UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

TEMA:

SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE IRIS PARA EL INGRESO DE PERSONAL A LA EMPRESA ELECTROSERVICIOS QUERUBÍN DE LA CIUDAD DE PUYO

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Electrónica y Comunicaciones.

SUBLÍNEA DE INVESTIGACIÓN: Sistemas Embebidos

AUTOR: Pérez Lescano Hugo Vinicio

TUTOR: Ing. Altamirano Meléndez Santiago Mauricio, Mg.

Ambato-Ecuador

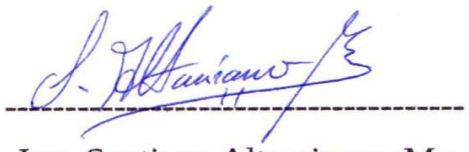
Agosto 2018

APROBACIÓN DEL TUTOR

En mi calidad de tutor del Trabajo de Investigación sobre el tema: "***SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE IRIS PARA EL INGRESO DE PERSONAL A LA EMPRESA ELECTROSERVICIOS QUERUBÍN DE LA CIUDAD DE PUYO"***, del señor **PÉREZ LESCANO HUGO VINICIO**, estudiante de la Carrera de Ingeniería **ELECTRÓNICA Y COMUNICACIONES**, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato Agosto, 2018

EL TUTOR

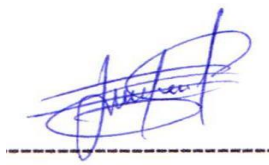


Ing. Santiago Altamirano, Mg.

AUTORÍA

El presente Proyecto de Investigación titulado: **SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE IRIS PARA EL INGRESO DE PERSONAL A LA EMPRESA ELECTROSERVICIOS QUERUBÍN DE LA CIUDAD DE PUYO**, es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato Agosto, 2018



Pérez Lescano Hugo Vinicio

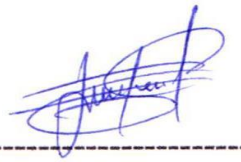
CC: 1600513970

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato Agosto, 2018



--

Pérez Lescano Hugo Vinicio

CC: 1600513970

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Jurado Lozada Marco Antonio, Mg. e Ing. Encala Ruiz Germán Patricio, Mg., revisó y aprobó el Informe Final del Proyecto de Investigación titulado "***SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE IRIS PARA EL INGRESO DE PERSONAL A LA EMPRESA ELECTROSERVICIOS QUERUBÍN DE LA CIUDAD DE PUYO***" presentado por el señor Pérez Lescano Hugo Vinicio, de acuerdo al numeral 9.1 de los Lineamientos Generales para la Aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ing. Mg. Elsa Pilar Urrutia Urrutia
PRESIDENTA DEL TRIBUNAL

Ing. Marco Antonio Jurado Lozada, Mg.
DOCENTE CALIFICADOR

Ing. Germán Patricio Encala Ruiz, Mg.
DOCENTE CALIFICADOR

DEDICATORIA

Esta tesis se la dedico a toda mi familia y seres queridos, a mi Padre Patricio Pérez por no rendirse jamás y forjarme como la persona que soy hoy en día, mis hermanos Diego y Patricio por apoyarme, alentarme y día a día darme fuerza para continuar, no hubiera podido lograr sin su confianza, consejos y aliento.

A la familia Aldás Cherrez grandes personas que agradezco infinitamente a Dios por ponerlas en mi camino ya que todo esto es posible por su continuo apoyo, la oportunidad de demostrar que pude, puedo y podre dar más de mi como persona y ahora como profesional.
Los amo Familia.

AGRADECIMIENTO

Primeramente agradecerle a Dios por mi familia, por rodearme de personas que desean mi bienestar, A mi Padre Patricio Pérez por su apoyo incondicional durante toda mi vida no me alcanzara la vida para agradecerle todo lo que hace por mí, sus enseñanzas desde que nací, el enseñarme a trabajar honradamente y que todo su esfuerzo tiene su recompensa.

A mi hermano Diego Pérez, mi amigo y confidente gracias por esta oportunidad que me has dado, sé que sacrificaste muchas cosas que deseabas con el único hecho que a mí nunca me faltara nada en la Universidad, estaré eternamente agradecido hermano y nunca olvidare que gracias a ti soy un profesional.

A mi hermano Patricio Pérez por sus palabras que me ayudaron a continuar y no desistir de mi objetivo, por todas las llamadas preguntando mi bienestar y sacrificios realizados para que Yo pudiera seguir estudiando.

A Erika Aldás mi ángel de la guarda, una persona de gran corazón a cual amo, respeto y agradezco por formar parte de vida y espero que siga así por el resto de mi existencia.

A Genoveva Cherrez gracias por la confianza, sus consejos y todas las habladas que terminaban en llanto sabiendo que todo va a estar bien, decirle ya tengo el cartón.

A mi novia Karen Aldás por acompañarme y estar junto a mí en los buenos y malos momentos apoyándome y dándome ánimos para continuar, sobretodo agradecerle por hacerme mejor persona Te Amo.

A mi tutor Ingeniero Santiago Altamirano por su paciencia, ayuda y guía en todo el proceso de elaboración de mi proyecto de Titulación.
Les agradezco a todos por creer en mí.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto detalla el diseño e implementación de un sistema de control de acceso por reconocimiento de iris para el ingreso de personal a la Empresa Electroservicios Querubín de la ciudad de Puyo, el mismo fue desarrollado partiendo de los problemas existentes en la empresa, debido a la falta de control al ingreso de personal, provocando pérdida de maquinaria embodegada por personas externas a la empresa, causando pérdidas económicas y un malestar general en la empresa en visto que todos resultan afectados, al no tener un control de acceso de personal, seguro y confiable.

El sistema cuenta con un sensor biométrico, de reconocimiento de iris, mediante el cual se realiza la autenticación para el registro del personal, permitiendo así el acceso a las instalaciones de la empresa, sin que existan confusiones al momento de identificar a las personas que laboran en la misma; la única forma de ingreso del personal es que el usuario se encuentre registrado en una base de datos del sistema de control de acceso.

El sistema posee una base de datos que permite almacenar la información de mayor relevancia correspondiente al usuario como son: nombres, apellidos, cédula de identificación y área designada de labores; para tener así una mejor seguridad, registrando a quienes ingresan a las instalaciones, gestionando dos niveles de acceso, que son: restringido y libre, para las diferentes áreas de la empresa.

Palabras clave: Acceso físico, biométrico, iris, identificación, base de datos.

ABSTRACT

The present research project details the implementation of an access control system for iris recognition for the entry of personnel to the Querubín Electroservices Company of the city of Puyo, this system was developed starting from the existing problems in the company, due to the lack of control over the entry of personnel, causing loss of machinery stored by people outside the company, causing economic losses and a general malaise in the company in view that all are affected, having no control of personnel access, insurance and trustworthy.

The system has a biometric, iris recognition sensor, through which authentication is performed for personnel registration, thus allowing access to company facilities, without confusion when identifying the people who work in the same; The only way for staff to enter is for the user to be registered in a database of the access control system.

The system has a database that allows to store the most relevant information corresponding to the users such as: names, surnames, identification card and designated area of work; to have a better security, registering those who enter the facilities, managing two levels of access, which are: restricted and free, for different areas of the company.

Keywords: Physical access, biometric, iris, identification, database.

INTRODUCCIÓN

En la actualidad a nivel mundial la demanda de control de acceso por medio de sensor biométrico se ha incrementado enormemente en los últimos años, teniendo de este modo distintas tecnologías que van desde sistemas detectores de firmas hasta detectores de patrones únicos en partes de los ojos como en el iris o retina. Según la Asociación Internacional de Identificación Biométrica, las tecnologías más utilizadas en los sistemas de control de acceso son: reconocimiento de huellas dactilares múltiples con un 38.3%, autenticación por huella digital única con un 28.4% y reconocimiento facial con un 11.4%. Es por eso que diferentes entidades sean públicas o privadas optan por estar al día con la tecnología en sistemas de autenticación, implementando un control de acceso de personal, con el objetivo de impedir el ingreso de entes no autorizados a diferentes áreas, brindando registro, identificación y evitando suplantaciones de personal.

En el presente proyecto se implementa un sistema de control de acceso por reconocimiento de iris para el ingreso de personal a la Empresa Electroservicios Querubín de la Ciudad de Puyo. El sistema identifica a los usuarios registrados en una base de datos y permite el acceso de forma única a los que tienen un nivel de acceso autorizado, registrando los intentos de acceso sean exitosos o no; el acceso de un usuario hacia la bodega de la empresa es controlado por un identificador de iris.

El trabajo consta de cinco capítulos, los cuales se describen brevemente a continuación:

En el primer capítulo, se da a conocer los motivos por el cual es necesario el desarrollo de esta investigación, con el análisis y planteamiento del problema, la justificación del porque se realiza el sistema, planteando así objetivos que conduzcan

el desarrollo del sistema de control de acceso por reconocimiento de iris para el ingreso de personal a la empresa Electroservicios Querubín de la ciudad de Puyo.

En el segundo capítulo, se detalla los aspectos teóricos para identificar las distintas formas de acceso de personas, con diferentes sensores biométricos existentes hasta la actualidad y la propuesta con la cual se dará solución al problema planteado.

En el tercer capítulo, se especifica la metodología, el tipo de investigación, recolección de la información y las actividades que se desarrollaron para la elaboración del proyecto de investigación.

En el cuarto capítulo, se explica de manera detallada el diseño e implementación del sistema de control de acceso por reconocimiento de iris para el ingreso de personal a la empresa Electroservicios Querubín de la ciudad de Puyo.

En el quinto capítulo, se indica las conclusiones y recomendaciones adquiridas al finalizar el proyecto.

CAPÍTULO I

EL PROBLEMA

1.1 TEMA

"*Sistema de Control de Acceso por Reconocimiento de Iris para el Ingreso de Personal a la Empresa Electroservicios Querubín de la Ciudad de Puyo*"

1.2 PLANTEAMIENTO DEL PROBLEMA

La seguridad en establecimientos públicos o privados comienza con un buen control de accesos de personal. La planificación de ingresos a áreas restringidas dentro de una empresa, ahonda en criterios dirigidos hacia la seguridad de bienes y personas, por lo tanto es trascendental resaltar la importancia de coordinar, el diseño del control de acceso con el proyecto constructivo de las instalaciones. En el último año alrededor del mundo se han registrado numerosos casos de ingresos ilegales a empresas y hogares con finalidades de robo, teniendo cifras que van desde los 21.140 ingresos para el caso de Colombia, hasta 1.1 millones de ingresos registrados en Estados Unidos, mostrando que el acceso a las instalaciones privadas es de baja seguridad [1].

Lo principal en un sistema de control de acceso de personal dentro de distintas empresas, es mantener un registro que indica las operaciones de verificación y acceso. En Ecuador menos del 40% de las empresas tienen implementado un sistema electrónico de control de acceso o un sistema de control de asistencia laboral, reflejando un bajo nivel de seguridad para las mismas. En los últimos 5 años se han

registrado hasta 18.168 casos anuales de robos o ingresos ilegales a hogares oempresas, teniendo un promedio de hasta 15.000 registros anuales en la última década [1].

