiloscopia. Crnl Torres Rolando

- *Bifurcación.* Es la separación o división de una línea en dos o más ramas.

- *Divergencia.* Es la separación de dos líneas que habían estado corriendo paralelas o casi paralelas.

2.4.4 *Puntos focales.* Se encuentran dentro de la zona de dibujo y reciben el nombre de Delta y Núcleo.

Figura 10. Puntos Focales

Fuente: Papiloscopia. Crnl Torres Rolando

2.4.5 *Clasificación de las huellas dactilares.* Las impresiones digitales pueden dividirse según su dibujo dactilar en tres grandes grupos: Presilla, Arco y Verticilo.

2.4.5.1 *Presilla.* Es el tipo de dibujo dactilar en que una o más crestas entran por cualquier lado de la impresión, hacen una recurva, tocan o pasan una línea imaginaria tendida desde el delta hasta el núcleo tienden a terminar hacia el mismo lado de la impresión por donde entraron.

2.4.5.2 *Arco.* Cuando las crestas papilares se extienden de uno al otro lado del dactilograma, casi en forma paralela entre sí.

2.4.5.3 *Verticilo.* Presenta dos formaciones delticas opuestas una a la derecha y otra a la izquierda, y las crestas papilares se agrupan alrededor de un núcleo; este puede adoptar la forma espiral, circunferencial sinuoso u ovoidal.

2.5 Descripción y análisis de los sistemas de seguridad

El sistema de seguridad es la interconexión de recursos, redes y dispositivos; cuyo objetivo es precautelar la integridad de las personas, los bienes y su entorno. El uso correcto de los mismos dependerá de las características y necesidades de lo que se necesite proteger, considerando el número de lugares a resguardar, junto con los potenciales riesgos que se puedan presentar.

Posee una central de monitoreo que administra los sistemas como: control de accesos, de intrusión, circuito cerrado de televisión, sistema contra incendios, entre otros; cuya finalidad es la supervisión y se realiza durante las 24 horas del día.

2.5.1 *Sistemas de control.* El sistema de control es el encargado de llevar lo que es un registro y a su permitir el acceso a un lugar restringido.

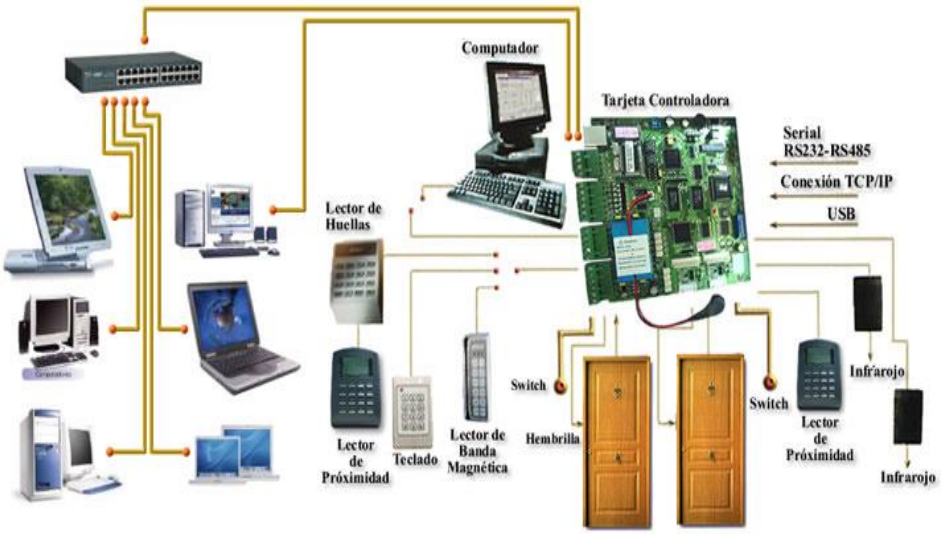
2.5.1.1 *Sistema de Control de Asistencia.* Permite controlar en forma sencilla y efectiva los tiempos de ingreso/salida de las personas registradas. El Control de Asistencia les pone fin a los retrasos, salidas temprano y regresos tardíos. "Conozca realmente el tiempo de trabajo del personal."

Habitualmente estos sistemas tienen un funcionamiento off-line y guardan un registro en memoria del histórico de accesos (con información del usuario, hora, día del acceso, etc.) y otros eventos como alarmas u otras incidencias. Este registro puede ser descargado a un PC u otro dispositivo compatible para su posterior tratamiento (KIMALDI, 2002).

2.5.1.2 *Sistema de control de acceso*. Posibilita controlar los accesos o restricciones a las diferentes áreas, sin importar la cantidad de personas que tengan ingresar a dicho lugar. Los terminales son equipos electrónicos que gestionan de manera automática la apertura segura de puertas, barreras, verjas y otro tipo de accesos tanto para la entrada de personas o vehículos. Es el control sobre "quien tiene acceso, cuándo y a dónde". Permite el ingreso sólo a personas autorizadas y en horarios autorizados a lugares que deben ser protegidos al máximo nivel (SAS, 2015).

Olvídese de los problemas de llaves, códigos, tarjetas; instale un control de acceso.

Figura 11. Sistema Control de Accesos



Fuente: http://goo.gl/Fx7RA4

2.5.2 *Componentes del sistema.* El sistema de control de acceso ha evolucionado año tras año, teniendo en la actualidad conjuntos administrables tan complejos que además de permitir o restringir el acceso de personal a las instalaciones pueden ofrecer registro de asistencia y control de personal. Para la implementación de los dispositivos, se realiza un estudio del tipo de seguridad requerido en cada zona y con la combinación de equipos existentes en el mercado; se puede brindar diferentes tipos de seguridad los cuales entres más complejos más difíciles de invadir, entre ellos tenemos:

2.5.2.1 *Sistemas biométricos.* Su funcionalidad es verificar la identidad de una persona basándose en características físicas o de su comportamiento; utilizando por ejemplo su mano, dedo de la mano, el iris de su ojo, su voz o su rostro**.**

2.5.2.2 *Cerradura electromagnética.* Su función principal es mantener bloqueada la puerta mientras no exista la orden de apertura. Consta de dos piezas: un potente electroimán que se fija en el marco de la puerta, formado por un núcleo o barra de hierro a la que se enrolla un cable barnizado de cobre creando una bobina; posee también una placa metálica que se instala sobre la puerta u objeto a controlar.

2.5.2.3 *Pulsador de salida y emergencia*. El pulsador de salida es aquel elemento que permite enviar una señal a la unidad de control, para autorizar la salida del área monitoreada; generalmente reemplaza a una lectora de salida desactivando la cerradura correspondiente sin necesidad de identificación.

2.5.3 *Sistema de circuito cerrado de televisión.* Es todo aquel sistema de televisión que no es abierto, es decir no puede verlo cualquier persona. La televisión comercial está abierta al público ya que a través del aire e incluso a través de cables (televisión por cable) se hace llegar a todo aquel que quiera observar la programación. En el caso del circuito cerrado, el video generado se conserva privado y únicamente son capaces de observarlo las personas asignadas para ello dentro de una organización. Lógicamente, en casi todos los casos el CCTV (circuito Cerrado de Televisión) tiene que estar acompañado de la grabación de los eventos que se vigila con el objeto de obtener evidencia de todos los movimientos importantes, y además el minimizar la vigilancia humana de los monitores (TECNOTRONICA, 2015).

Figura 12. Circuito Cerrado de Televisión

Fuente: http://goo.gl/29a8CY

2.5.4 *Aplicaciones para el CCTV.* Probablemente el uso más conocido del CCTV está en los sistemas de vigilancia y seguridad; en aplicaciones tales como establecimientos comerciales, bancos, oficinas gubernamentales, edificios públicos, aeropuertos, entre otros.

A continuación, se enlistan algunos ejemplos:

- Monitoreo del tráfico en un puente.
- Control de procesos industriales como Fundiciones, Panaderías.

- Ensamble manual o automático.
- Vigilancia en condiciones de absoluta oscuridad, utilizando luz infrarroja.
- Resguardo vehículos de transporte público.
- Observación de áreas claves como negocios, tiendas, hoteles, casinos.
- Estudiar el comportamiento de empleados.
- Custodia de los niños en el hogar, en la escuela, parques, guarderías.
- Seguridad de estacionamientos, incluyendo identificación de las placas.
- Vigilancia de puntos de revisión, de vehículos o de personas.
- Análisis facial para identificación de criminales en áreas públicas.

Lógicamente, en casi todos los casos el CCTV tiene que estar acompañado de la grabación de los eventos que se vigila, con el objeto de obtener evidencia de todos los movimientos importantes y además el minimizar la vigilancia humana de los monitores.

2.5.5 *Componentes básicos de un CCTV*

2.5.5.1 *La cámara*. El punto de generación de video de cualquier sistema de CCTV. Hay muchísimos tipos de cámaras, cada una para diferentes aplicaciones y con diferentes especificaciones y características:

- Blanco y Negro, Color o Duales (para aplicaciones de día y noche).
- Temperatura de funcionamiento.
- Resistencia a la intemperie.
- Iluminación (sensibilidad).
- Condiciones ambientales (temperatura mínima y máxima, humedad, salinidad).
- Resolución (calidad de imagen).
- Sistema de formato (americano NTSC, europeo PAL).
- Voltaje de alimentación.
- Dimensiones.
- Tipo de lentes que utiliza.
- Calidad y tamaño del CCD. - EL CCD es el chip que inicialmente capta la imagen y su tamaño y calidad es muy importante.
- El más comúnmente usado en el CCTV es el de 1/3”.

2.5.5.2 *El monitor*. La imagen creada por la cámara necesita ser reproducida en la posición de control. Un monitor de CCTV es prácticamente el mismo que un receptor de televisión, excepto que este no tiene circuito de sintonía. Pero la característica principal es la durabilidad de su pantalla. Debemos recordar que en el CCTV se requieren 24 horas de trabajo sin pérdida de la calidad de la imagen, durante muchos años y en condiciones desfavorables (TECNOTRONICA, 2015).

2.5.5.3 *Medios físicos de transmisión.* En la actualidad la mayoría de las redes están conectadas por algún tipo de cable, que actúa como medio de transmisión de señal entre los equipos. Hay distintos tipos de cables para cubrir las diferentes necesidades, estos se pueden agrupar en tres grupos principales:

2.5.5.4 *Dispositivos de registro.* Cuando se considera un sistema CCTV, hay dos tipos de dispositivos de registro que están disponibles en el mercado; Sistema de seguridad DVR (digital video recorder / grabador de video digital) y un sistema de seguridad NVR (network video recorder / grabador de video de red)

Grabador digital de video (DVR). Un grabador de video digital, graba, procesa y administra imágenes enviadas desde cámaras de seguridad analógicas. La conexión entre el DVR y la cámara analógica es utilizando el cable coaxial.

Grabador de video de red (NVR). Este dispositivo graba y administra imágenes previamente digitalizadas; las cuales son enviadas desde las cámaras IP a través de una red. Los NVR basados en computadoras o PCs, son simplemente un software que se instala en una computadora y administra las mencionadas cámaras. La potencia de estos equipos está dada por la cantidad de cámaras IP que puede administrar y la resolución a la que puede manejarlas.

Características técnicas de un grabador NVR

- Cantidad de cámaras a instalar.
- Calidad de imagen a grabar según las características técnicas de las cámaras.
- Ancho de banda de grabación.
- Tiempo de almacenamiento requerido, capacidad de discos duros.
- Salidas de video requerida: BNC, VGA.

- Modos de grabación: por movimiento, eventos alarma y normal.
- Funciones para conexión en RED o internet.
- Compatibilidad con otras marcas (ONVIF).
- Software de monitoreo en Red.
- Entradas y salidas de alarmas.

2.5.6 *UPS.* (Uninterruptible Power Supply) que en español quiere decir "Sistema de Alimentación Ininterrumpida"; es un dispositivo que gracias a su batería (6v.12v/5Ah.7,2Ah), puede proporcionar energía eléctrica tras un apagón a todos los dispositivos electrónicos conectados a él.