Otro punto importante es la integración de sistemas de control de acceso, puesto que efectivamente este crecimiento en la infraestructura da la facilidad de compartir recursos en cuánto a diferentes sistemas electrónicos de seguridad, básicamente en identificación y sistemas de control de acceso ya que se optimizan recursos humanos y materiales al momento en que no se requiere de redes independientes porque éstas se empiezan a convertir en un sistema globalizado, lo cual evidentemente requiere cierta capacitación para que el personal pueda utilizarlo sin inconvenientes. El sistema de control de seguridad de personal en entidades, empresas y negocios con numeroso personal, que se ha implementado a nivel nacional, utiliza la tecnología tradicional (Chapas Eléctricas, tarjetas RFID, sistemas de acceso por clave) [2].

La Empresa Electroservicios “QUERUBÍN” es una entidad que se encuentra sometida a la aplicación de normas de solvencia, prudencia financiera, contable y al control directo de la Gerencia. En la actualidad la empresa está ubicada en la Provincia de Pastaza, ciudad de Puyo, en las calles Francisco de Orellana y General Villamil, la misma cuenta con 16 trabajadores distribuidos en áreas de administrativas, de contabilidad, servicio técnico entre otras. El control de acceso de personal se realiza por medio de un guardia ubicado en la entrada de las instalaciones de la empresa, de forma tradicional sin una identificación estricta, únicamente de forma visual.

El sistema de seguridad utilizado actualmente en la empresa Electroservicios Querubín, para la verificación del acceso y control de personal, se basa únicamente en el monitoreo de empleados y clientes, por medio de cámaras de seguridad instaladas en diferentes lugares estratégicos de la empresa. En la empresa no se tiene un control de acceso estricto, autorizando el ingreso a las diferentes áreas de forma única al personal identificado por guardias de seguridad, provocando inconvenientes para reconocer al personal que ha ingresado sin autorización; a causa de los errores

de naturaleza humana.

En la actualidad debido a la falta de un sistema de control de acceso más seguro y de alta gama, la empresa ha sido víctima de una cantidad no identificada de robos de maquinaria y suministros eléctricos ubicados en las instalaciones de la empresa, denominada mercadería embodegada, generando en el año 2017 pérdidas económicas valoradas aproximadamente en 2700 dólares, ya que sin ninguna dificultad personas ajenas a las instalaciones, o empleados de áreas diferentes a las designadas, tienen facilidad de acceso.

1.3 DELIMITACIÓN

Área: Física y Electrónica
Línea de investigación: Sistemas Electrónicos
Sublínea de investigación: Sistemas Embebidos

Delimitación Temporal:
El proyecto de investigación se desarrolló en el periodo Agosto 2017 – Agosto 2018 de acuerdo a lo establecido en el Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Delimitación Espacial:

La investigación se desarrolló en la empresa Electroservicios Querubín de la Ciudad de Puyo.

1.4 JUSTIFICACIÓN

Los sistemas de control de acceso de personal por reconocimiento de iris, brindan seguridad, rigidez, confiabilidad, tranquilidad y calma. Todas estas características ayudarán a la Empresa Electroservicios Querubín ubicada en la ciudad de Puyo, a mantener un control rígido en el acceso de personal a sus instalaciones. Siendo estrictos en el permiso de ingreso y manejando la seguridad con un sistema de control de acceso, que garantice la identificación de los usuarios, para que el personal

que se encuentre dentro de determinadas zonas de la empresa, sea el autorizado por Gerencia.

En la actualidad la empresa antes mencionada no cuenta con un sistema de control de acceso automatizado y electrónico, debido a los antecedentes delictivos no identificados acontecidos en la empresa, que han provocado una pérdida considerable de mercadería sustraída de la bodega, Electroservicios Querubín encuentra necesaria la implementación del sistema de control de personal para sus instalaciones.

Los sistemas de control de acceso son la tecnología con más demanda en el mercado actual, se ha migrado de sistemas mecánicos y con personal especializado, a tener procesos de control de entrada y salida completamente automatizados con diferentes tipos de tecnologías y dispositivos. Es importante realizar un estudio adecuado, segmentando las zonas, los grupos de acceso, los horarios permitidos, el nivel de acceso de cada usuario, medir la cantidad de personas o carros que transitan por cada zona y establecer claramente los objetivos de cada control de acceso [2].

El presente proyecto será implementado con tecnologías alámbricas de bajo costo que utiliza un sistema de reconocimiento biométrico capaz de proporcionar en tiempo real identificación, tanto en el movimiento como en la distancia además se conecta a través de tecnologías de integración con todas las plataformas existentes haciéndolo factible, fiable y escalable, para obtener un prototipo de bajo costo y de libre acceso para los operarios de empresas y entidades que requieran de un sistema de control de acceso de personal, ayudando a mejorar su eficiencia, al tener tecnología actual es un reemplazo ideal para los sistemas tradicionales utilizados en la actualidad. Del mismo modo que el prototipo es lo suficientemente potente para utilizarse en diferentes estaciones de trabajo que requiera un sistema de control de acceso de un nivel más alto.

Por lo anteriormente expresado, el presente proyecto es factible para su implementación en la Empresa Electroservicios Querubín, debido a su gran interés en adquirir el sistema de control de acceso, por necesidad, tecnología utilizada y bajo

costo, además en un futuro las entidades y empresas pueden adoptar el sistema de control de acceso de personal por reconocimiento de iris en sus instalaciones.

1.5 OBJETIVOS

1.5.1 Objetivo General

Implementar un prototipo de Sistema de Control de Acceso por Reconocimiento de Iris para Ingreso de Personal a la Empresa Electroservicios “QUERUBÍN” de la ciudad de PUYO.

1.5.2 Objetivos Específicos

- Analizar los parámetros técnicos de los sistemas de control de acceso de personal utilizados en la actualidad.

- Seleccionar la tecnología y equipos electrónicos adecuados a ser utilizados en el sistema de control de acceso por reconocimiento de iris para personal.

- Diseñar un prototipo de control de acceso por reconocimiento de iris para el ingreso de personal.

CAPÍTULO II

MARCO TEÓRICO

2.1 ANTECEDENTES INVESTIGATIVOS

Alrededor del mundo se han desarrollado numerosos sistemas de control de acceso para personal, utilizando tecnologías de radiofrecuencia o sistemas biométricos, y según el avance tecnológico en el que se encuentre cada país, este tipo de sistemas se ha hecho muy popular, implementándose dentro de empresas o residencias. De tal forma, existen trabajos y proyectos que buscan crear un sistema fiable, escalable, robusto, confiable y de bajo costo para el control de acceso y autentificación a partir de patrones biométricos como el reconocimiento de huellas dactilares, geometría de mano o iris.

En el país no se encuentra en ningún repositorio de proyectos o investigaciones relacionadas con el control de acceso de personal por reconocimiento de Iris, sin embargo se han desarrollado sistemas que utilizan otro tipo de reconocimiento y en otros países se han realizado investigaciones que detallan métodos de reconocimiento de iris; los que se detallan a continuación:

Zynnia Verónica Vargas Vergara en el año 2013 en Guayaquil-Ecuador, desarrolló un proyecto de investigación con el tema “Sistema de Control de Acceso y Monitoreo con la Tecnología RFID para el Departamento de Sistemas de la Universidad Politécnica Salesiana Sede Guayaquil”, en donde el acceso al laboratorio se realiza de forma controlada, permitiendo el ingreso solo al personal autorizado. En el

proyecto se utiliza un módulo de identificación inalámbrica, RFID (Radio Frequency Identification) con el fin de controlar al personal. El software de gestión es desarrollado en LabVIEW y mediante una comunicación UDP con un módulo lector RFID, se identifica una etiqueta electrónica a distancia. Con el control de acceso se evita la pérdida de equipos o se identifica a los responsables del extravío de los mismos, generando ahorros económicos a la universidad con la reposición [3].

Justo Javier Saavedra Guada en Sartenejas en el año 2016 en Venezuela, desarrolló un proyecto de investigación con el tema “Diseño e Implementación de un sistema de Control de Acceso para la Empresa Seebeck de Instrumentación y Control C.A.” El Sistema está basado en un controlador embebido que posee un CPU Am188ES, controlando de forma autónoma el acceso de personas a distintas zonas, mediante la apertura de cerraduras electrónicas, el mecanismo funciona a través de tarjetas de identificación por Radio Frecuencia (RFID), procesa el número de identificación comparándolo con una base de datos, verificando atributos a puertas de acceso, debido a que la empresa no cuenta con un sistema de acceso automatizado para sus clientes [4].

Daniel Alejandro Cadena Moran y Luis Guillermo Romero Sánchez en el año 2011 en Sangolquí-Ecuador, realizaron un proyecto de tesis con el tema “Diseño e Implementación de un Sistema de Control e Inventario Electrónico a través de la Internet basado en la Tecnología RFID para los laboratorios del DEEE-ESPE”, el cual utiliza como hardware el microcontrolador PIC 18F97J60 ya que dispone de un módulo de comunicación Ethernet. De forma complementaria se utiliza el lector RFID ÍD-20 para registrar los “tags” de los usuarios, debido a la inexistencia de un sistema de seguridad para tener un control de acceso de usuarios a los laboratorios de las instalaciones de DEEE-ESPE [5].

Jorge Alberto Alvarado Sánchez en el año 2008 en México, desarrolló un “Sistema de Control de Acceso con RFID”, en el proyecto de investigación se utilizó la tecnología de autoidentificación inalámbrica por radio frecuencia, la que consiste de etiquetas que almacenan información codificada para que los lectores puedan leerlas

e identificarlas a distancia. Se optó por esta tecnología debido a su bajo costo y mayor capacidad de funcionamiento, teniendo la facilidad de instalar equipos RFID en red, separados hasta en 1km de distancia, ya que el sistema utiliza un bus de datos con el protocolo RS-485 [6].

Álvaro Javier Balsero Meneses y Cristian Germán Vargas García en el año 2016 en Bogotá-Colombia, proponen un “Diseño e Implementación de un Prototipo para el Control de Acceso en la Sede de Ingeniería de la Universidad Distrital Francisco José de Caldas mediante el uso de torniquetes controlados por carnet con Tecnología NFC y Lector Biométrico de Huella Dactilar”, el control de acceso incorpora tecnologías mejoradas de comunicación e identificación de datos, como es NFC (Near Field Comunication), un sistema que optimice y tecnifique de manera general el ingreso de la comunidad universitaria a las instalaciones, debido a que existía congestión y su estándar de seguridad era bajo. Utilizando reconocimiento biométrico como lo es el lector de huella dactilar enlazado a tecnología NFC, implementada en un carnet de identificación personalizado, aumentando los estándares de seguridad para el control de acceso de funcionarios y estudiantes a las instalaciones [7].

Jorge Eduardo Velásquez Valencia, Álvaro Andrés Linares Jaramillo en el año 2013 en Pereira-Colombia, plantean “Soluciones Inteligentes para el Control de Acceso Físico Mediante el uso de Tecnología Biométrica”, el sistema permite la autenticación y verificación de ingreso de personal a las distintas áreas a las cuales se encuentren autorizados, por medio de dispositivos programables (FPGA’s y sistemas embebidos) se puede obtener una solución óptima para controlar el acceso a residencias e instalaciones [8].

Juan José García Garrigos en el año 2006 en Valencia-España, presenta un “Sistema de Autenticación Biométrica de Huella Dactilar asistido por Interfaz de Voz para el Control de Accesos”, el proyecto realizado para la Empresa Fermax Electrónica S.A.E., sistema electrónico para el control de acceso basado en autentificación biométrica de huella dactilar, facilitando el acceso a inmuebles de los usuarios, los cuales registraran sus huellas para poder ser autenticados posteriormente, únicamente

desplazando su dedo sobre un lector de huella dactilar para poder abrir la puerta, autentificando como usuario autorizado, por la falta de seguridad, ya que existe un nivel bajo de control de acceso, evitando duplicados de otros objetos (llaves) [9].

Jaime R. Michilena C., Estefanía G. Torres A. en el año 2012 en Ibarra-Ecuador, proponen un "Sistema Electrónico para Control de Acceso de Personas por Reconocimiento de Huella Dactilar, con Autenticación Remota en Base de Datos a través de una WLAN", el mismo que utiliza el software AVR STUDIO para la programación de microcontroladores AVR en lenguaje C y ensamblador, el simulador Proteus para la depuración de errores, proporcionando una solución de seguridad integrada, permitiendo la entrada de personas en un punto de acceso [10].

Jorge Enrique Gutiérrez Ricardo en el año 2007 en Bogotá-Colombia, desarrolló el "Estudio de Factibilidad para el Control de Acceso Biométrico, en una Empresa Empleando Lectores de Huella Digital". El control de acceso emplea un lector de huella digital, compuesto por una base de datos, motor de búsqueda, reconocimiento y validación de los usuarios al acceso, haciendo imposible las suplantaciones de identidad y el acceso a personas no autorizadas a la entidad, ya que el control de acceso de personas se lo hacía manualmente es decir con la supervisión de un vigilante, lo cual no presenta fiabilidad y control robusto y confiable [11].

La revista Computación y Sistemas en el año 2012 publica un artículo con el tema "*Avances en el Reconocimiento de Iris: Perspectivas y Oportunidades en la investigación de Algoritmos Biométricos*", el artículo científico realiza un análisis de la evolución y tendencias en la tecnología de reconocimiento de iris de los humanos, evidenciando para la fecha de investigación, la necesidad de implementar algoritmos de reconocimiento de alta fiabilidad, automatizados e inteligentes. Demuestra que la tecnología de mayor impacto utilizada para el reconocimiento de iris es la explotación de información con el vídeo-iris, mostrando sistemas con cámaras integradas a una misma función, trabajando en red, con el propósito de reconocer a más de un sujeto por segundo en ambientes abiertos. Finalmente se proyecta que el avance intelectual en el campo de detección de iris, permitirá en un futuro cercano,

obtener sistemas de video vigilancia con reconocimiento de individuos [12].
En la Universidad Tecnológica de Pereira-Colombia en octubre de 2014 se presenta el trabajo de investigación de un *"Sistema de Lectura y Análisis de Iris"*, el proyecto utiliza el software Matlab para realizar el procesamiento digital de las imágenes. El proceso de reconocimiento se realiza a partir de una imagen fotográfica del ojo, con la que, mediante los métodos de conversión a escala grises y sauvola, se determina las coordenadas centrales del iris. Al agregar límites superiores e inferiores a las coordenadas polares del centro del iris se obtiene un recorte de la imagen, la misma que se transforma a coordenadas rectangulares y de forma posterior es estirada para analizar los patrones de luminosidad mediante un histograma, el mismo que guarda la información para el reconocimiento del iris [13].

En la Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, en el año 2014, se presenta una tesis de ingeniería con el tema: "*Evaluación y Mejora de un Sistema de Reconocimiento de Iris a Distancia Utilizando Cámara de Alta Resolución*". En la memoria técnica presentada se realiza un estudio de diversos proyectos diseñados para fortalecer e incrementar la fiabilidad de los sistemas de reconocimiento de iris. En el método utilizado se desarrollan distintos algoritmos de clasificación de características, generando una base de datos de imágenes de distintos rostros mediante una cámara de alta resolución, con el fin de evaluar el reconocimiento de iris a distancia [14].

De los resultados obtenidos del proyecto de investigación se determina que el rendimiento de la identificación por medio de la textura del iris decae de forma dramática debido a que el iris absorbe las longitudes de onda del espectro visible utilizado por la cámara, sin embargo al utilizar métodos combinados de codificación por Daugman y la implementación de mapas de pesos en la clasificación por color iridial y textura, entregan al sistema una taza de rendimiento que está alrededor del 90%, acercándose al rendimiento de los sistemas de iluminación infrarroja [14].

En la Universidad Autónoma de Madrid-España, Escuela Politécnica Superior, en el año 2008 se presenta un proyecto de fin de carrera titulado: "*Reconocimiento*

Automático de Patrones de Iris". La investigación realizada se enfoca en el estudio de las características que permiten identificar a las personas en base a patrones específicos de la estructura ocular, de forma específica, del iris. El proyecto resume que la metodología utilizada de forma general por los sistemas de reconocimiento de iris, basan su funcionamiento en tres etapas: pre-localización de la ubicación del iris en la imagen capturada, identificación de los bordes circulares que limitan el anillo del iris y la normalización y codificación de la información entregada por el iris; para generar el patrón del mismo. En un sistema de reconocimiento de iris, una parte importante es la velocidad de procesamiento, pues tras capturar la imagen, el usuario no puede esperar eternamente a recibir una respuesta. El sistema de reconocimiento implementado es bastante rápido, realiza la segmentación y codificación en un promedio de 4, segundos en un computador que opera con Matlab [15].

2.2 FUNDAMENTACIÓN TEÓRICA.

2.2.1 Sistemas de Control de Acceso de Personal.

Un Sistema de Control de Acceso de Personal es un conjunto de elementos electrónicos que permiten o evitan el ingreso de un usuario a un área específica. La identificación es validada por medio de diferentes tipos de lectura como: procesos biométricos, clave por teclado o tarjetas de proximidad; utilizados por controladores que generan señales eléctricas, permitiendo el accionamiento de mecanismos de seguridad como: electro-imanes, cantoneras, pestillos o motores; que bloquean la apertura de puertas, torniquetes o talanqueras [16].

Los sistemas de control de acceso de personal en empresas, entidades y diferentes instalaciones, son herramientas de última tecnología que permite a quienes lo poseen obtener un control y seguridad en el ingreso de personal. La fusión e integración adecuada de diferentes dispositivos electrónicos, permite reducir los costos de componentes de seguridad, y a su vez el ahorro de personal encargado de la supervisión de ingreso; de esta forma se reduce los costos variables de la entidad, considerando que se tiene un solo pago inmediato por sistema y que los gastos de mantenimiento preventivo o correctivo del sistema, son inferiores a salarios

permanentes del personal de seguridad [2].

2.2.2 Gestión de Control de Acceso

La gestión del control de acceso es un sistema implementado como una medida de seguridad física, necesaria para adoptar y establecer grupos de personas con niveles de autorización para acceder a determinadas zonas [17].

La gestión de acceso concede a usuarios autorizados el derecho a utilizar un servicio y deniega el acceso a los no autorizados, en ésta gestión se manejan los siguientes conceptos básicos:

- **Acceso.-** Es el nivel y alcance de la funcionalidad de un servicio o área que un usuario está autorizado a utilizar.
- **Identidad.-** Es la información que define el dominio de las personas reconocidas por la organización.
- **Derechos.-** Es la configuración real de un usuario en la cual se indica los servicios o grupos de servicios que se autoriza utilizar o áreas a las que las personas pueden acceder [18].

Todos los tipos de control de acceso se basan en otorgar permisos a las personas que pretenden acceder o moverse por un edificio o una zona determinada de éste. Los sistemas de control de acceso son utilizados en diferentes aplicaciones como: el acceso de entrada a un recinto o edificación, a zonas y estancias de alta seguridad en las que se custodian objetos de alto valor y a zonas de trabajo peligrosas o con altas probabilidades de ocurrencia de accidentes [19].

2.2.3 Políticas del Control de Acceso.

Las políticas de control de acceso son normas y procedimientos utilizados para identificar las medidas de seguridad física que se deben implementar y establecer los permisos para los diferentes grupos de usuarios. El acceso o la limitación del mismo en distintas organizaciones utilizan múltiples niveles de control, desde el acceso a la propiedad, pasando por el acceso a áreas determinadas del edificio y a continuación a

funciones, equipos o salas específicas [17].

Las instalaciones deben tener un plano de distribución actualizado que documenta las áreas restringidas, las medidas de seguridad y los lugares en dónde se han implementado dichas medidas. Los dispositivos de control de acceso se instalan en todas las entradas y salidas garantizando que solo el personal autorizado acceda a las áreas restringidas. Las políticas de control de acceso incluyen y delimitan los siguientes elementos:

- Determinan las áreas restringidas y los grupos de personas para las que se crean las restricciones.
- Especifican los tipos de controles de acceso que se deben utilizar.
- Determina circunstancias en las que se permite el acceso a las áreas restringidas.
- Especifica un método de monitoreo del control de acceso.
- La gestión de acceso debe verificar todas las solicitudes de acceso a un servicio o área clasificada como restringida.
- Registrar y monitorear el estado de identidades y las peticiones de acceso; los roles de los usuarios cambian con el tiempo afectando los derechos de acceso.
- El sistema de control de acceso debe permitir la revocación o limitación de derechos [17] [18].

2.2.4 Sistemas de Alarma.

Un sistema de alarma es un elemento de seguridad que no evita un problema (intrusión, incendio, inundación, fuga de gas, etc.) pero que sí tiene la capacidad de advertirlo, permitiendo la rápida actuación sobre el problema para disminuir los posibles daños a producirse [20].

Los sistemas de seguridad y alarma tienen gran importancia, siendo los equipos antitrusión y contra incendios los que más interés generan entre los propietarios de los bienes inmuebles. Los sistemas de alarmas tienen conexiones de entrada para los

dispositivos detectores y por lo menos una de salida para activar equipos de alerta como sirenas o luces. De forma alternativa a las conexiones de salida, se utilizan distintas operaciones como: de llamar a un número, abrir el rociador o cerrar las puertas que se ejecutan de forma manual por un operador o automática por el sistema [20].

Los equipos de alarma están conectados a una Central Receptora, utilizando un medio de comunicación, como: una línea telefónica RTB o una línea GSM, un transmisor por radiofrecuencia llamado Trunking, transmisión TCP/IP que utiliza una conexión de banda ancha ADSL y últimamente servicios de Internet por cable o Cable Módem [20].

2.2.5 Tipos de Control de Acceso.

Los tipos de control de accesos de acuerdo al área de cobertura se dividen en: Sistemas Autónomos y Sistemas en Red.