También puede regular el flujo de electricidad, controlando las subidas y bajadas de tensión y corriente existente en la red eléctrica.

El UPS mantiene la energía a las cargas críticas, aun cuando la energía eléctrica está en sobre-voltaje, debajo de voltaje, fuera de frecuencia, etc.

2.5.6.1 *¿Por qué necesitamos una UPS?* El 50% de los problemas ocasionados en los equipos eléctricos e informáticos y las pérdidas de información son debidos a interrupciones y perturbaciones en el suministro de la RED eléctrica.

Esto supone unas pérdidas en el mundo de aproximadamente 26 billones de dólares *(GARCÍA Cruz, y otros, 2007).*

Figura 13. Partes UPS

Fuente: https://goo.gl/JsPqyC

CAPITULO III

3. IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD

3.1 Selección de equipos para el sistema de seguridad

3.1.1 *Selección de equipos del sistema de CCTV.* Para poder hacer la selección de los equipos debemos tener en cuenta los siguientes aspectos:

3.1.1.1 *Alcance del sistema.* Este sistema tiene la función principal de facilitar las labores de vigilancia, monitoreo y control de personas, bienes; mediante captura de imágenes extraídas de las cámaras ubicadas estratégicamente para cubrir todo el laboratorio. Las cámaras deben ser gestionadas y visualizadas por personal de seguridad autorizado para estas actividades, este sistema además brinda visualización en tiempo real y se compone de dispositivos de grabación para tener respaldo de video las 24 horas al día.

3.1.1.2 *Selección conceptual.* El sistema está constituido de tres subconjuntos: subsistema de gestión, de cámaras y medios de transmisión. Los mismos que hacen uso de tecnología digital (la más actual) debido a las múltiples ventajas que ofrece respecto a la tecnología antigua de medios analógicos.

3.1.1.3 *Análisis y Selección del sistema.* Uno de los alcances del sistema es obtener una visión clara de los equipos del laboratorio las 24 horas del día, por tal motivo se instalaron las cámaras adecuadamente para cubrir todo el laboratorio y además enfocarse en visualizar el ingreso al mencionado lugar.

3.1.2 *Selección de equipos del sistema de control de accesos.* El laboratorio de automatización de procesos industriales es nuevo y posee equipamiento costoso, por lo que surge la necesidad de implementar un sistema de seguridad.

El sistema de control de accesos tiene el objetivo de controlar el personal que ingresa al laboratorio y administrar además el horario de dicha entrada según los permisos asignados. Cada persona que ingrese al laboratorio posee su propia huella dactilar única.

Para el sistema de intrusión los medios que serán instalados tienen la función de detectar y alertar remotamente el intento de violación o sabotaje de las medidas de seguridad instaladas.

- Existen medios pasivos y activos. Los medios pasivos son elementos de carácter estático y permanente, que permiten retardar un intento de invasión sin detectarlo, por ejemplo: vallas, cercados, setos, puertas y barreras. Los medios activos son elementos mecánicos o electrónicos que detectan la intrusión y emiten una señal que es audible o visible para la persona de seguridad a cargo, por ejemplo: detectores de apertura, de manipulación y movimiento.

- Selección conceptual. Para el sistema de control de accesos se requiere identificación de la persona al ingreso por medio de huella dactilar, por esta razón se utiliza lector biométrico y para salir del laboratorio se utiliza un pulsador.

- Análisis y Selección del sistema. Por medio de un análisis y estudio de los equipos pertinentes, poder resguardar los bienes existentes en el laboratorio. A continuación, se detalla todos los equipos que se va a utilizar para el laboratorio:

Tabla 2. Equipos para el Laboratorio

Equipos de acceso y cctv del laboratorio		
Dispositivo	**Cantidad**	**Lugar**
UPS	1	Laboratorio
Cámaras	2	
NVR	1	
Lector biométrico	1	Puerta
Cerradura electro-magnética	1	
Cerrojo electro-mecánico	1	
Pulsador de emergencia	1	

Fuente: Autores

3.1.2.1 *Cámara.* Tomando en cuenta las características para la selección de cámaras, la ideal para la implementación es la cámara de red tipo bullet que cuenta con sensor CMOS que es la tecnología actualmente utilizada, además consta de visión nocturna e infrarroja que nos permite ver en ambientes con bajos niveles de iluminación o en oscuridad. Para crear imágenes se apoyan en la tecnología de iluminación con “leds”, que permite inclusive ver en la gama multicolor para más información (ver anexo A)

3.1.2.2 *Grabador de video de red (NVR).* Para la selección del NVR se tomó en cuenta la cantidad de cámaras, calidad de procesamiento de la imagen, capacidad del disco duro, el tipo de salida de video debido a la conexión a un monitor, y lo más importante la compatibilidad que debe existir entre las marcas (ver anexo A)

3.1.2.3 *Cerraduras.* Para mejor seguridad del laboratorio de automatización de procesos industriales, se reemplazó la puerta de madera por una puerta metálica y para asegurarse de que no puedan abrirla manualmente se colocó dos cerrojos uno electro-mecánico y el otro electro-magnético, ambos funcionan a 12 V de corriente continua, conectadas en paralelo; para más información (ver anexo A).

3.1.2.4 *Dispositivo biométrico.* Se eligió el Reloj Biométrico-Control de Asistencia Con Huella X300, debido a cubre las necesidades para implementar el control de acceso y a su vez tiene conexión al computador para poder ver reportes de los usuarios que ingresan (ver anexo A).

Existen medios pasivos y activos. Los medios pasivos son elementos de carácter estático y permanente, que permiten retardar un intento de invasión sin detectarlo, por ejemplo: vallas, cercados, setos, puertas y barreras. Los medios activos son elementos mecánicos o electrónicos que detectan la intrusión y emiten una señal que es audible o visible para la persona de seguridad a cargo.

Tabla 3. Comparación de equipos biométricos

Equipo Biométrico Características	**Biométrico ICLOCK990**	**Biométrico X7**	**Biométrico X300**
Funciones	Control de Acceso Tiempo y Asistencia	Control de Acceso	Control de Acceso
Capacidad			
Huellas	10000	200	1000
Tarjetas	10000	200	1000
Contraseñas	10000	8	1000
Conexiones	Botón de Salida / Sensor de Puerta Salida de Alarma	Botón de Salida / Sensor de Puerta Salida de Alarma	Comunicación TCP/IP USB host
Alimentación	12VCD / 270mA en Standby y 330mA en Operación	12VCD / 90mA en Standby y 120mA en Operación	5V DC 2A

Fuente: Autores

3.1.2.5 *Sistema de alimentación ininterrumpida (UPS).* Para seleccionar el UPS ideal se debe calcular, sumando las potencias de todos los equipos dentro del cuarto de control, los cuartos de interconexión y obviamente todos los dispositivos eléctricos del proyecto. Tomando en cuenta los parámetros descritos anteriormente tenemos:

Tabla 4. Potencia de equipos

Equipos	**Potencia**
NVR	30W
Cámaras	15W
Cerradura electro-magnética	12W
Cerrojo electro-mecánico	12W
Monitor	75W
Equipo Biométrico	10W
Total	154W

Fuente: Autores

$$154+30\%(46.2) + 25\%(38.5) = 238.5$$

Al total de las potencias de los equipos se debe sumar el 30% por incremento de equipos y además el 25% de seguridad lo cual nos da un valor de 238.4 vatios, en el mercado hay de 250 vatios, cumpliendo los parámetros para la selección para más detalles (ver anexo A)

El UPS permite que los equipos no se perjudiquen al momento de una interrupción del suministro eléctrico o cuando regrese la energía súbitamente, debido que en ese preciso instante se evidencia el sobre voltaje; además este equipo es necesario para que funcione ininterrumpidamente el sistema.

3.2 Diagramas de instalación

Para la interconexión de los dispositivos debemos tomar en cuenta el flujo de energía eléctrica y la transmisión de datos.

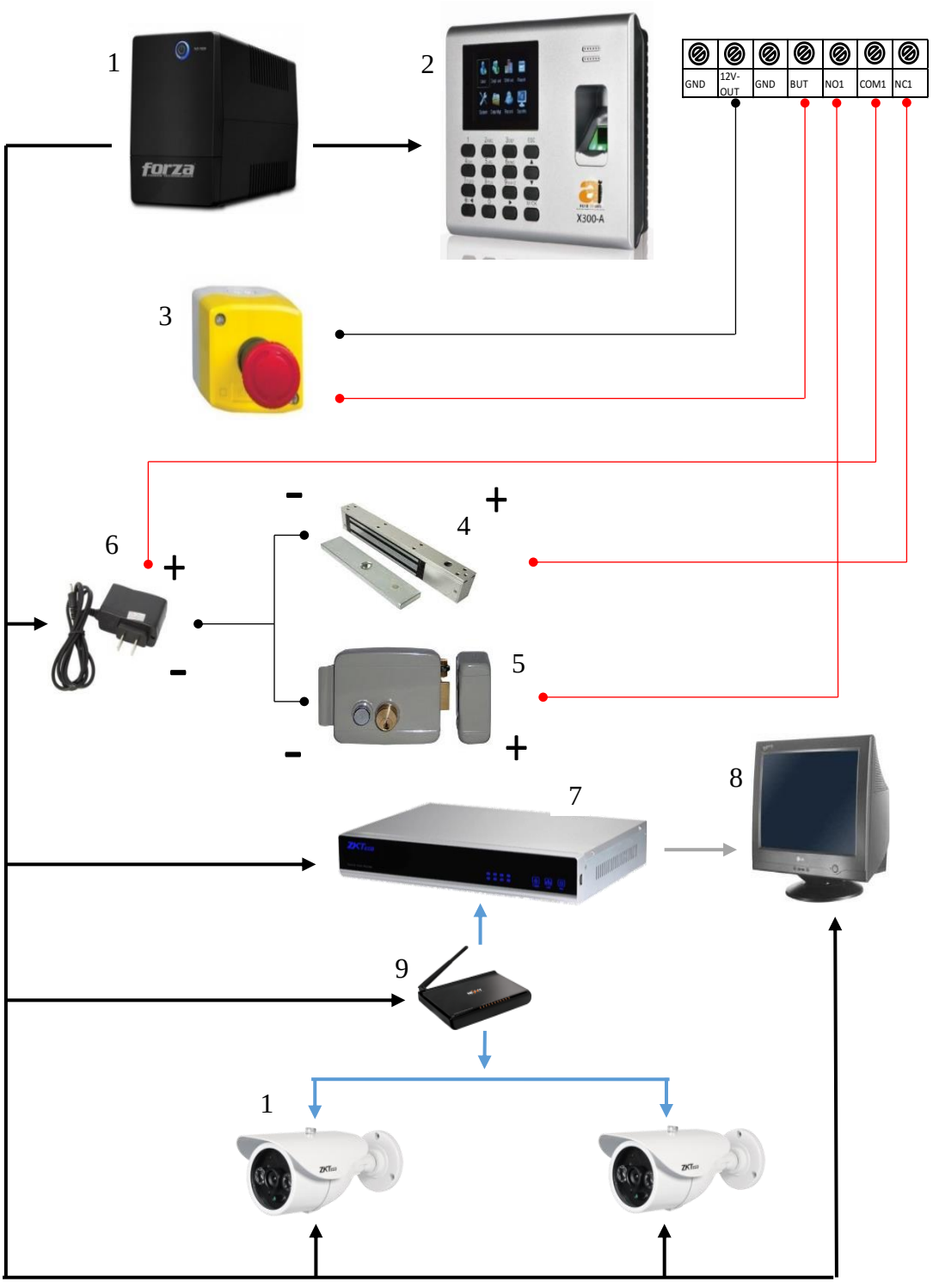
3.1.1 *Sistema de alimentación ininterrumpida (UPS).* Controla el flujo de energía eléctrica, proporciona corriente ininterrumpida para los dispositivos conectados a éste aparato mediante una alimentación de corriente normal.