Los sistemas de control de acceso de personal, representan la tecnología con más demanda en el mercado para seguridad de áreas restringidas; el desarrollo tecnológico ha trabajado con sistemas mecánicos y con personal especializado, hasta llegar a tener procesos de control completamente automatizados, con diferentes tecnologías y dispositivos [2] [16]. Así la selección del tipo de sistema a instalarse depende del ámbito de trabajo, a continuación se especifica las características principales de los dos tipos de sistemas mencionados.

a) Sistemas de Control de Acceso Autónomos

Los Sistemas de Control de Acceso Autónomos son un conjunto de componentes que permiten controlar la apertura de una o más puertas, sin estar conectados a un computador o a un controlador central. Los sistemas autónomos no guardan registros de eventos, siendo ésta la principal desventaja ya que cuando permite el acceso a un usuario no almacena la fecha, ni la información que identifique al mismo; algunos controles de acceso autónomos tampoco pueden limitar el acceso por horarios o por grupos de puertas. En otras palabras, éstos sistemas solo usan el método de

identificación, ya sea por: clave, proximidad o bibliometría como una "llave" electrónica [16].

b) Sistemas de Control de Acceso en Red

Los Sistemas de Control de Acceso en Red son un conjunto de componentes que se integran a través de un computador o controlador local o remoto, donde se hace uso de un software de control para llevar un registro de todas las operaciones realizadas sobre el sistema con fecha, horario, autorización, etc. [16].

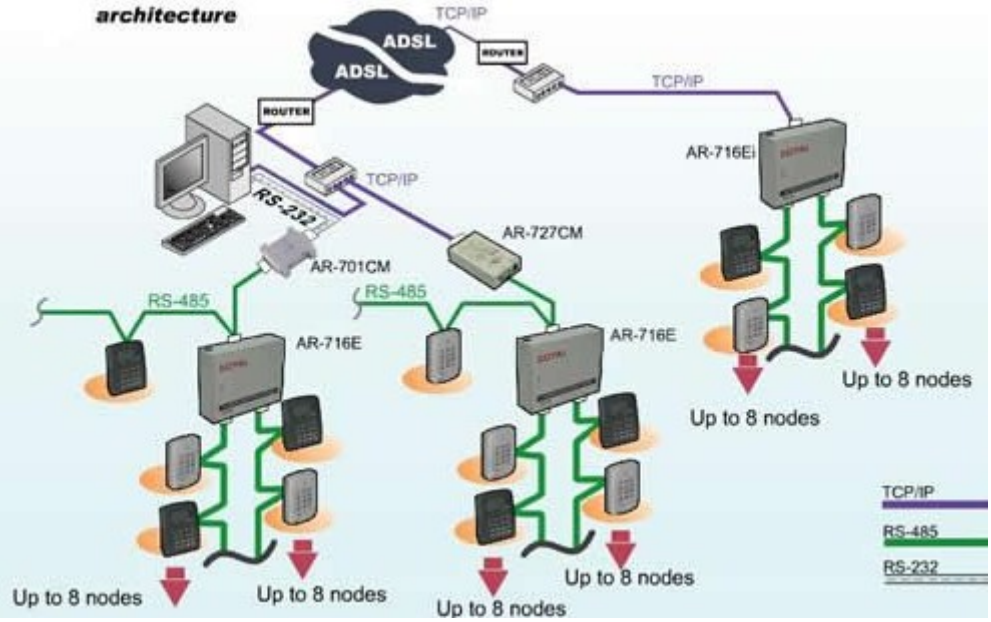


Fig.2. 1: Estructura de un Sistema de Control de Acceso en Red [16]

En la Fig.2. 1 se observa una estructura de un Sistema de Control de Acceso que funciona en Red, los dispositivos se organizan en nodos, en donde cada nodo contiene los equipos que controlan el acceso a áreas específicas.

La comunicación entre cada nodo y el dispositivo central se realiza mediante diferentes protocolos de comunicación de acuerdo al nivel en que se encuentre el mismo; pasando desde RS-485 o RS-422 para el control de dispositivos en el área local, RS-232 para la comunicación entre los nodos de un área local y el computador central, hasta el protocolo Ethernet para el control de nodos de área extensa o

remotos [16].

2.2.6 Componentes de un Control de Acceso.

Los componentes de un Sistema de Control de Acceso son dependientes del tipo de sistema utilizado, teniendo en cuenta que, de forma mínima un sistema debe satisfacer el acceso controlado mediante los conceptos simbólicos de: la puerta, la cerradura y la llave. Los elementos fundamentales de un Control de Acceso Automático, con conexión a un ordenador en red son: lector o terminal, credencial, servidor, controlador, mecanismo de apertura, elementos de alimentación [21] [22].

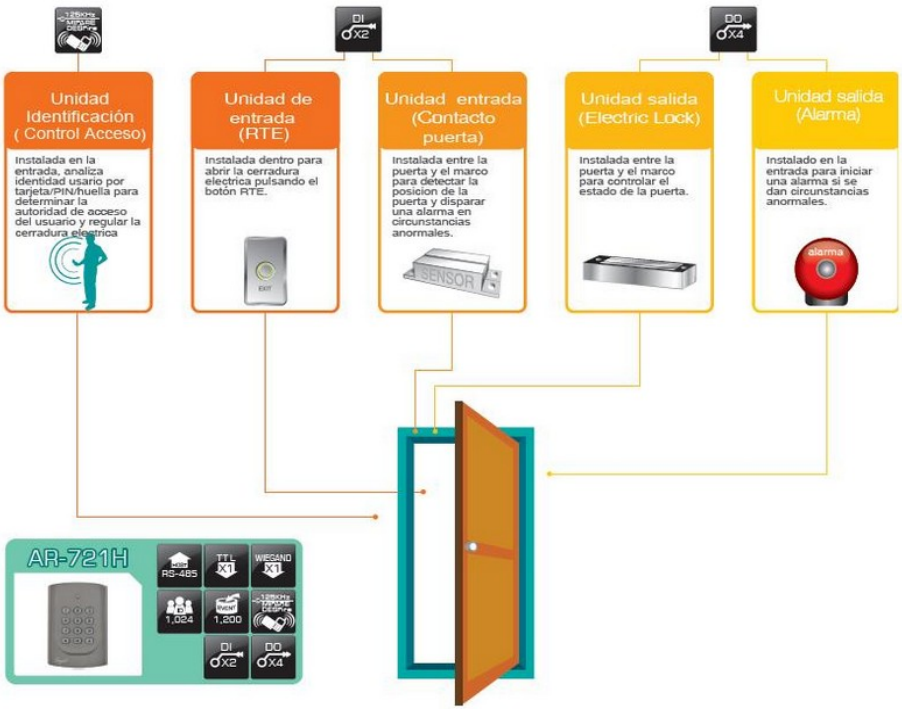


Fig.2. 2: Elementos de un Sistema de Control de Acceso.[22]

En la Fig.2. 2 se observa los elementos de un Sistema de Control de Acceso, en donde, la unidad de identificación está comprendida por el lector y credencial, la unidad de entrada es el mecanismo de apertura, y el controlador con los elementos de alimentación deben instalarse en un gabinete de seguridad [22].

a) Lector /Terminal

El lector o terminal es el equipo que procesa la información para identificar a la persona que desea obtener el acceso. Éste se comunica con una credencial y envía su información al controlador para verificar si el usuario tiene permiso de acceso, en el caso de sistemas autónomos la verificación se realiza en el mismo terminal, no necesita comunicarse con el controlador o computador central [21].

b) Credencial

La credencial es un mecanismo que identifica a un usuario, de la misma se obtiene información para verificar el permiso de acceso a las zonas permitidas. Puede definirse como algo que una persona posee, sabe o es, tales como: tarjetas, códigos, parámetros biométricos de seguridad, entre otros [21].

c) Servidor

El servidor es un computador encargado de almacenar la información referente a los elementos del sistema de control de acceso como: usuarios, niveles de acceso, puertas; también almacena información de eventos del sistema como: intento de acceso, sea exitoso o no, señales de alarma, entre otros. Es la unidad donde se ejecutan las instrucciones de los programas llevando un registro de todos los eventos presentados en el sistema. Los sistemas autónomos no requieren de un servidor para funcionar, éstos almacena la información de forma directa en el terminal [21].

d) Controlador

El controlador es el único elemento encargado de decidir las acciones sobre los mecanismos de apertura, permitiendo o denegando el acceso a los usuarios, mediante funciones programadas por zonas, horarios o niveles de acceso. Los demás elementos solo generan información o ejecutan acciones. El controlador se comunica con el servidor, en donde se concentra la información del sistema en general, consultando en cada intento de registro la información de configuración y programación, como la de eventos producidos. Con la información obtenida el

controlador ejecuta las acciones correspondientes, como apertura de puertas o informes de alertas de seguridad [21].

e) Mecanismos de Apertura

Los mecanismos de apertura son elementos de seguridad, que mediante señales eléctricas bloquean o permiten la apertura de puertas. Cuando el controlador determina que el usuario tiene permiso de acceso, envía señales eléctricas a éstos dispositivos, los que permiten el ingreso de una persona, mediante la activación o desactivación de contactos magnéticos o cerraduras eléctricas, dependiendo de la aplicación [21].

f) Elementos de Alimentación

Los elementos de activación, son circuitos electrónicos que generan un acondicionamiento de tensiones y corrientes eléctricas para energizar todos los componentes del sistema de control de acceso. Los elementos electrónicos que forman parte de un sistema de control de acceso se energizan a diferentes voltajes, por lo que es necesario utilizar elementos que alimenten dichos dispositivos de una manera independiente. Además se debe garantizar el funcionamiento del sistema por un periodo determinado en el caso de cortes de energía eléctrica [21].

2.2.7 Tecnologías de Auto-identificación

a) Sistemas de Acceso por Proximidad

Los sistemas de acceso por proximidad trabajan con tecnología inalámbrica de autoidentificación por radiofrecuencia permitiendo identificar de forma automática un objeto, gracias a una onda emisora transmitida por radiofrecuencia desde el mismo. Los objetos utilizan sistemas activos o pasivos para difundir la onda electromagnética. En los sistemas activos las etiquetas de RFID utilizan una fuente de poder integrada que genera la señal de radio frecuencia, mientras que en los sistemas pasivos se utiliza las características de la inducción electromagnética, para generar la señal RF de identificación.

En un sistema de control de acceso por proximidad el usuario no mantiene contacto físico con los equipos, teniendo como consecuencia un menor desgaste de los mismos en comparación a tecnologías invasivas [21].

En este tipo de sistema, observado de forma esquemática en la Fig.2. 3, el lector siempre inicia la comunicación leyendo los objetos de identificación como: pulseras, llaveros o tarjetas; que se encuentran a distancias de unos centímetros. Ésta tecnología utiliza micro-controladores integrados con comunicación Ethernet, RS-232 o RS-485, además cuenta con un software para almacenar los registros que identifican las tarjetas en una base de datos [3] [5].

Fig.2. 3: Sistema de Control de Acceso por RFID [5].

Las etiquetas RFID son diseñadas para distintas aplicaciones, teniendo así en el mercado etiquetas con variaciones en su forma física, características de alimentación, almacenamiento de datos, frecuencia de funcionamiento o tipo de comunicación[21].

De acuerdo a la frecuencia de funcionamiento, por mencionar dos tipos muy importantes de las etiquetas en sistemas de control de acceso por proximidad, se tiene: Etiquetas transponder que trabajan a una frecuencia de 125kHz, utilizadas para servicios que no requieren más de un dato. Etiquetas mifare con una frecuencia de operación de 13.56MHz, las que permiten almacenar información con la que es posible crear diferentes servicios [21].

b) Sistemas de Acceso por Clave

Los sistemas de acceso por clave funcionan en base a la captura de una contraseña, o clave de acceso, la que se entrega al dispositivo de control a través de un teclado numérico o alfanumérico como se indica en la Fig.2. 4.

Los usuarios poseen un único código de identificación, que será utilizado para acceder a los lugares a los que tienen permiso. Éstos sistemas de forma general son económicos, pero su desventaja es que el nivel de seguridad es bajo, ya que las personas registran en libretas, agendas o elementos de apoyo de memoria, las claves para no olvidarlas, perdiendo de esta forma toda la confidencialidad objetiva de esta tipología [21].

Fig.2. 4: Sistema de Control de Acceso de Teclado [21].

c) Sistemas de Tarjetas Magnéticas.

Los Sistemas de Control de Acceso de Tarjetas Magnéticas, funcionan mediante dispositivos fabricados en base de PVC o Polyester como las mostradas en la Fig.2. 5, en la que se encuentra una banda magnéticamente codificada. Al pasar la banda magnética por un lector especializado a ellas, se descifra su código, y si se trata de un código válido se envía la señal eléctrica que permite la apertura de la puerta [21][23].

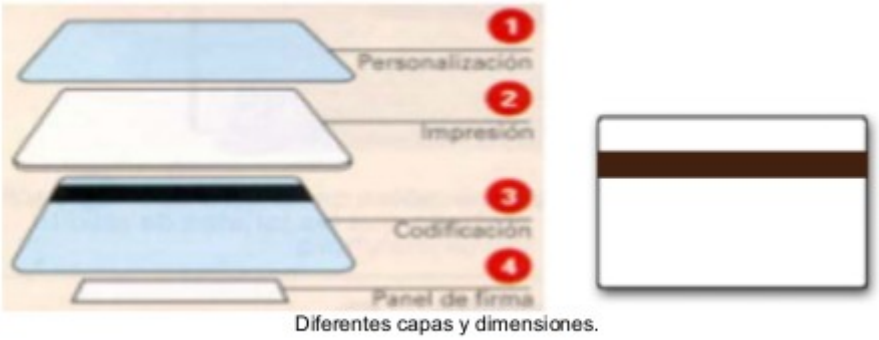


Fig.2. 5: Tarjetas codificadas magnéticamente [23].

Los sistemas de control de accesos que funcionan con tarjetas magnéticas tienen varias ventajas como: son sistemas de bajo costo, de tiempos prolongados de vida y de acceso rápido; que utilizan una tecnología ya probada, en donde el duplicado de las tarjetas tiene un nivel de dificultad, . Sin embargo éstos equipos están sujetos a problemas como la pérdida de la información de la banda magnética debido a la fricción en la lectura de las tarjetas o la exposición de las mismas a campos electromagnéticos fuertes [21].

d) Código de Barras.

Los sistemas de control de accesos que funcionan con código de barras, utilizan una tarjeta de aspecto similar a la tarjeta de banda magnética, cambiando la banda, por un código de barras impreso sobre ella, el que puede incluso ser resguardado con una banda protectora para evitar la duplicación de la tarjeta por fotocopias [21].

El código de barras es una imagen de líneas negras y espacios en blanco diferentes grosores, impresas en paralelo, que contienen información codificada. La ventaja es que al pasar la tarjeta por el lector no existe rozamiento, solo hay un haz de luz que lee el código en cuestión, con lo cual su vida útil es aún mayor y son baratas. Además, la impresión tiene un bajo coste y la personalización y codificación es sencilla y se puede realizar bajo demanda. Sin embargo su principal desventaja es que no admite que se rayen, ya que de esa manera se altera el código, además son

fácilmente falsificables, siendo esto un gran problema para un sistema estricto de control de acceso [21].

e) Tarjetas Inteligentes

Las tarjetas inteligentes son esquelas rectangulares fabricadas en plástico, PVC o Polyester, las mismas que contienen un microprocesador como se muestra en la Fig.2. 6. Éstas tarjetas tienen la capacidad de realizar pequeños cálculos, manejar programas y guardar información [23].

Es importante distinguir entre una tarjeta inteligente y una tarjeta con chip, ya que éstas son de apariencia similar a las indicadas en la Fig.2. 5, sin embargo en una tarjeta con chip convencional el circuito integrado no es un microprocesador, sino una memoria, siendo ésta la única diferencia. Las tarjetas con chip de memoria y con microprocesador se dividen en tarjetas de contacto y sin contacto.

Fig.2. 6: Apariencia de una tarjeta inteligente o con chip [23]

Las tarjetas inteligentes son utilizadas en aplicaciones financieros como sistemas de pago o sistemas que contienen información para accesos o intercambio de datos [23].

2.2.8 Sistemas de Reconocimiento Biométricos

Los sistemas de reconocimiento biométricos son sistemas caracterizados por reconocer algún parámetro físico o de comportamiento de un usuario para identificarlo de forma única e inequívoca, determinando o verificando su identidad. Los seres humanos de forma general tienen características morfológicas únicas que las distinguen de otras personas, como por ejemplo: huella dactilar, iris, geometría de

la mano, características faciales, tono o frecuencia de la voz, entre otras [21].

El proceso de autenticación utilizado de forma general es, en primera instancia los lectores biométricos leen y capturan las imágenes digitales o analógicas a analizar mediante mecanismos automáticos, de forma posterior, de acuerdo a la base de datos de los lectores y a las funciones del sistema se agrega información a la base de datos o se establece una decisión determinando si el usuario es válido o no [21] [23].

La exactitud de un equipo biométrico es medida a través de dos parámetros porcentuales que son el falso rechazo y la falsa aceptación. La falsa aceptación es el hecho de permitir el acceso a una persona no registrada en la base de datos del sistema. En cambio el falso rechazo es un proceso en el que se niega el acceso a una persona registrada en la base de datos, estas situaciones suelen suceder cuando las personas han sufrido algún incidente provocando un cambio temporal que influye en algún parámetro característico de la lectura [21].

Los sistemas biométricos funcionan en base a reconocimientos para “volver a conocer” a un usuario que ya fue registrado de forma previa. La autenticación se realiza de dos maneras diferentes identificación y verificación. La primera es la comparación de la muestra recogida de la persona con todos los registros de una base de datos de rasgos biométricos, este método requiere de un alto tiempo de proceso, puesto que se debe comparar la muestra con cada registro anteriormente almacenado, determinando una coincidencia. El sistema de verificación utiliza la identificación del usuario mediante un ÍD, tarjeta u otro método; así, se selecciona de la base de datos el patrón registrado para dicho usuario, y compara la característica biométrica obtenida con la almacenada, siendo éste un proceso simple [21].

Con referencia a los sistemas de control de acceso convencionales, los sistemas biométricos tienen algunas ventajas y desventajas, las que se detallan a continuación:

Ventajas:

- La autenticación por rasgos biométricos no requieren memorización de datos

por parte del usuario, garantizando que la persona tenga un acceso constante.

- El medio de identificación es personal y único.
- Los rasgos biométricos no pueden ser robados, facilitando obtener una seguridad jurídica, almacenando registros de ingresos con la identidad del usuario.
- El uso de sistemas biométricos es simple, seguro y cómodo.
- Integración y escalabilidad sencilla con sistemas ya existentes.
- No se puede realizar registros por los compañeros.

Desventajas:

- Son sistemas costosos.
- El tiempo de autenticación es mayor.
- Tienen menor resistencia al vandalismo en comparación a sistemas de tarjetas, debido a la sensibilidad de los sensores que utilizan.
- No tienen precisión absoluta.

Los Sistemas de Control de Accesos Biométricos utilizan distintas características físicas de las personas, así, dependiendo del tipo de característica se encuentran en el mercado sistemas con las siguientes tecnologías de reconocimiento de biometría:

a) Huella Dactilar

La huella dactilar de un individuo es un patrón único formado por el tejido de las células epiteliales de los dedos, éste patrón determina la identidad de un individuo de una forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni entre familiares o entre dedos de la misma persona.

En la tecnología de reconocimiento de huellas dactilares como se muestra en la Fig.2. 7, los sistemas toman una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos, y es de esta imagen normalizada que se extrae las minucias (remolinos de la huella), que compara con las que se encuentran en la bases de datos. El reconocimiento automático se puede enlazar con diferentes tecnologías, integrando un sistema rápido y ágil que permite optimizar el proceso de ingreso a entidades, logrando seguridad y fiabilidad. Éstos sistemas

permiten un mayor flujo de entrada y un nivel de seguridad mayor, teniendo control y verificación del personal que ingresa, eliminando guardias que soliciten un carnet para permitir el acceso [7] [8] [10].

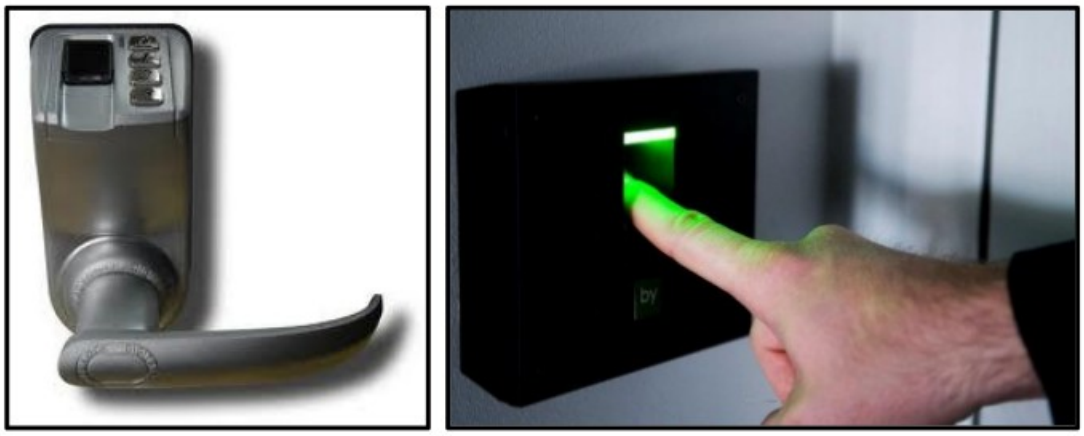


Fig.2. 7: Sistema de captura y registro y comparación de huellas dactilares [21].

La tecnología de captura digital de huellas dactilares utiliza métodos ópticos y capacitivos. En el método óptico, el usuario apoya el dedo sobre un punto de vidrio en donde un dispositivo proyecta una luz y la imagen es capturada por medio de un dispositivo de carga acoplada (CCD). En el método capacitivo los sistemas analizan el dedo por medio de la detección de campos eléctricos alrededor del dedo, utilizando sensores y circuitos integrados [23].

Las ventajas que presenta un sistema que utiliza huellas dactilares son que éstas son únicas y permanentes durante toda la vida para cada dedo de cada individuo, son de uso sencillo, utilizan espacios reducidos, son sistemas de bajo costo y no invasivos. Sin embargo éstos sistemas requieren de una elevada calidad de imagen digital y contacto físico, además está sujeta a temas penales [21].

b) Geometría de Mano

La autenticación de usuarios por medio de la geometría de la mano fue una de las primeras tecnologías utilizadas en sistemas de identidad, en este método se crea una imagen tridimensional de la mano en la que se analiza sus características como: las medidas de la mano, longitud de los dedos, la curvatura, áreas y posiciones relativas

de los dedos y nudillos, entre otras, los equipos utilizados en estos sistemas se ilustran en la Fig.2. 8 [21].