3.1.2 *Dispositivo de acceso biométrico.* En la parte posterior posee las terminales de energía y de transmisión de datos, las cuales debemos identificar previamente. NC (Normalmente Cerrado), NO (Normalmente Abierto), COM (común), OUT 12V (Salida de 12V de energía eléctrica). De la terminal OUT del biométrico de acceso conexionamos al común (COM) del pulsador de salida, en el mismo dispositivo se encuentra el conector BUT a este lo enlazamos al normalmente abierto (NO) del botón antes mencionado. Así queda configurado para que el "pulsador de salida" permita el cierre de sesión sin afectar la estructura de programación del biométrico de acceso.

Para energizar el cerrojo electro-magnético conectamos el normalmente cerrado (NC1) del acceso biométrico al positivo de la cerradura referida. El cable que proviene del normalmente abierto (NO1) del biométrico empalmamos al positivo de la cerradura electro-mecánica, las terminales negativas de ambas cerraduras (electro-magnética y electro-mecánica) las enlazamos a la negativa del conector de energía, la terminal positiva que queda de éste último se acopla al común (COM1) del dispositivo de acceso biométrico. De esta manera queda estructurado el sistema para que al ingresar la huella registrada se abran los cerrojos y el usuario pueda acceder al laboratorio. Una vez finalizada la tarea dentro del laboratorio la o las personas que se encuentran dentro del laboratorio puedan salir pulsando el botón de cierre de sesión. Tenga en cuenta que la responsabilidad de los bienes rige sobre la persona que ha registrado el último acceso hacia las instalaciones.

3.1.3 *Grabador de video de red (NVR).* Las cámaras, el router, y monitor, tienen su propio conector de alimentación eléctrica y se conectan a las terminales de energía eléctrica respectivas ubicadas en el UPS. Para la transmisión de datos usamos cable UTP con terminales RJ45, a este conjunto se le denomina cable Ethernet # 6. Cada cámara la conectamos a una terminal del router, a este último lo acoplamos al NVR; las conexiones entre estos dispositivos realizamos con el cable Ethernet # 6. Para visualizar las grabaciones de imágenes realizadas por el conjunto anterior, al NVR lo enlazamos al monitor mediante cable VGA, y todo este sistema toma el nombre de Circuito Cerrado de Televisión. El acceso biométrico sumado al circuito cerrado de televisión proporciona el monitoreo, control y vigilancia requeridas para el Laboratorio de Automatización de Procesos de la Escuela de Ingeniería Industrial; resguardando los bienes e identificando a las personas que hacen uso de las instalaciones.

Figura 14. Diagrama de Instalación



1	UPS	6	Cerrojo electro-mecánico	Flujo de energía eléctrica (Cable de corriente)
2	Biométrico X300	7	NVR	Flujo de alimentación eléctrica (Cable flexible # 10)
3	Pulsador de salida	8	Monitor	Flujo de datos (Cable Ethernet categoría 5)
4	Cargador 12V	9	Router	Flujo de datos imágenes (Cable VGA)
5	Cerradura electro-magnética	10	Cámaras	

Fuente: Autores

3.3 Preparación y Ubicación de dispositivos

3.3.1 *Preparación de equipos de un sistema de CCTV.* Al hablar de preparación se hace referencia a lo que es al manejo, almacenaje y uso de los equipos:

Para el almacenaje, no colocar cosas pesadas sobre las cámaras y el NVR.

Para el traslado de los equipos; llevarlos con cuidado, si se caen los componentes internos puede sufrir daños irreparables.

3.3.2 *Ubicación de equipos de un sistema CCTV.* Para la ubicación se debe tomar en cuenta el lugar adecuado.

3.3.2.1 *Preparar el lugar (laboratorio).* Se identifican los lugares en los que debe hacerse mayor vigilancia.

Monitorear la mayor superficie posible del laboratorio, priorizar las áreas que más interesa vigilar teniendo en cuenta que no existan objetos que bloqueen la vista.

3.3.2.2 *Instalar las cámaras.* Selecciona un ángulo alto y ancho para las cámaras

El mejor sitio de visualización es la parte superior de la habitación enfocando la cámara hacia abajo, asegurarse que pueda ver claramente lo que son las entradas y salidas.

3.3.2.3 *Montar las cámaras en el techo.* Algunas cámaras vienen con almohadillas adhesivas para fijarlas en la pared o techo, pero la forma más segura es atornillándolas.

Los pasos para montar las cámaras son:

- Colocar la plantilla en la ubicación adecuada.
- Marcar el lugar en donde colocará el tornillo.
- Hacer el agujero para cada tornillo usando un taladro.
- Colocar tacos de sujeción en cada agujero.
- Atornillar la cámara contra el techo.
- Colocar la cámara apuntando el ángulo deseado.

3.3.2.4 *Conectar la cámara a su fuente de alimentación.* Casi todas las cámaras vienen con un adaptador de corriente que se puede conectar a cualquier toma eléctrica de cualquier instalación domiciliaria.

3.3.2.5 *Conectar la cámara con cables ethernet al NVR.* El equipo de vigilancia se conecta con cables Ethernet # 6. Los cables son fáciles de utilizar por cuanto son flexibles, cuando se instalan varias cámaras se debe conexionar a un router y posteriormente al NVR.

3.3.2.6 *Conectar monitor al NVR.* Esta conexión se realiza por medio de cable VGA que trasmite la señal de video hacia el monitor.

3.3.2.7 *Resolver problemas de conexión.* Comprobar que las cámaras, el NVR y el monitor estén conectados a la fuente de alimentación, en nuestro caso el UPS.

Revisar que estén encendidos, asegurase de que los cables Ethernet y VGA estén conexionados correctamente a los dispositivos respectivos.

Además, se debe colocar los cables en canaletas para protegerlos de la desconexión accidental, deterioro, intemperie; la estética de presentación del cableado juega un papel importante.

3.3.3 *Preparación de equipos de un sistema de control de acceso*. Al hablar de preparación hacemos referencia a lo que es el manejo, almacenaje y uso de los equipos:

Para el almacenaje, no colocar elementos pesados, corrosivos, o líquidos sobre el dispositivo biométrico.

Trasladar los equipos con cuidado los componentes internos son sensibles y están calibrados para un uso específico, si se caen sufren daños irreversibles.

Para el uso del equipo biométrico se debe tener cuidado que el sensor de huella no sufra ralladuras, agrietamientos, golpes, en lo posible no tenga contacto con líquidos de cualquier tipo, porque si sufre algún tipo de daño el sensor deja de funcionar y no cumple su objetivo.

3.3.4 *Ubicación de equipos de un sistema de control de acceso.* Para la ubicación del equipo biométrico lo más importante es que sea visible y a su vez fácil para el registro de los usuarios.

3.3.4.1 *Preparar el lugar (laboratorio).* Para la preparación tomar en cuenta los siguientes puntos:

- Dibujar un diagrama del lugar en el que se puede colocar el equipo biométrico.

- Debe tener en cuenta el fácil acceso del usuario hacia el dispositivo, la iluminación adecuada y la visibilidad del mismo.

3.3.4.2 *Instalar el equipo biométrico.* La instalación se debe hacer tomando en cuenta los siguientes parámetros:

- Seleccionar el lugar donde va a instalarse el equipo biométrico

- Se instala al lado derecho de la puerta para poder abrirla fácilmente, debido a que las personas se registran frecuentemente con los dedos de la mano derecha y con la izquierda abrir la puerta.

- La altura del biométrico es de carácter ergonómico, es decir el dispositivo se ubica a una altura promedio tomando en cuenta la estatura media de las personas en el Ecuador.

- Seleccionar el lugar donde va a instalarse equipos adicionales

- El cerrojo electro-mecánico se instala en la cara interior de la puerta al lado central- izquierdo.

- La cerradura electro-magnética se la aloja en la sección superior de la puerta permitiendo la apertura al introducir la huella.

- El pulsador de salida se ubica en un lugar visible para en el caso de emergencia abandonar el laboratorio rápidamente.

3.4 Software ZKivision

El software de cliente ZKiVision es una pieza de software de red de video vigilancia proporcionada por ZK Tecnología. Es compatible con varios sistemas operativos y posee múltiples funciones tales como: monitoreo, grabación en vídeo, y la vinculación de alarma de múltiples cámaras IP a través de LAN e Internet.

3.4.1 *Requisitos Mínimos de Software y Hardware.* Los requisitos mínimos que se requieren para que el sistema pueda funcionar son:

Sistema Operativo: Windows 2000 / Windows XP / Windows 2003 / Windows Vista / Windows 7 (32 bits). Se recomienda Windows XP.

CPU: Pentium 4 o superior Inter, 2.6 GHz o superior se recomienda.

Adaptador de vídeo: Resolución de 1024 x 768 píxeles o superior. Mínimo de memoria de 256 MB, ATI (AMD). Se recomienda adaptador de vídeo con la memoria 1G o superior.

Memoria: 1 GB de capacidad mínima de. Se recomienda 2G o superior.

Disco duro: espacio libre mínimo de 80 GB (dependiendo del número de dispositivos y configuración de vídeo).

3.4.2 *Configuración de NVR.* Introducir la dirección IP del NVR en la barra de direcciones del navegador de Internet Explorer (la dirección IP predeterminada: 192.168.1.88), por ejemplo, http://192.168.1.88, y entra en la pantalla del inicio.

Figura 15. Inicio NVR

Fuente: Autores

Si utiliza el inicio de sesión de internet explorer por primera vez, el sistema avisará cargar el plugin. El nombre de usuario y contraseña de acceso corresponden a los que están en el manual. El administrador por defecto es “admin” y la contraseña respectiva.

Atención:

- Asegurar de que el equipo esté conectado correctamente al internet.

- Configurar la dirección IP, la máscara de subred y la puerta de entrada al NVR respectivamente (Si no hay equipos de enrutamiento en la red, asigna la dirección IP al mismo segmento de red; si lo hay, es necesario ajustar la máscara de subred y la puerta de entrada correspondientes.).

- Aprovechar el ping (IP de NVR) para examinar si la red está conectada correctamente.

- El control web se puede descargar y distinguir automáticamente, y se elimina el control original cuando actualiza la nueva versión.

Después de iniciar la sesión, entra en la pantalla principal como se muestra:

Figura 16. Pantalla principal

Fuente: Autores

El menú se encuentra en la parte superior de la pantalla, que divide en:

Vídeo búsqueda: Seleccionar y entrar en la interfaz de reproducción de vídeo búsqueda.

Ajuste de alarma: Seleccionar y entrar en la interfaz de ajuste de alarma.

Configuración del sistema: Seleccionar y entrar en la interfaz de panel de control.

Relacionado: Buscar la información de la versión de NVR.

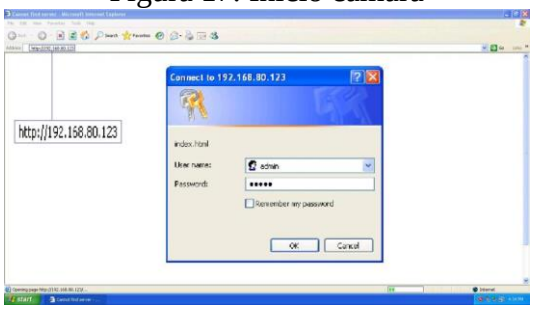
Salida: Salir de la pantalla de operación de NVR.

3.4.3 *Configuración de cámaras.* Todas las cámaras poseen tecnología POE/IP, poseen una dirección pre-establecida que permite acceder a las configuraciones del equipo, tienen el mismo método de configuración.

Los productos de esta serie utilizan el sensor CMOS mega-píxeles, equipados con luz infrarroja de la matriz de puntos; disponen de una excelente visión nocturna. Algoritmo de codificación H.264 optimizado, así garantiza un efecto de transmisión de vídeo más clara y más suave. Estos dispositivos son fáciles de instalar, utilizar, convenientes para realizar el monitoreo en el día o la noche en diversos lugares de corto alcance, así como el acceso remoto del video a través de la red.

3.4.3.1 Uso del navegador web de la cámara. Abrir el navegador, en la barra de dirección entra directamente el nombre de dominio o la dirección IP de la cámara (por ejemplo: http://192.168.1.86), hace clic en enter para aparecer la pantalla de iniciar sesión indicada como lo siguiente:

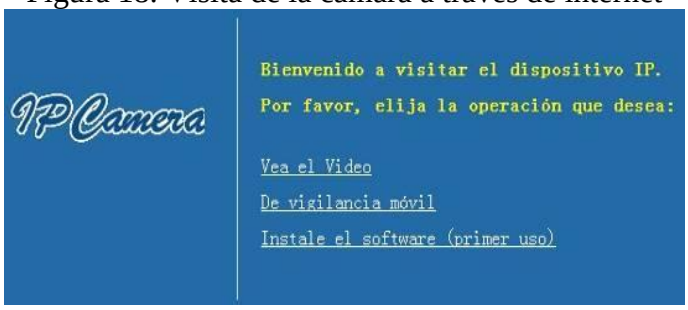
Figura 17. Inicio cámara



Fuente: Autores

Al entrar el nombre y la contraseña del usuario, hace clic en "OK" y la página de la guía como la siguiente:

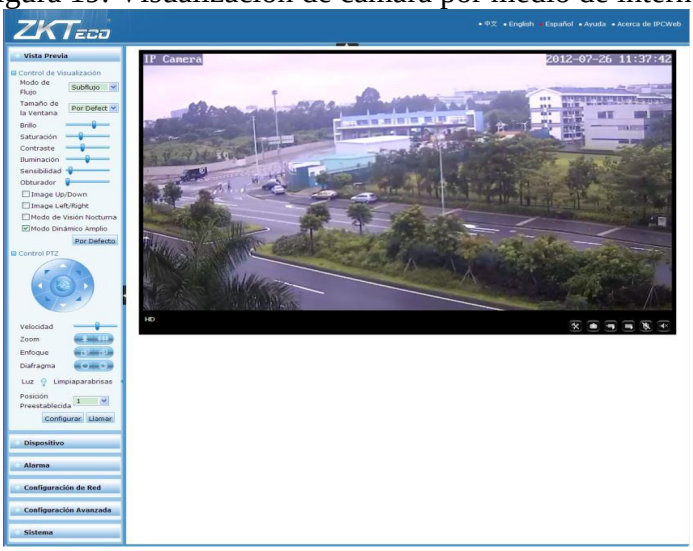
Figura 18. Visita de la cámara a través de internet



Fuente: Autores

Haga clic en "Ver el Video" en la página de la guía para entrar en la "Vista Previa" de la interfaz, y el vídeo se reproducirá con normalidad.

Figura 19. Visualización de cámara por medio de internet



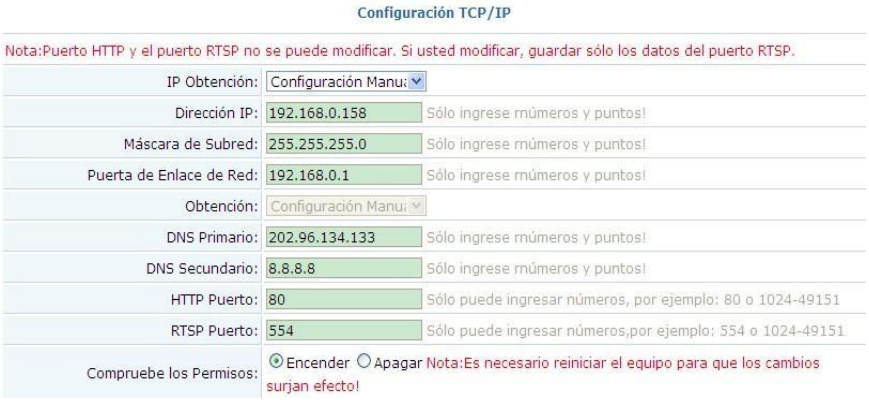
Fuente: Autores

Nota: Conexión por primera, descargar e instalar el ActiveX para ver el video con normalidad.

Este ActiveX es necesario para el programa de aplicación Web que se ejecuta sin ningún tipo de peligro para su equipo.

Por favor consulte [Manual de Usuario sobre WEB Server] en el CD suministrado al administrador del laboratorio para más detalles.

Figura 20. Configuración IP



Fuente: Autores

IP Obtención: Cuando se selecciona "Configuración manual", se necesita escribir a mano la dirección de IP, mascara de sub-red y la puerta de red; cuando se selecciona [Adquisición automáticamente] al conectarse con la LAN, la cámara obtiene la dirección IP activa asignada por el servidor DHCP.

Dirección IP: El valor por defecto es 192.168.1.88, se puede cambiarlo según sea necesario. Al lograr el éxito la modificación la cámara se reiniciará automáticamente.

Máscara de Subred: El valor por defecto es 255.255.255.0, se puede cambiarlo según sea necesario.

Puerta de Enlace de Red: El valor por defecto es 192.168.1.1, si la cámara y el PC están en diferentes segmentos, es necesario establecer la dirección de la pasarela.

(DNS) Obtención: DNS (servidor de nombre de dominio) puede traducir el nombre de dominio a la dirección IP. Cuando se selecciona [Configuración manual], se necesita escribir a mano la dirección preferida y alternativa de DNS; en el caso de [Adquisición automáticamente (IP)] selecciona [Adquisición automáticamente (DNS)], al conectarse con la red de área local, la cámara obtendrá automáticamente la dirección de DNS.

DNS Primario: El valor por defecto es 192.168.1.1, se puede modificarlo de acuerdo con su necesidad.

DNS Secundario: Cuando el DNS preferido no se puede conectar o se produce un error, el sistema se conectará con el DNS alternativo.

HTTP Puerto: El valor por defecto es 80. Si se necesita el cambio, por favor póngase en contacto con su administrador de red o consulte a un profesional.

RTSP Puerto: El valor predeterminado es 554. Si es necesario utilizar el reproductor que soporta el protocolo RTSP en conexión con la cámara para transmitir videos, necesita la direccione de URL, el código del flujo de datos principal; si es modificado el Puerto de RTSP, entrará la dirección IP: Puerto (código del flujo de datos). Después de terminar con éxito la modificación del Puerto, se reiniciará de nuevo la cámara.

Compruebe los Permisos: Si se selecciona [Encender], en momento de utilizar el reproductor que soporta el protocolo RTSP el usuario tiene que iniciar sesión.

3.5 Instalación del software y carga del programa

3.5.1 *Instalación del Sistema CCTV.* Para la instalación debemos primero revisar que las conexiones estén bien para luego proceder a la carga del programa.

Encender. Conectar la línea de la fuente de alimentación, pulse el botón de encendido, la luz indicadora funciona, NVR enciende, el modo de salida de video es de multi-pantalla por defecto, el sistema iniciará automáticamente la función de grabación.

Acceder al sistema. Después de inicio normal, haga clic una vez en el botón derecho del ratón para acceder al menú, aparece un cuadro de diálogo de [acceder], el administrador introduce la contraseña respectiva.

- Menú de registro, se abre el sub-menú de lista, búsqueda y copia de seguridad.

Figura 21. Menú Registro

Fuente: Autores

- Menú de alarma aquí se abre el sub-menú de modo detección, alarma de entrada, red de alarma, salida de alarma, anomalía y despertador digital.

Figura 22.Menú Alarma

Fuente: Autores

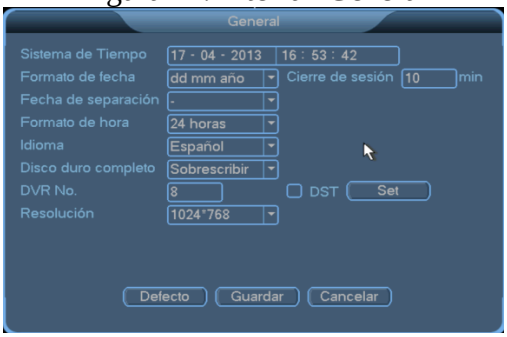
- Menú marco aquí se abre el sub-menú de general, red, mostrar, cuenta, PTZ y Tour.

Figura 23. Menú Marco

Fuente: Autores

- Sub-menú general en el cual se debe configurar lo que es la hora, formato de fecha, formato de hora, idioma resolución, etc.

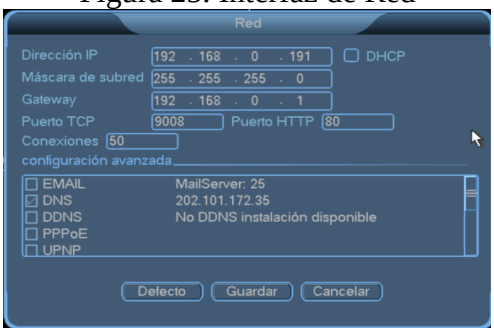
Figura 24. Interfaz General



Fuente: Autores

- Sub-menú de red en el cual se debe configurar lo que es dirección IP se puede dejar la que viene de fábrica o a su vez pulsando el botón [DHCP].

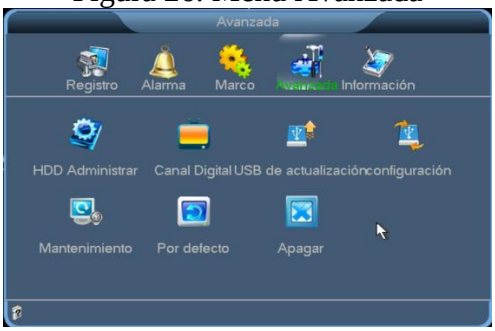
Figura 25. Interfaz de Red



Fuente: Autores

- Menú avanzado, se abre el sub-menú de HDD administrador, canal digital, USB configuración, Mantenimiento, por defecto y apagar.

Figura 26. Menú Avanzada



Fuente: Autores

- Sub-menú de canal digital en donde se configura la conexión de nueva cámara, se debe elegir el canal que se a conectar, luego hacer doble chip en buscar dispositivos, para finalmente seleccionar el dispositivo y poner guardar.

Figura 27. Registro de Nueva Cámara

Fuente: Autores

Apagar. Para el apagado del grabador de video de red (NVR) del sistema de seguridad se puede hacer mediante tres formas.

Medida I: Pulse el encendido de la alimentación a estado OFF para que el grabador de video de red se apague.

Medida II: En el [menú del sistema], [apagar el sistema] seleccionar [apagar], y el equipo se apagará.

Medida III: En el [menú del sistema], [menú principal], [herramientas de administración], [apagar el sistema], se selecciona [apagar], para que el grabador de video de red se apague.

3.5.2 *Instalación del Sistema de Acceso*. Para la instalación del controlador de accesos primero se debe colocar el CD en el computador en donde se va quedar para posterior revisión de parte de la persona encargada del laboratorio y luego debemos revisar que las conexiones estén bien para luego procedemos a la instalación y la carga del programa.

3.5.3 *Instalación del software*. Antes de instalar el software, es mejor cerrar todas las otras aplicaciones y programas (desactivar el antivirus), con el fin de no tener conflictos en el proceso de instalación el motivo es que los programas y el antivirus impiden la correcta instalación.

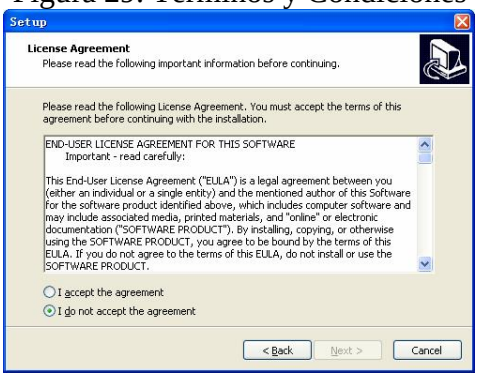
- Seleccionar el idioma y hacer clic en Aceptar,

Figura 28. Inicio Instalación

Fuente: Autores

- Por favor, lea el Acuerdo cuidadosamente. Si desea instalar seleccione aceptar el contrato y hacer clic en siguiente.