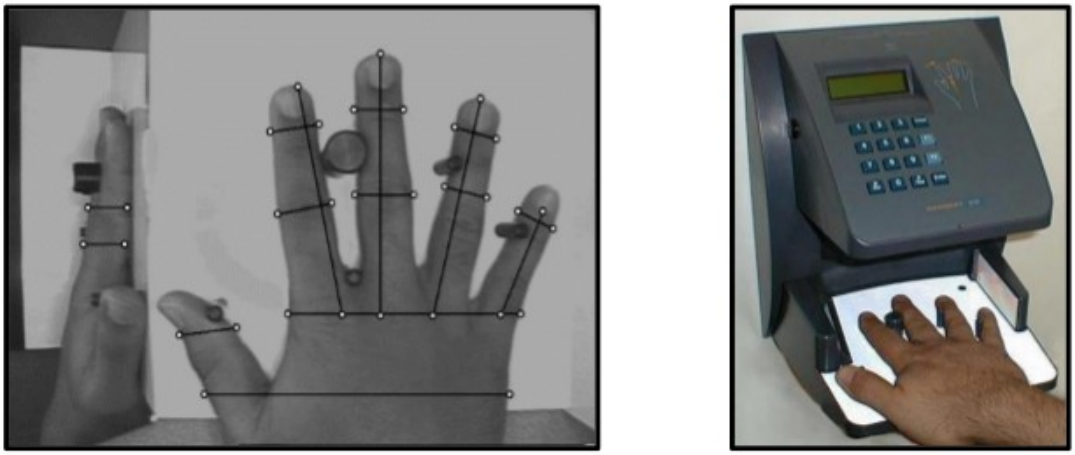


Fig.2. 8: Sistema de captura y registro y comparación de geometría de la mano [21].

En los seres humanos, la geometría de la mano tiene una forma distinta y es poco variante con el tiempo. Para la captura de la geometría de la mano, ésta es apoyada en una superficie en donde mediante una cámara digital se recoge un modelo descriptivo para comparar con los registros del sistema [21] [23].

Entre las ventajas que presenta el uso de ésta tecnología se tiene que es de fácil captura, poco intrusivo y tiene un diseño estable a lo largo de la vida. Por otro lado éstos sistemas requieren de mucho espacio físico y entrenamiento [21].

c) Reconocimiento Facial

El reconocimiento facial es un método que se basa en identificar características de la cara como distancia de los pómulos, los lados de la boca, los perfiles de los ojos y la posición de la nariz. Éste método es poco invasivo, utiliza una cámara para tomar una foto a la cara y medir las distancias y proporciones entre los puntos que separan las partes exteriores e interiores de los ojos, boca y nariz, obteniendo de ésta manera una plantilla única para identificar a una persona con precisión, de la forma observada en la Fig.2. 9 [21].

Fig.2. 9: Sistema de captura y registro y comparación de reconocimiento facial [21].

Entre las ventajas de utilizar sistemas de reconocimiento facial se tiene los hechos de que son un método que no requieren contacto, son sistemas poco intrusivos, de fácil chequeo, máxima higiene y además aporta información adicional de los usuarios como estado de ánimo. Sin embargo en éstos sistemas el porcentaje de falso rechazo se incrementa debido al cabello suelto o posición de la cabeza, además el rostro es variante en el espectro temporal, el sistema es sensible a los cambios de luz y no es de alta fiabilidad [21].

d) Reconocimiento de Voz

El reconocimiento mediante interfaz de voz para usuarios, consiste en la capacidad de un dispositivo para reconocer comandos de voz a través de un micrófono, gracias a mensajes pregrabados que servirán de guía para el administrador. Ésta tecnología permite crear sistemas embebidos como los mostrados en la Fig.2. 10, dando como resultado mejor accesibilidad a inmuebles, garantizando un control de acceso un poco seguro, a cualquier persona autorizada al mismo.

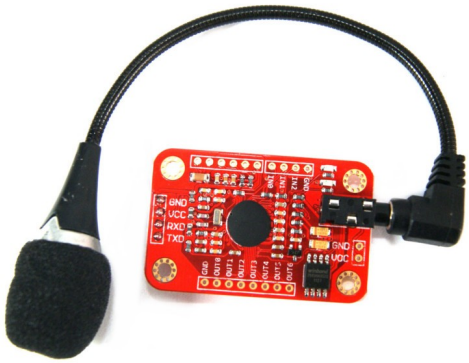


Fig.2. 10: Sistemas embebidos de reconocimiento de voz [9].

El reconocimiento de voz (Speech Recognition Processor Sand RESCUE-4128) consiste esencialmente en el proceso de interpretación de una palabra pronunciada por una persona, después de capturar la señal acústica que corresponde a la pronunciación de estas a través de un micrófono caracterizado por un transductor de voz de tipo omnidireccional o direccional.

La señal de voz digitalizada primero es transformada en un conjunto útil de características o medidas muestreadas a una frecuencia fija, se realiza tareas de procesado digital de la señal mediante el uso de microprocesadores o microcontroladores, empleando transformaciones de Fourier para extraer características de la señal obteniendo el espectrograma de la palabra [9].

f) Sistemas Combinados

Los sistemas combinados son sistemas que utilizan dos a más tecnologías de identificación ya sean convencionales o biométricos con la finalidad de incrementar el grado de confiabilidad que se busca para el sistema, siendo una solución para incrementar la protección en aquellas áreas en la que se quiera dotar de más seguridad. En cualquier caso es importante realizar un diseño adecuado para obtener la máxima seguridad sin comprometer el tiempo de autenticación.

2.2.9 Sistema de Reconocimiento de Iris.

Un sistema de reconocimiento de iris es un grupo de componentes integrados que buscan determinar patrones únicos de los seres humanos para crear procesos de autenticación.

El iris es una membrana muscular del ojo, ubicada enfrente del cristalino y detrás de la córnea, el mismo es único para cada individuo y tiene 200 rasgos individuales diferentes que se mantienen inalterables en el tiempo a menos que sufran heridas. La identificación se realiza por medio de un escaneo ocular efectuado por una cámara, convirtiendo la información de los rasgos en un código único, los equipos utilizados en éstos sistemas se visualizan en la Fig.2. 11 [21].

Entre los rasgos que permiten distinguir a los usuarios se encuentran surcos de contracción, huecos, estrías, fibras de colágeno, manchas y anillos negros. Debido a éstas opciones el reconocimiento de iris es un sistema de mayor fiabilidad en comparación a sistemas de huellas dactilares, teniendo una probabilidad de error de 10^{-78} .Conociendo que la población mundial estimada es de 10^{10} éste sistema es infalible [21].

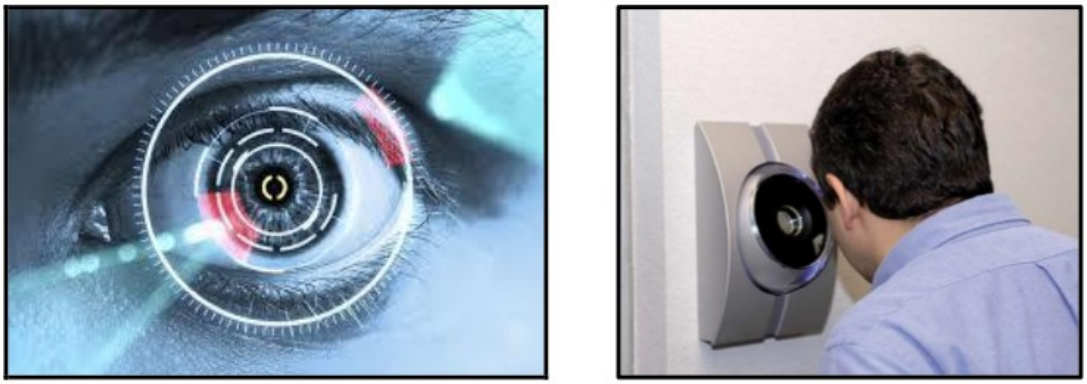


Fig.2. 11: Sistema de captura y registro y comparación de reconocimiento de iris o retina [21].

En estos sistemas la persona a identificarse tiene que mirar a través de unos binoculares, ajustando la distancia y ubicación entre el ojo y una cámara; mirando a un punto determinado. Dentro de este tipo de tecnologías existen sistemas que trabajan en función a fotografías, en los que el usuario debe especificar al dispositivo mediante un pulsador, que el ojo se encuentra en la posición correcta para realizar la captura; y otros de costos elevados que basan su funcionamiento en capturas y procesos de vídeo en donde la captura se realiza de forma automática [21] [24].

Entre los inconvenientes que presentan éste tipo de tecnologías se menciona la escasa aceptación de los usuarios, los equipos son altamente costosos y algunos de ellos son invasivos, además presenta problemas de reconocimiento con el uso de lentes de contacto [21] [24].

El proceso de reconocimiento de iris utilizado de forma genérica por la mayoría de sistemas es el indicado en el diagrama de bloques de la Fig.2. 12. La metodología

utilizada distingue 4 etapas en el tratamiento de datos para el reconocimiento de patrones en el iris, que son: la adquisición de imágenes, un pre-procesamiento en el que se realiza la segmentación y normalización de la imagen, la codificación y el reconocimiento en base a datos ya almacenados [25] [26].

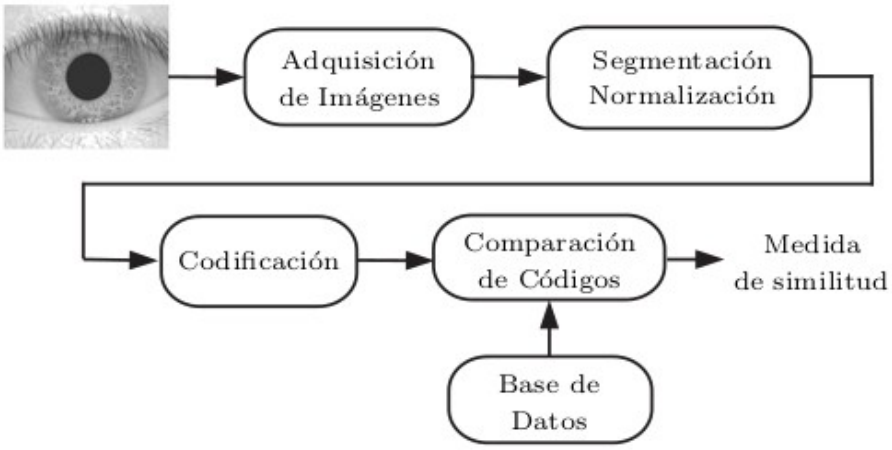


Fig.2. 12: Diagrama de bloques de un sistema de reconocimiento de iris [25]

La etapa inicial en el proceso de reconocimiento de iris es la adquisición de las imágenes, siendo una etapa de alta importancia debido a que el performance del sistema depende de la calidad de la imagen capturada, para este fin es recomendable que la fotografía cumpla las siguientes condiciones:

- La imagen del iris debe tener una resolución adecuada en cantidad de pixeles.
- El enfoque debe ser adecuado para distinguir los detalles del patrón del iris
- Tener un contraste alto con un nivel de iluminación adecuado para no generar molestias al usuario [26].

El iris es la región compuesta por la membrana coloreada y circular del ojo, comprendida entre la pupila y la esclerótica, observada en la Fig.2. 13. La región del iris puede ser modelada como dos círculos no concéntricos, el exterior representa el límite entre el iris y la esclerótica mientras que el interior es el borde formado por el iris y la pupila [26] [27].