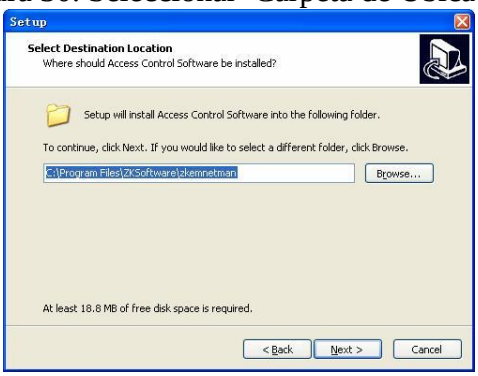
Figura 29. Términos y Condiciones



Fuente: Autores

- Seleccionar la carpeta donde instalar el software y hacer clic en siguiente.

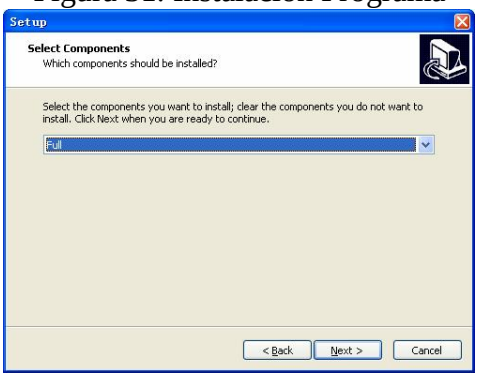
Figura 30. Seleccionar Carpeta de Ubicación



Fuente: Autores

- Seleccionar el componente de instalación del software y hacer clic en siguiente.

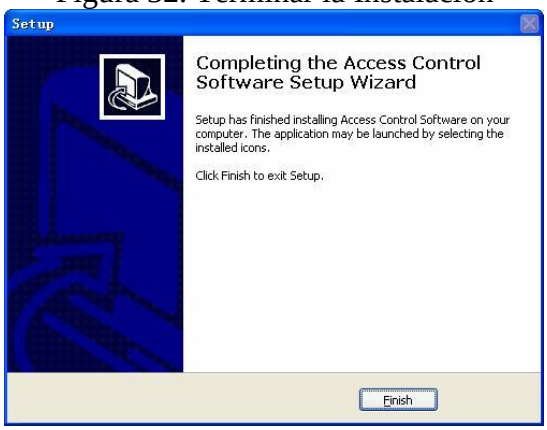
Figura 31. Instalación Programa



Fuente. Autores

- Hacer clic en Instalar y luego de terminar la instalación, hacer clic en Finalizar para completar el proceso.

Figura 32. Terminar la Instalación

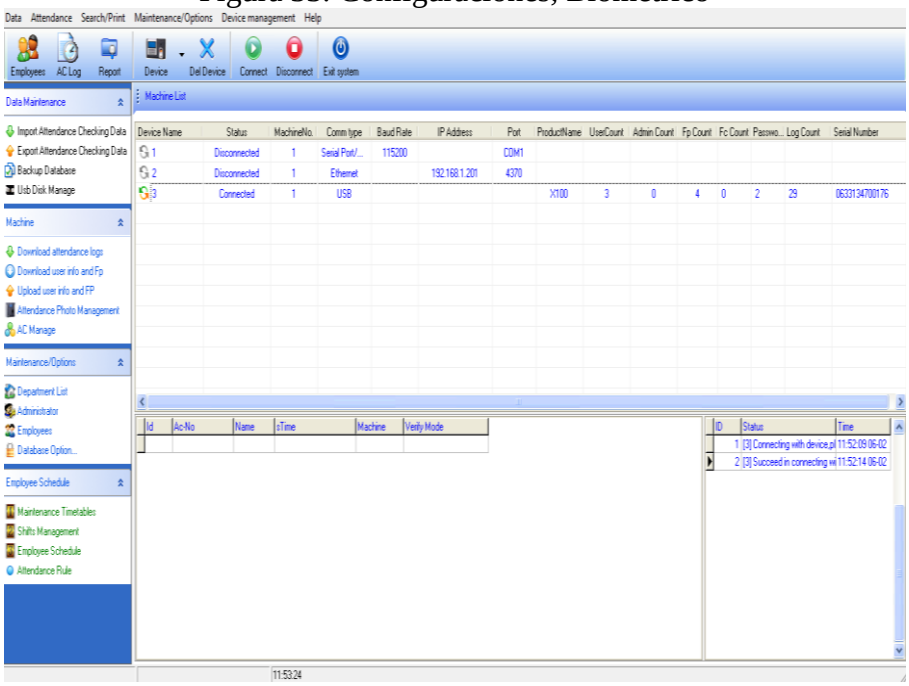


Fuente: Autores

3.5.4 *Manejo del software.* Como se debe usar el programa para poder controlar el dispositivo biométrico.

3.5.4.1 *Abrir el programa.* Por defecto aparecen 3 configuraciones para poder conectarse a los equipos biométricos, la utilizada es por medio de USB o a través de cable ethernet.

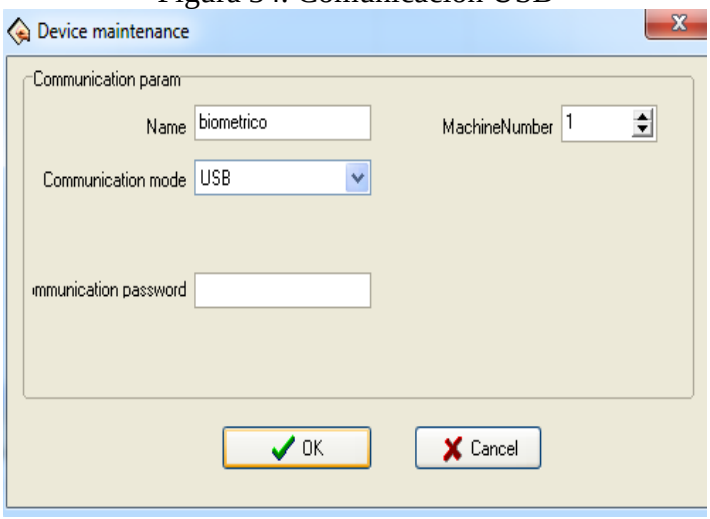
Figura 33. Configuraciones, Biométrico



Fuente: Autores

- Antes de conectarse al equipo biométrico es recomendable asignarle un nombre para poder identificarlo fácilmente.

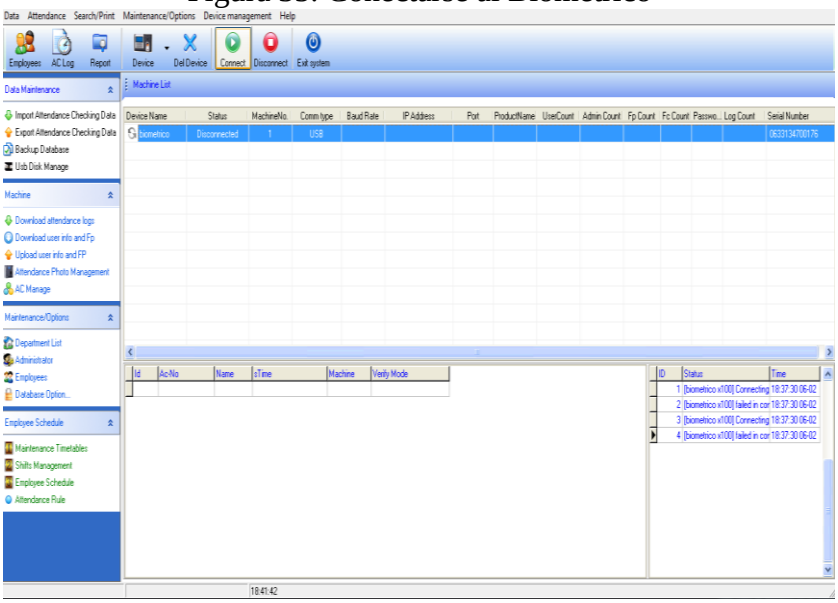
Figura 34. Comunicación USB



Fuente: Autores

- Presionar conectar y esperar que se conecte

Figura 35. Conectarse al Biométrico

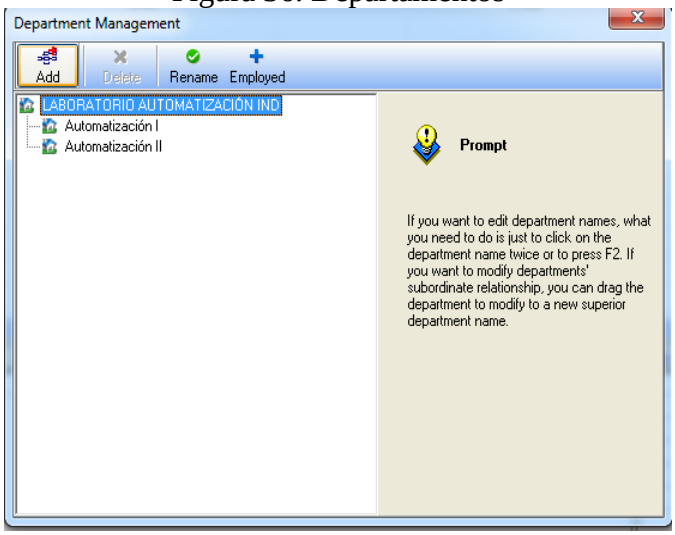


Fuente: Autores

3.5.4.2 *Crear departamentos o áreas Seleccionar deparment list (lista de departamentos)*

- Seleccionar rename (cambiar nombre) y asignar el nombre de la empresa o institución, luego seleccionar add (añadir) y creamos los departamentos, respesctivos.

Figura 36. Departamentos

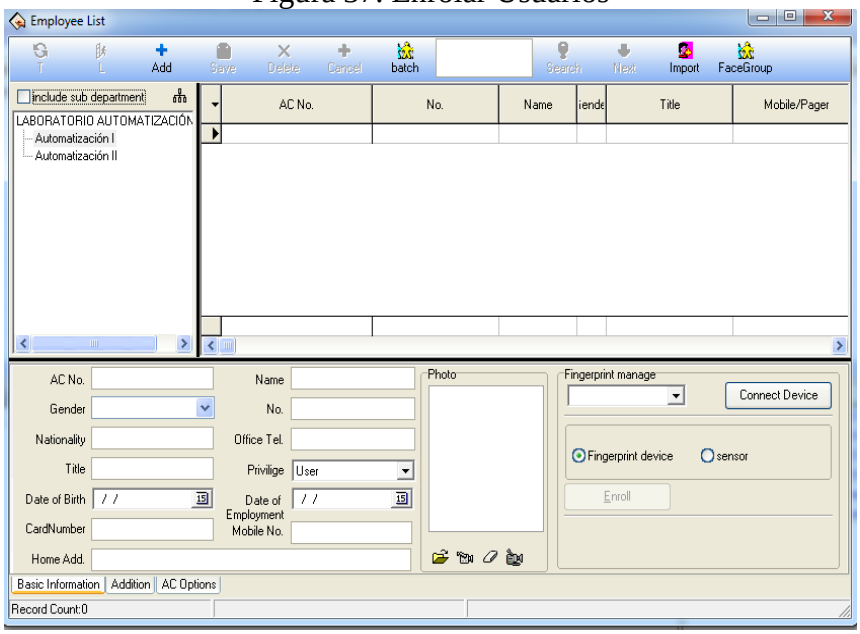


Fuente: Autores

3.5.4.3 *Enrolar usuarios*

- Dentro del departamento Laboratorio de Automatización hemos creado 2 departamentos Automatización I y Automatización II

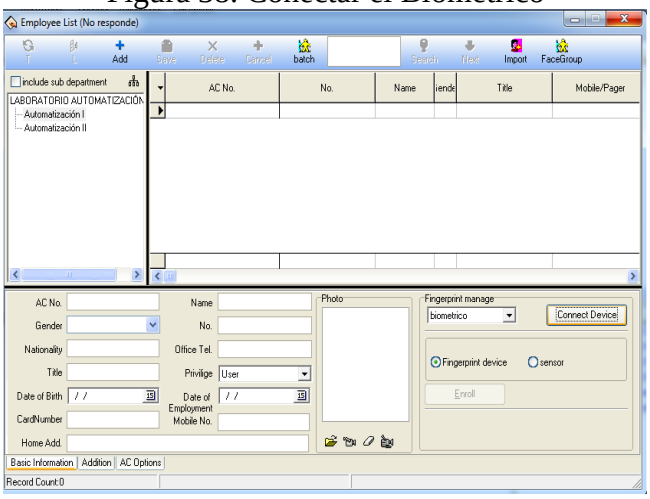
Figura 37. Enrolar Usuarios



Fuente: Autores

- Se debe conectar al biométrico en el cual se va a registrar las huellas de los usuarios.

Figura 38. Conectar el Biométrico



Fuente: Autores

Ejemplo 1: agregar un usuario, primero seleccionar el departamento luego escribir el nombre, después presionar enrol (enrolar) para registrar la huella respectiva directamente desde el biométrico repitiendo tres veces la puesta de la huella.

Figura 39. Insertar Huella

Fuente: Autores

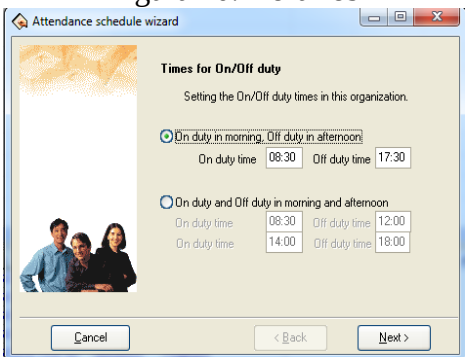
- Por último, presionar add (añadir) y así queda registrado nuestro nuevo usuario

3.5.4.4 *Asignación de Horarios*

- Seleccionar la opción maintenance timetables (mantenimiento de horarios)

- El software nos da a elegir los horarios continuo y separado la hora de almuerzo.

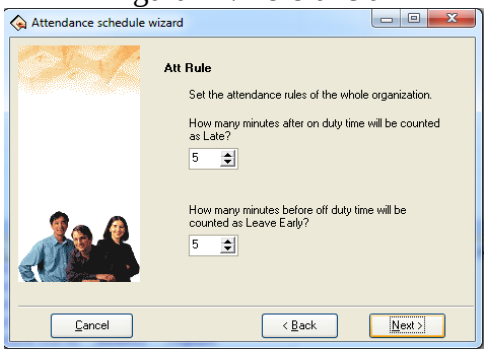
Figura 40. Horarios



Fuente: Autores

- En este cuadro se nos pregunta a cerca de la tolerancia en minutos a la entrada antes de considerar el atraso.

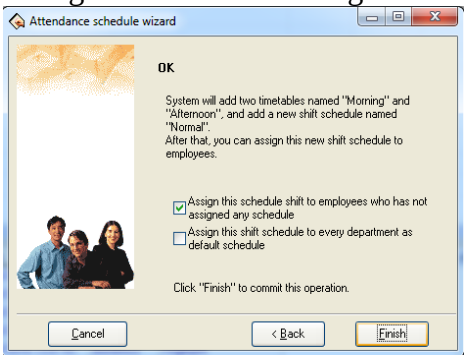
Figura 41. Tolerancia



Fuente: Autores

- Aquí se nos pregunta si este horario se le puede asignar a todos los usuarios que no tengan aun horario designado e igual en los departamentos.

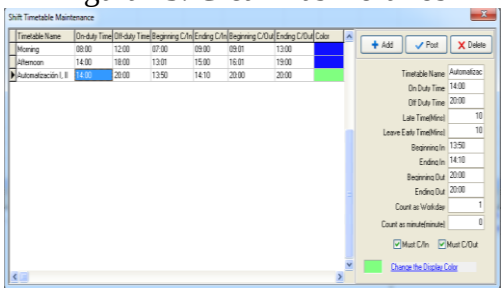
Figura 42. Horario Designado



Fuente: Autores

- En este cuadro nos permite crear más horarios, presionar add (añadir) y crear otro horario, el cual será para los estudiantes tanto de Automatización I como de Automatización II además de crear un horario corrido para los usuarios que no estén en el horario de clases respectivo.

Figura 43. Crear más Horarios

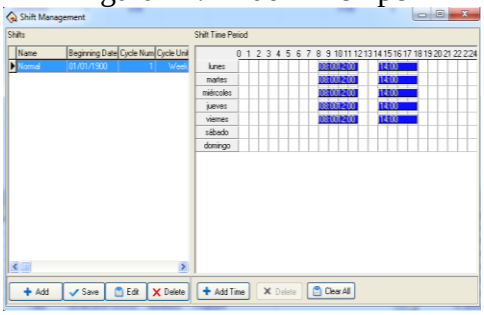


Fuente: Autores

3.5.4.5 *Seleccionar shifts mangement (manejo o gestión de turnos)*

- Presionar add time (añadir tiempo)

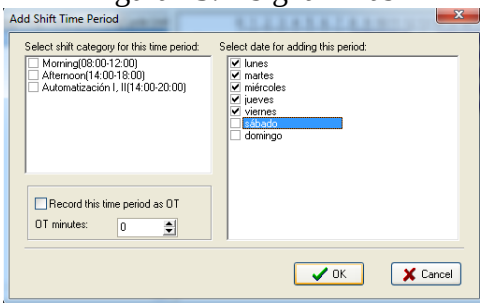
Figura 44. Añadir Tiempo



Fuente: Autores

- Aquí se asigna los días para cada horario

Figura 45. Asignar Días



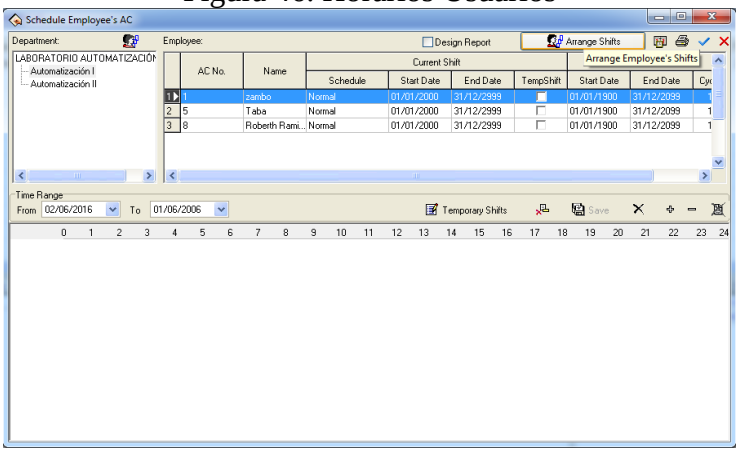
Fuente: Autores

- Al terminar solo le damos guardar en save (guardar) y salir en la X

3.5.4.6 *Entrar a employee schedule (horario de empleados)*

- En este cuadro se detalla los horarios, los mismos que estan asignados a los usuarios. A cada usuario le asiganamos el horario, para esto presionamos arrange shifts (carbiar turno)

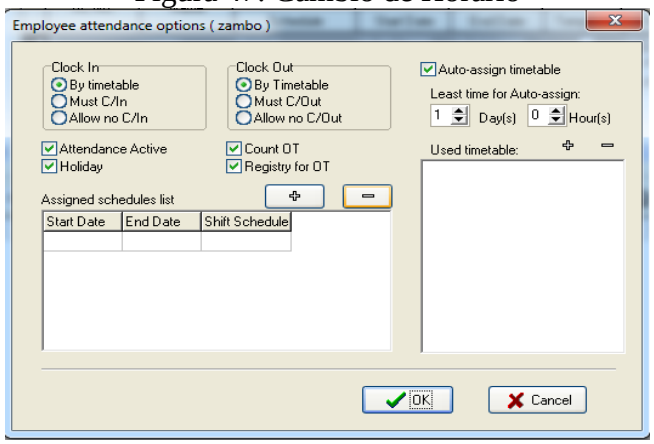
Figura 46. Horarios Usuarios



Fuente: Autores

- Se abre un cuadro en el cual se muestra el horario actual solo procedemos a eliminarlo y después agregamos un nuevo horario y presionar aceptar

Figura 47. Cambio de Horario



Fuente: Autores

- Una vez que todos los usuarios tengan su respectivo horario salimos presionando la tecla cerrar.

CAPITULO IV

4. PRUEBAS, RESULTADOS Y MANTENIMIENTO DEL SISTEMA DE SEGURIDAD

4.1 Descripción y manejo del sistema biométrico

4.1.1 *Análisis del sistema.* El sistema se ha implementado de manera que satisfaga las necesidades de resguardar los bienes existentes al interior del laboratorio.

Descripción general. El sistema de control de accesos y asistencia surge de la necesidad de controlar el ingreso de las personas al laboratorio y además llevar un registro de asistencia de los estudiantes que asisten a la cátedra de Automatización de Procesos de la Escuela de Ingeniería Industrial.

Análisis y descripción de requerimientos. El dispositivo de acceso biométrico permite el ingreso y control de los estudiantes junto con el personal autorizado con el fin de generar reportes los cuales pueden ser descargados por medio de cable USB o a través de tarjeta SD.

Descripción del usuario. El equipo biométrico cuenta con la interacción de dos usuarios (administrador y persona autorizada) los mismos que poseen diferentes actividades que deben desarrollar.

El administrador es el encargado de llevar el control de horarios, reportes e ingreso de nuevos estudiantes.

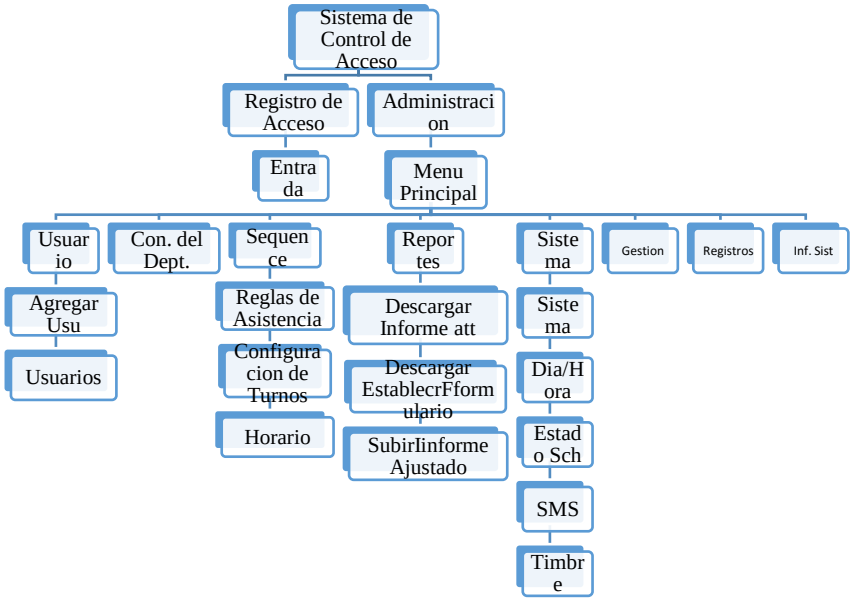
Las personas autorizadas usan el laboratorio ingresando al sistema en el horario programado por el administrador.

Existen medios pasivos y activos. Los medios pasivos son elementos de carácter estático y permanente, que permiten retardar un intento de invasión sin detectarlo, por ejemplo: vallas, cercados, setos, puertas y barreras. Los medios activos son elementos mecánicos o electrónicos que detectan la intrusión.

4.1.2 *Diagramas de navegación.* Se dividen en los siguientes:

4.1.2.1 *Diagrama general de navegación del sistema*. Es todo lo que contiene el equipo biométrico en sus características.