En la etapa de pre-procesado se debe localizar el iris dentro de la imagen, detectando

los bordes exteriores e interiores y eliminando el ruido producido por las pestañas y párpados, teniendo de ésta forma una imagen segmentada [28]. El algoritmo propuesto para localizar las figuras geométricas correspondientes al sector del iris utiliza dos técnicas del procesamiento de imágenes: el operador de Canny, que genera un mapa de bordes permitiendo localizar el borde exterior del iris y la Transformada de Hough que identifica las curvas paramétricas [29] [30].

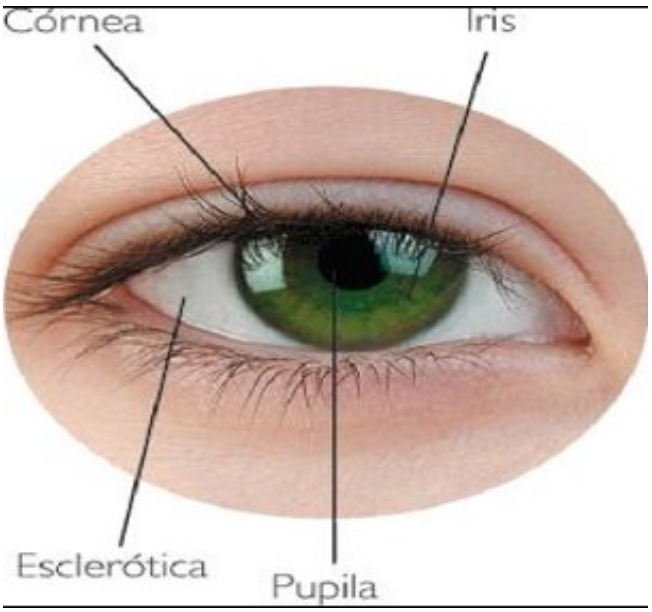


Fig.2. 13: Partes del ojo. Identificación del iris [27]

El borde interior del iris se localiza utilizando el reflejo producido por el sistema de iluminación en la pupila. La ubicación del reflejo se evalúa buscando una ventana que contiene circunscrito el borde exterior del iris, de la forma indicada en la Fig.2. 14 (b), generando una nueva imagen que contiene el reflejo con el borde interior del iris de la forma observada en la Fig.2. 14 (c).

Finalmente, con el operador de Canny y la Transformada de Hough se calcula los parámetros del círculo interno [26].

Los párpados son localizados utilizando el operador de Canny solamente en los bordes horizontales, y aplicando la Transformada de Hough para determinar los parámetros correspondientes. Las curvas segmento-lineales se buscan en una ventana

que circunscribe el iris, como el de la Fig.2. 14 (b), en dónde se utiliza la mitad superior y la mitad inferior para detectar los párpados de cada parte [25] [26].

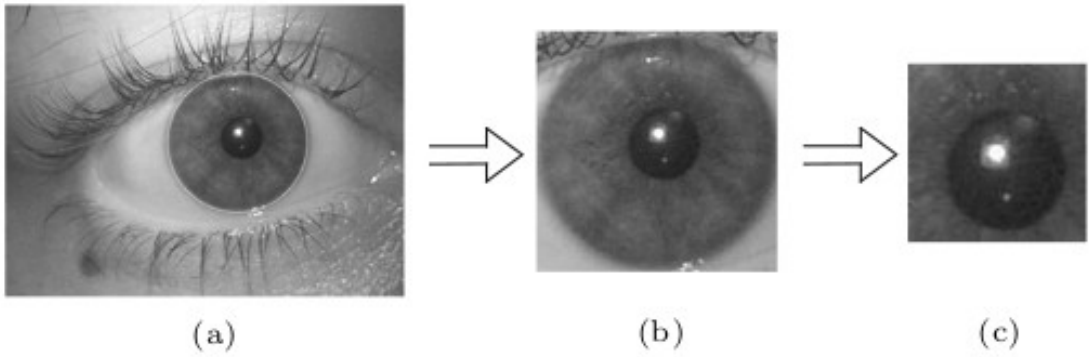


Fig.2. 14: Proceso de segmentación de la pupila. (a) Iris segmentado (b) Ventana del reflejo de la pupila (c) Recuadro sobre el reflejo[9].

De la imagen obtenida del proceso de segmentación se genera un nuevo perfil donde la región del iris es independiente del tamaño del mismo y permite compararlo con otros irises. La etapa de normalización produce que varias imágenes del mismo iris, adquiridas bajo diferentes condiciones, tengan las mismas características espaciales [26]. El algoritmo utilizado por la mayoría de sistemas para ejecutar la normalización se basa el método propuesto por Daugman, en el que cada punto dentro de la región del iris es reasignada a un par de coordenadas polares (r,θ) en donde θ es el ángulo y r es el radio acotado que toma valores entre 0 y 1. [15] [31].

La redistribución de las coordenadas cartesianas en el plano (x,y) de la región de iris a la representación polar no-concéntrica es modelada por medio de las ecuaciones 2.1 y 2.2 [15].

$$I(x[r,\theta], y[r,\theta]) \rightarrow I(r,\theta) \qquad 2.1$$

$$\begin{aligned} x(r,\theta) &= (1-r)\,x_p(\theta) + r x_l(\theta) \\ y(r,\theta) &= (1-r)\,y_p(\theta) + r y_l(\theta) \end{aligned} \qquad 2.2$$

En dónde $I(x,y)$ es la región de la imagen que contiene el iris, el par ordenado

(x, y) son las coordenadas cartesianas originales, (r, θ) son las coordenadas polares normalizadas correspondientes, y x_p , y_p , x_l y y_l son las coordenadas de los límites de la pupila y el iris a lo largo de la dirección θ. EL modelo creado considera la dilatación de la pupila y el tamaño variable de las imágenes, así se produce una representación normalizada de dimensiones constantes. La región del iris es modelada como una hoja flexible delimitada en la parte superior por el contorno de la pupila y en la inferior por el contorno del iris, de la forma indicada en la Fig.2. 15 [15].

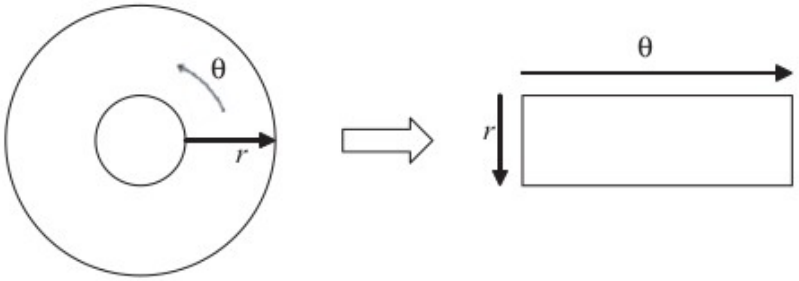


Fig.2. 15: Ejemplo de normalización por el método de Daugman [15].

Después de la etapa de normalización, se procede a la codificación y comparación de la información biométrica para realizar el reconocimiento. La codificación debe extraer la información biométrica contenida en el patrón de iris y generar un código único de asociación. En la etapa de comparación, miden las diferencias que existe entre los códigos binarios de una imagen receptada y una almacenada, y en base a esta medida se decide si los códigos han sido generados por el mismo iris o no [26].

Los filtros Gabor [32], son muy eficientes en el análisis de texturas en imágenes. El método de codificación de Daugman pasa la imagen normalizada del iris mediante un filtro Gabor bi-dimensional, y luego cada pixel de la imagen resultante se representa mediante dos bits. Otra forma de codificar la imagen de manera más sencilla es utilizar una serie de filtros Log-Gabor unidimensionales, descomponiendo la imagen del iris normalizado en un grupo de señales unidimensionales S_i , una por cada fila de la imagen de la forma indicada en la Fig.2. 16 [26].

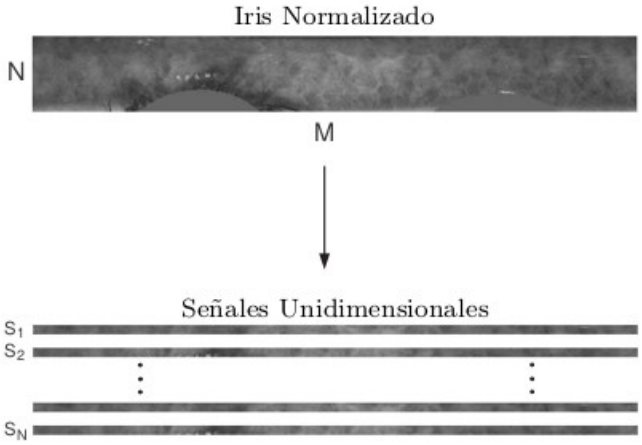


Fig.2. 16: Descomposición de la imagen normalizada en arrays de bits [26].

Cada señal S_i es pasada mediante el filtro Log-Gabor, obteniéndose un grupo de señales filtradas S_i^F . Finalmente, cada muestra de las señales S_i^F se codifica con dos bits ubicando su fase en el plano complejo, como se indica en la Fig.2. 17 [26].

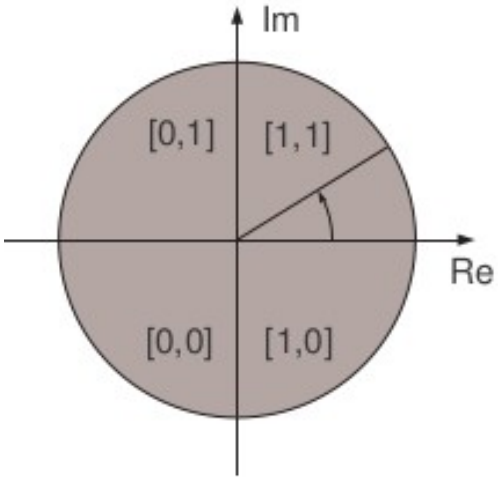


Fig.2. 17: Codificación de fase de las señales filtradas de la imagen normalizada [26].

El código obtenido mediante este proceso puede representarse como una matriz de (M × 2N), donde M y N son la cantidad de filas y columnas del iris normalizado[10]. En el proceso de identificación o reconocimiento se debe comparar el código obtenido con un código almacenado, obteniendo una medida de diferencia;

el método más común para la identificación del iris es por comparación de la distancia de Hamming [26]. En éste método se miden las diferencias que existe entre dos códigos binarios, utilizado también como Código corrector de errores, la idea es mantener el error lo menor posible con relación a un error deseado [33].

La distancia de Hamming entre dos cadenas de bits es calculada usando la función XOR, en donde se cuenta la cantidad de bits erróneos (cantidad de 1 lógicos en la operación) y se divide para el número de bits comparados. Para el caso de Daugman en sistemas de detección de iris, la distancia de Hamming máxima permitida es de 0.3 [33].

2.2.10 Tarjetas Embebidas de Sistemas Electrónicos.

Las tarjetas embebidas de sistemas electrónicos son circuitos electrónicos cuya funcionalidad es controlar de forma automática los procesos de algunas máquinas u operadores. En todo sistema electrónico se tiene dispositivos de estos tres tipos: de entrada, de salida y de proceso [34].