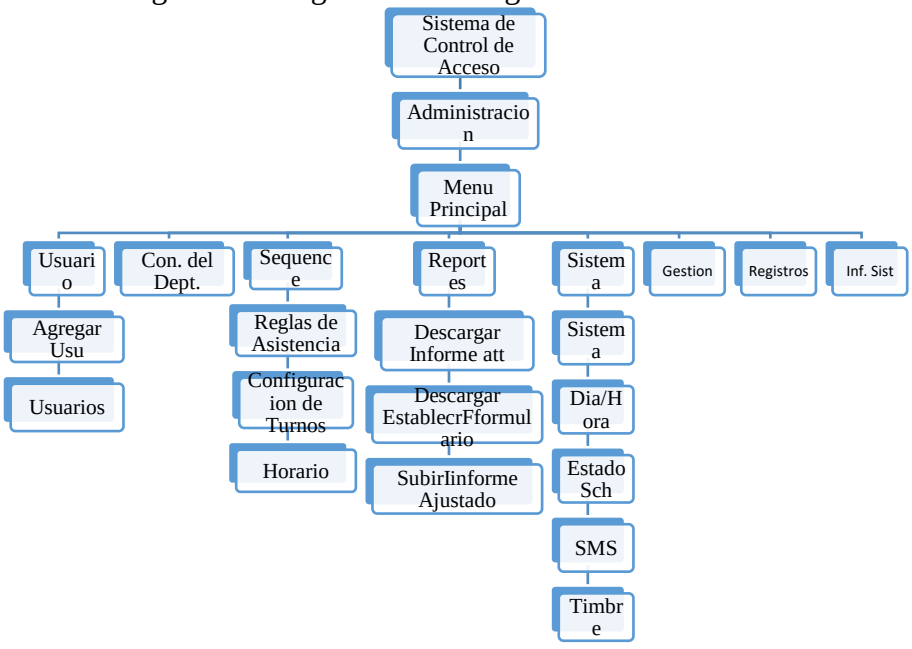
Figura 48. Diagrama General de Navegación del Sistema



Fuente: Autores

4.1.2.2 *Diagrama de navegación administrador*. Los parámetros más importantes.

Figura 49. Diagrama de Navegación Administrador



Fuente: Autores

4.1.2.3 *Diagrama de navegación estudiante.* Es el registro de ingreso que puede ser utilizado por el usuario.

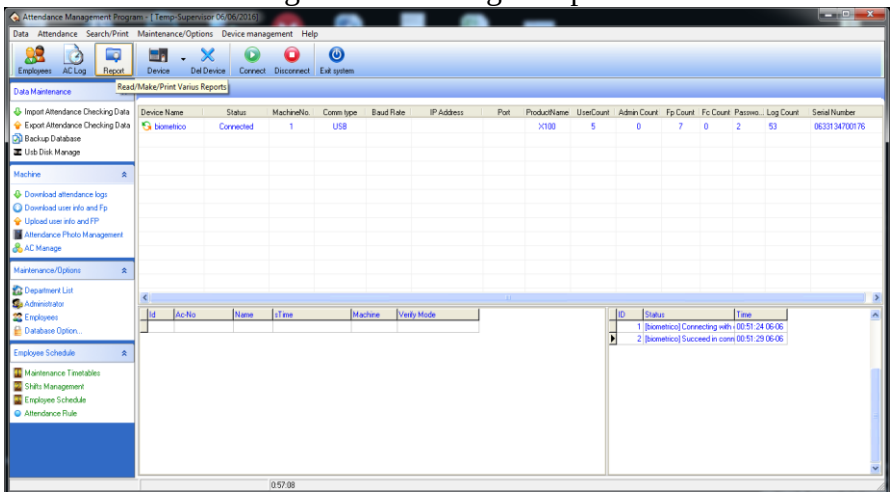
Figura 50. Diagrama de Navegación Estudiante

Fuente: Autores

4.1.3 *Reportes de asistencia de usuarios.* Se debe primero descargar las marcaciones del equipo biométrico a la computadora, presionando download attendance logs (descargar registros de asistencia). El biométrico solo toma la huella y la almacena, nada más; el software es quien toma esos registros y los tabula.

Ya con esta información descargada procedemos a seleccionar report (reporte)

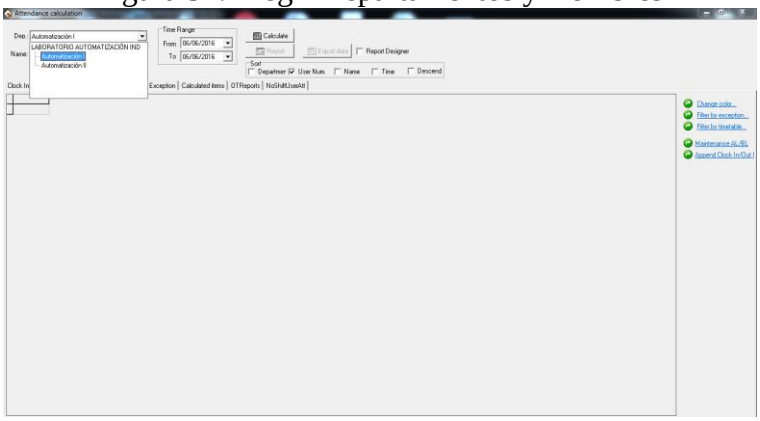
Figura 51. Descargar Reporte



Fuente: Autores

Nos da a elegir de donde queremos el reporte, de todos los departamentos, o de uno solo y si de un usuario o varios si fuese el caso.

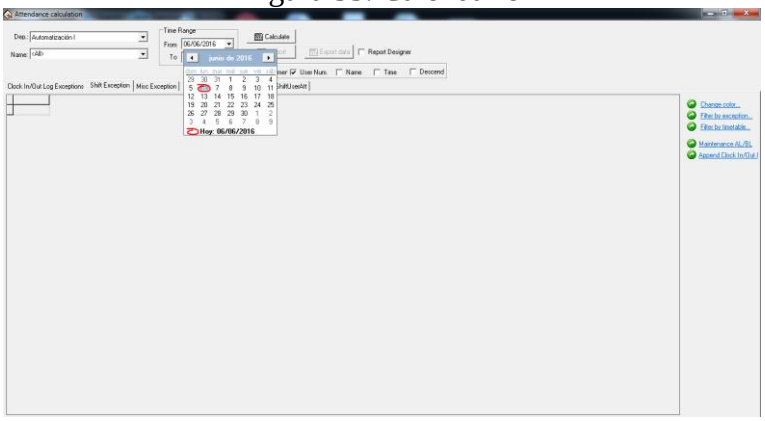
Figura 52. Elegir Departamentos y Nombres



Fuente: Autores

Seleccionar el rango de fechas puede ser diario, semanal, mensual, etc.

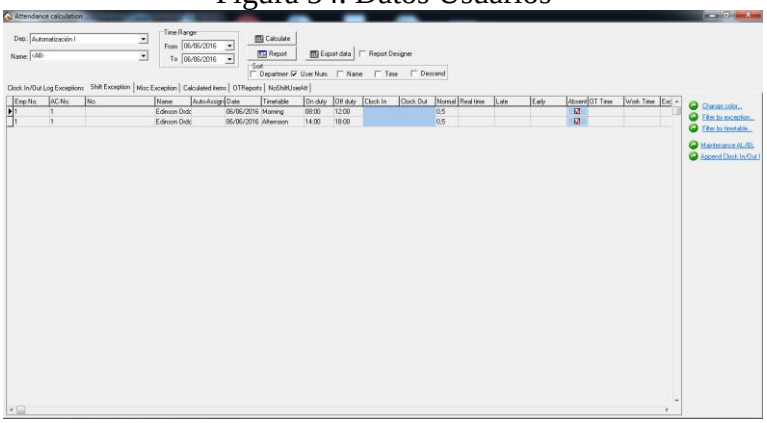
Figura 53. Calendario



Fuente: Autores

Presionar en calculate (calcular). En el mismo aparecen las marcaciones del usuario, nos muestra el AC no, nombre, fecha, horario.

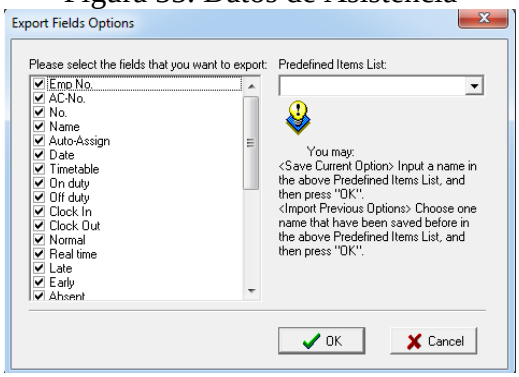
Figura 54. Datos Usuarios



Fuente: Autores

Al final para sacar el reporte en un documento de Excel, presionar en export data (exportar datos).

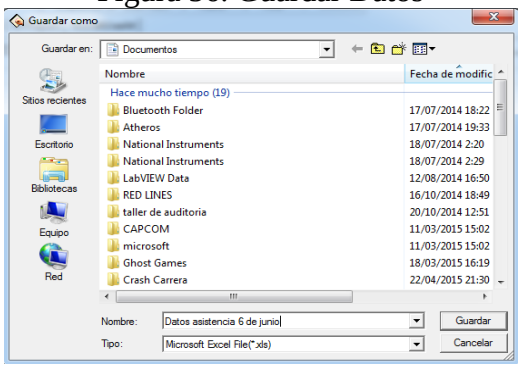
Figura 55. Datos de Asistencia



Fuente: Autores

Guardar datos en el computador los datos.

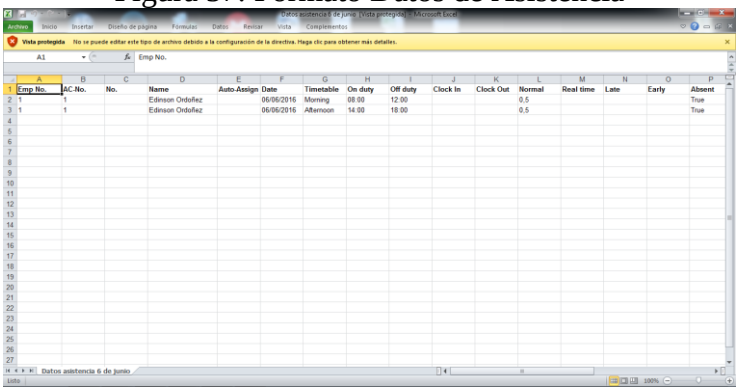
Figura 56. Guardar Datos



Fuente: Autores

Formato de cómo se descarga el archivo de Excel al computador.

Figura 57. Formato Datos de Asistencia



Fuente: Autores

4.2 Medición y monitoreo

Las principales mediciones que se efectuaron en la Implementación del Sistema de Seguridad y Control de Asistencia Biométrico, para el laboratorio de automatización de procesos industriales en la Escuela de Ingeniería Industrial-ESPOCH son las siguientes:

- Comprobar la correcta conexión de los equipos y que no existan cables expuestos, para garantizar un correcto funcionamiento del sistema y salvaguardar la integridad física de las personas que ingresen al laboratorio.

- Que el usuario asimile y se familiarice con la utilización de un sistema electrónico para la identificación de su identidad física.

- Se monitorice la actividad dentro del laboratorio, por seguridad tanto de las personas como de los bienes.

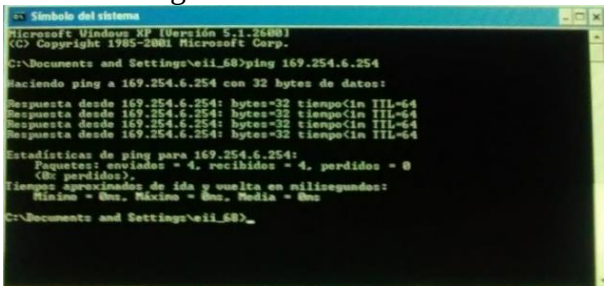
- Se resguarde los instrumentos, equipos y enseres pertenecientes al laboratorio, mediante el acceso controlado hacia el mismo.

4.3 Pruebas y resultados del sistema

4.3.1 *Pruebas del sistema CCTV.* Se verifica la correcta conectividad de las cámaras del NVR y del router.

Pruebas de funcionamiento. Para verificar que las cámaras estén correctamente conectadas se accede mediante un computador a la red por medio del CMD en donde se escribe el comando ping (IP de la cámara), cuando exista comunicación se visualiza.

Figura 58. Interfaz CMD



Fuente: Autores

Para el monitoreo de las cámaras se visualiza las figuras 54 y 55, cuando no presenten ningún problema.

Figura 59. Monitoreo cámaras día

Fuente: Autores

Figura 60. Monitoreo cámaras noche

Fuente: Autores

4.3.2 *Pruebas del sistema de control de acceso.* Ingreso de nuevo usuario.

4.3.2.1 *Interfaz del usuario.* La interfaz principal de estudiantes muestra la hora y fecha e indica que se debe poner la huella para ingresar.

Figura 61. Pantalla Inicio Biométrico

Fuente: Autores

Al colocar la huella se permitirá el respetivo acceso.

Figura 62. Acceso Correcto

Fuente: Autores

Caso contrario dirá intente de nuevo.

Figura 63. Acceso Incorrecto

Fuente: Autores

4.3.2.2 *Interfaz del usuario administrador*. Comprende todos los formularios que permiten gestionar el sistema.

El primer paso es iniciar sección con una cuenta previamente asignada como administrador.

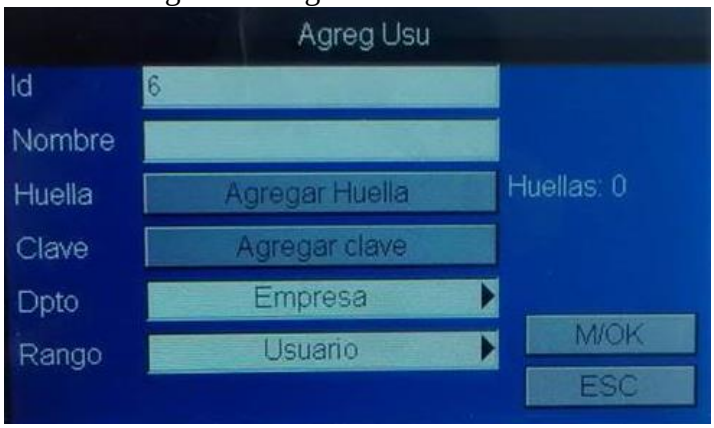
Al iniciar sección modo menú principal primero se debe mantener pulsado el botón de menú luego pide la huella del administrador y el sistema despliega un menú que le permite administrar todo el sistema en cuanto a lo que es registras, borrar usuarios y asignar horarios.

Figura 64. Menú Dispositivo Biométrico

Fuente: Autores

Para registrar nuevos usuarios la interfaz va a salir, donde sale el número de registro, nombre de usuario, huella (donde se puede registrar dos dedos), clave, departamento y rango donde se puede configurar si se asigna usuario o administrador.

Figura 65. Ingreso Nuevo Usuario



Fuente: Autores

4.4 Apagado del Sistema

Observación. Procure poseer la llave de la cerradura electro-mecánica (para uso de la parte mecánica), puesto que una vez apagado el sistema; se desactivan el cerrojo electro-magnético y el dispositivo de acceso biométrico.

- El sistema debe apagarse correctamente a fin de no causar daños en los equipos. Esto se debe realizar con el fin de efectuar el mantenimiento preventivo.

- Apague el NVR primero desde el sistema operativo, es decir visualizando la pantalla en el monitor. Luego desde el botón de "encendido/apagado" que se encuentra en la parte posterior.

- Apagar el dispositivo biométrico, desde la parte frontal del mismo.

- Desconecte los cables de alimentación de las cámaras y NVR, las cuales están conectadas en el UPS.

- Apague el UPS del botón de "encendido/apagado" ubicado en la parte frontal del dispositivo y desconecte el UPS de la alimentación principal de energía.

- Antes de volver a encender el sistema, asegúrese de que se han conectado todos los cables de alimentación al UPS. Encienda el UPS y los respectivos dispositivos.

4.5 Plan de mantenimiento del sistema

4.5.1 *Mantenimiento al Dispositivo "NVR".* Revisión de conexiones y limpieza.

4.5.1.1 *La limpieza exterior.* Se la realizamos con un paño seco.

4.5.1.2 *Para la limpieza interior.* Se debe abrir el NVR para hacer la limpieza interior de polvo acumulado y además de una revisión de los circuitos internos que contiene.

- Apagamos el dispositivo desde el monitor y luego desde el botón situado en la parte posterior izquierda del mismo.

- Desconectamos los cables de alimentación de energía y de datos respectivamente.

- Desmontamos la tapa con la ayuda de un destornillador Phillips.

Figura 66. Destornillar NVR

Fuente: Autores

- Una vez abierto con un paño seco limpiamos la base de lámina sin tocar la “placa electrónica”.

Figura 67. Interior NVR

Fuente: Autores

- Para la limpieza de la placa electrónica remover el polvo con una brocha de cerdas suaves y pequeñas, posteriormente “sopletear” con una lata de aire comprimido para remover cualquier suciedad atrapada en ella. Si se usa el compresor de aire, se recomienda secar con una sola pasada usando un secador de cabello.

- Una vez limpio internamente el “NVR” procedemos a colocar la tapa, atornillar y volver a ubicar en la caja de protección.

- Para volver a ponerlo en funcionamiento conectamos el cable de datos, el de transmisión de video y finalmente el cable de alimentación de energía.

4.5.2 *Para dar mantenimiento al cableado y cajas protectoras*. Tomar las precauciones necesarias para realizar el "trabajo en altura".

Figura 68. Caja de Derivación

Fuente: Autores

- Para verificar la toma de energía eléctrica y las terminaciones respectivas del cable de transmisión de datos de las cámaras. Desmontar con cuidado la tapa de la caja de derivación.

- Una vez abierta, realizar la limpieza de la caja de derivación; dicho elemento debe estar libre de polvo para el correcto flujo de energía y transmisión de datos.

Figura 69. Caja de Derivación Cargador

Fuente: Autores

4.5.3 *Para dar Mantenimiento a la Cámara*

La cámara es un elemento sensible debido a sus componentes internos:

Para darle un mantenimiento preventivo, primero desconectamos de la fuente y de la conexión de la transmisión de datos.

- Limpiamos exteriormente el polvo con la ayuda de un paño seco.
- Si se aloja polvo en el interior del visor, desmontar cuidadosamente girándolo.
- Una vez limpia la cámara volvemos a conectarla al cable de transmisión de datos y luego a la toma de energía.

CAPITULO V

5. COSTOS

Para la implementación de la tesis se consideraron las mejores ofertas de los dispositivos a instalar, por supuesto sin dejar de lado la calidad, eficiencia y tecnología. Los Costos directos corresponden a los elementos que influyen directamente en la instalación, y los Costos Indirectos a los asignados a materiales y recursos secundarios.

5.1 Costos Directos

Tabla 5. Costos directos

Ítem	Denominación	Unidad	Precio [USD]
1	UPS	1	89,00
2	NVR 4 canales	1	435,68
3	Cámara IP tipo bullet	3	265,44
4	Equipo control de acceso	1	200,00
5	Chapa Magnética	1	75,04
6	Chapa Eléctrica	1	88,00
7	Cable Ethernet	40 metros	32,00
8	Extensión de cable 10M	3	25,62
9	Puerta metálica	1	240,00
10	Caja	1	35,00
11	Caja de paso 10x10x7	2	10,48
12	Canaleta 20x12	12	31,20
13	Cable flexible # 10	10 metros	8,00
14	Pulsador	1	3,00
Total			1588,46

Fuente: Autores

5.2 Costos indirectos

Tabla 6. Costos indirectos

Ítem	Denominación	Precio [USD]
1	Materiales e imprevistos	450,00
Total		450,00

Fuente: Autores

5.3 Costos totales

Tabla 7. Costos totales

Ítem	Denominación	Precio [USD]
1	Costos directos totales	1588,46
2	Costos indirectos totales	450,00
Total		2038,46

Fuente: Autores

CAPÍTULO V

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Se implemento un sistema de seguridad y control de asistencia biométrico para el Laboratorio de Automatización de Procesos Industriales.

Se verifico la secuencia de ingreso al laboratorio por medio de un biométrico más el control de seguridad por medio de cámaras.

Se realizó la implementación por medio de un biométrico X300 que es basado en huellas dactilares, y el sistema de seguridad por medio de unas cámaras ZKteco.

Se verifico que la tecnología para el ingreso por medio de un biométrico es precisa y robusta, que no es fácil burlarla.

Además, cuenta con un UPS para que en el caso que se valla la electricidad los elementos no se dañen.

6.2 Recomendaciones

En lo posible NO desconectar el UPS de la toma-corriente, porque se apagan todos los dispositivos; en caso de hacerlo, procure tener a mano la llave del cerrojo electro-mecánico.

En lo referente al enrolamiento de los usuarios se recomienda que se use el dedo índice y/o anular, puesto que el dedo pulgar es susceptible de accidentes, Además el acceso biométrico permite el registro de dos huellas por cada cliente.

Revisar periódicamente las conexiones de los cables Ethernet al router.

Preferentemente el registro de usuario que utilice el laboratorio se descargue el administrador.

BIBLIOGRAFÍA

BORJA, César Tolosa y BUENO, Álvaro Giz. 2009. Sistemas Biométricos. 2009, Vol. I.

CORTÉZ, Germán Alexis Cortés. 2013. 10 consejos para comprar la UPS de su sistema de seguridad. *Seguridad Electronica en Latinoamerica.* [En línea] 08 de Mayo de 2013. http://www.ventasdeseguridad.com/.

DOMINGUEZ, Hugo Martín y VACAS, Fernando Sáez. 2006. *Un enfoque sociotécnico.* Madrid : Fundacion Rogelio Segovia, 2006.

GARCÍA Cruz, Ricardo Daniel, y otros. 2007. UPS. *Fuentes de Poder de Computadoras.* [En línea] 1 de Septiembre de 2007. https://grupo1t1.wordpress.com/.

GARCÍA, Javier Ortega, FERNÁNDEZ, Fernando Alonso y BELMONTE, Rafael Coomonte. 2008. *Biometria y seguridad.* Madrid, España : Fundacion Rogelio Segovia, 2008.

GARCÍA, Juan López. 2009. Algoritmo para la identificación de personas basado en huellas dactilares. *Algoritmo para la identificación de personas basado en huellas dactilares.* [En línea] 08 de Septiembre de 2009. http://upcommons.upc.edu/bitstream/handle/2099.1/8082/proyecto%20final%20de%20carrera.pdf?sequence=1.

GONZÁLES, Juan Carlos, y otros. 2009. *Tecnologias Biométricas aplicadas a la seguridad en las organizaciones.* Lima, Peru : Facultad de Ingeniería de Sistemas e Informática, 2009. Vol. VI.

KIMALDI. 2002. Control de Acceso biometrico y RFID. *Kimaldi.* [En línea] 12 de Julio de 2002. http://www.kimaldi.com/.

LACIE. 2013. Libro blanco biométria. Estados Unidos : Seagate, 2013, Vol. I.

PÉREZ, Pablo, y otros. 2011. *Estudio sobre las tecnologías biométricas aplicadas a la seguridad.* España : Creative Commons, 2011.

REDOLFI, Lusiano. 2013. *Domotica.* Argentina : Fox andina, 2013. Vol. 1.

SAS, SEGURIDAD Y EQUIPOS. 2015. Circuito Cerrado de Televisión, Biometria. *Seguridad y Equipos de Alta Tecnoligia.* [En línea] 17 de Septiembre de 2015. http://seguridadseat.com/.

TECNOTRONICA. 2015. Circuito cerrado de televisión. *Circuito cerrado de televisión.* [En línea] 20 de Octubre de 2015. http://tectronika.com/.

TORRES CASIMIRO, Rolando Manuel. 2013. *Papiloscopia.* Peru : Policia nacional del Peru, 2013.