Los dispositivos de entrada generan una señal eléctrica a partir de una señal externa de otro tipo (por ejemplo la temperatura, la actuación con la mano sobre un pulsador). Los elementos de proceso reciben las señales de los dispositivos de entrada y deciden cual es la acción a realizar. La función de los periféricos de salida es ejecutar las acciones que decididas por los de proceso [34].

En la Fig.2. 18 se tiene la imagen de una tarjeta embebida utilizada para el diseño de sistemas electrónicos. En la placa electrónica se observa distintos periféricos como botones y pines de entrada y salida que permiten ejecutar distintas funciones como: detección de señales de entrada, activación de señales de salida, gestión de protocolos de comunicación, entre otros. Las tarjetas embebidas son utilizadas para diseñar sistemas electrónicos que requieren de un procesador de características con básicas de velocidad de procesamiento y memoria como por ejemplo para el diseño de termómetros digitales, centrales de alarma, tarjetas de adquisición de datos [34].

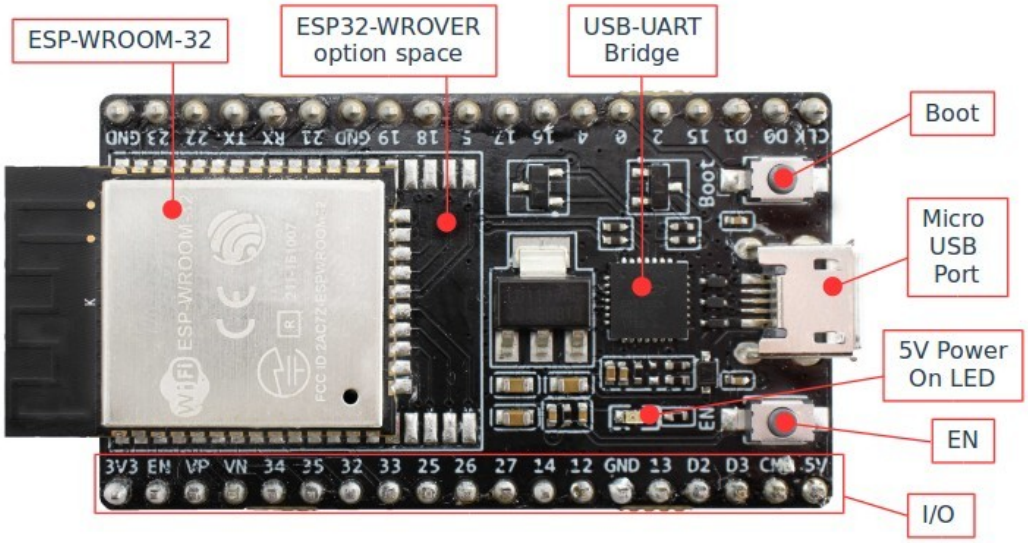


Fig.2. 18: Ejemplo de tarjeta embebida de sistemas electrónicos [34].

2.2.11 Sistemas de Interfaz Humano-Máquina.

Los sistemas de interfaz de Humano-Maquina (HMI) son dispositivos o sistemas que permiten crear una interfaz entre la persona y la máquina. En un inicio éstos sistemas utilizaban paneles compuestos por indicadores y comandos, tales como luces pilotos, indicadores digitales y análogos, registradores, pulsadores, selectores y otros que se interconectaban con la máquina o proceso. En la actualidad, las máquinas y procesos están implementadas con controladores y otros dispositivos electrónicos que dejan disponibles puertas de comunicación, es posible contar con sistemas de HMI bastantes más poderosos y eficaces, además de permitir una conexión más sencilla y económica con el proceso o máquinas[35].

De forma general se puede distinguir dos tipos de HMIs: de Terminal de Operador y de PC+Software.

El HMI de terminal operador es un dispositivo construido para ser instalado en ambientes agresivos, donde pueden ser solamente de despliegues numéricos, o alfanuméricos o gráficos. Pueden ser además con pantalla sensible al tacto (touch screen). En la Fig.2. 19 se observa un ejemplo de una pantalla utilizada para

interfaces humano-máquina, el dispositivo indicado puede programarse pata indicar el estado de las variables de control de un sistema e integrar funciones “touch” con botones para el control de procesos [35].

Fig.2. 19: Dispositivo HMI de terminal-operador[35].

El HMI de PC + Software constituye otra alternativa basada en un computador en donde se carga un software apropiado para la aplicación. El PC puede ser cualquiera según lo exija el proyecto, en donde existen los llamados Industriales(para ambientes agresivos), los de panel (Panel PC) que se instalan en gabinetes dando una apariencia de terminal de operador, y en general veremos muchas formas de hacer un PC, pasando por el tradicional PC de escritorio [35].

2.2.12 Cerraduras Magnéticas

La cerradura magnética es un conjunto de elementos que dispone de un mecanismo de activación manual, una llave o un pulsador a distancia, que por medio de dispositivos electrónicos permite bloquear la apertura de puertas. Dicho mecanismo provoca el deslizamiento de uno o varios pestillos hacia uno o varios cerraderos fijos, o la sujeción de una barra de hierro una una base magnetizada. En la Fig.2. 20 se observa una cerradura electrónica de placas magnéticas, las cerraduras de este tipo funcionan a 12 o 24 voltios de corriente continua, creando un campo magnético de fuerzas de bloqueo superiores a los 180 kilopondios [36].

Fig.2. 20: Cerradura electrónica de placas magnéticas [36].

2.3 PROPUESTA DE SOLUCIÓN

Un sistema de control de acceso por reconocimiento de iris para ingreso de personal a las instalaciones de la Empresa Electroservicios QUERUBÍN, permitirá tener un registro de personal más seguro y rígido, impidiendo suplantaciones e ingreso de personal no autorizado a las instalaciones.

CAPÍTULO III

METODOLOGÍA

3.1 MODALIDAD DE LA INVESTIGACIÓN

El presente trabajo de investigación se realizó bajo los conceptos de investigación aplicada ya que busca la generación de conocimiento con aplicación directa a los problemas de la sociedad o el sector productivo. Se utilizaron los conocimientos adquiridos para dar solución a los problemas de seguridad en la empresa Electroservicios Querubín, creando un sistema de control de acceso por reconocimiento de iris mediante los siguientes tipos de investigación:

Se utilizó la investigación bibliográfica documentada, para la adquisición de información sobre bases teóricas que facilitó el diseño del sistema de control de acceso. La explicación científica de las bases del proyecto se tomaron de libros, artículos técnicos y proyectos desarrollados yá en otros países y en el Ecuador donde se realizaron estudios de: enlaces y redes de datos para sistemas de control de acceso, servidores web, programación, aplicaciones web y desarrollo de aplicaciones IOT.

Se utilizó la investigación de campo con la que se realizó un estudio sistemático para determinar las características del sistema que requiere la empresa. La recolección de información y adquisición de datos se tomaron directamente de la empresa Electroservicios Querubín de la Ciudad de Puyo.

Se utilizó la investigación experimental para realizar el diseño e implementación de los elementos de control del prototipo, realizando pruebas de funcionamiento para validar el sistema de control de acceso.

3.2 RECOLECCIÓN DE INFORMACIÓN

La información para el estudio y dimensionamiento de equipos y materiales se obtuvo de la Unidad de Tecnología y Administración de la empresa Electroservicios Querubín de la Ciudad de Puyo; y de bibliotecas afines a la documentación teórica requerida, de la Universidad Técnica de Ambato.

La recolección de información se inició de forma previa a la presentación y reconocimiento del proyecto de investigación utilizando como recursos: tablas comparativas y fichas de observación.

3.3 POBLACIÓN Y MUESTRA

Por las características de la presente investigación se determinó que no se requería de un estudio de población y muestra.

3.4 PROCESAMIENTO Y ANÁLISIS DE DATOS

El procesamiento y análisis de datos se realizó mediante una clasificación de la documentación obtenida, presentando una descripción ordenada de los entornos a estudiarse en el proyecto. Se realizó un análisis crítico de los datos obtenidos durante la recolección de información, considerando los siguientes lineamientos:

- Se eliminó información de baja relevancia.
- Se obtuvo parámetros técnicos, específicos y concretos que determinen las características del sistema a ser diseñado.
- Se interpretó la información que permite plantear estrategias de solución al problema.

3.5 DESARROLLO DEL PROYECTO

En el desarrollo e implementación de un sistema de control de acceso por reconocimiento de iris para el ingreso de personal a la Empresa Electroservicios Querubín de la ciudad de Puyo, se procedió con la siguiente organización de actividades.

- Análisis de las características de los sistemas de control de acceso de personas en la actualidad.
- Comparación de las fortalezas y vulnerabilidades de los sistemas actuales de control de acceso de personas.
- Clasificación de los sistemas de control de accesos en función de eficiencia, fiabilidad, escalabilidad y seguridad.
- Análisis de los dispositivos electrónicos a utilizar en el sistema de control de acceso de personal.
- Análisis de la tecnología a ser usada en el sistema de control de acceso de personal.
- Acoplamiento de los componentes electrónicos y tecnología a ser utilizada para armar un prototipo de sistema de control de acceso de personal.
- Programación el algoritmo del sistema de control de acceso de personal.
- Automatizar el sistema de control de acceso por reconocimiento de iris para acceso de personal.
- Integración de la plataforma Ethernet al sistema de control de acceso de personal.
- Implementación de la base de datos que permita la recolección de los mismos.
- Implementación de un prototipo de sistema de control de acceso de personal por reconocimiento de iris para la Empresa Electroservicios Querubín.
- Ejecución de las pruebas de funcionamiento del prototipo del sistema.
- Elaboración del Informe Final del Proyecto de Investigación.

CAPÍTULO IV

PROPUESTA

En la empresa Electroservicios Querubín de la ciudad de Puyo se ha detectado la intranquilidad de sus dirigentes y propietarios, debido a precedentes que afectan de forma directa a la seguridad económica de la empresa; de manera específica a la seguridad de los bienes activos almacenados como mercadería. Los administradores de la empresa han detectado ausencia de equipos y suministros, enfocando el problema al tipo de control de seguridad utilizado en las unidades de almacenamiento.

La seguridad de acceso a las distintas áreas de la empresa Electroservicios Querubín (Administración de Bienes Ventas y Desarrollo Tecnológico) es controlada por medios humanos mediante guardias de seguridad, existiendo vulnerabilidades debido al carácter natural del error humano. En consecuencia, para incrementar el nivel de seguridad de la empresa es de gran importancia el diseño e instalación de un sistema de control de acceso, con el que se obtendrá un control rígido en el ingreso de personal a las áreas vulnerables de la empresa, asegurando los activos tangibles de la misma.

4.1 ANÁLISIS DE FACTIBILIDAD.

El desarrollo del proyecto tuvo una factibilidad técnica, económica y bibliográfica de la forma detallada a continuación:

4.1.1 Factibilidad Técnica

La realización del presente proyecto tiene factibilidad técnica dado que los equipos y elementos electrónicos necesarios para el desarrollo del prototipo del sistema de control de acceso, se encuentran en el país o son de fácil importación y el software implementado se desarrolla bajo entornos de licencias libres.

4.1.2 Factibilidad Económica

El presente proyecto es económicamente factible debido a que el financiamiento de la investigación es solventada con los recursos económicos del investigador y la empresa Electroservicios Querubín de la ciudad de Puyo.

4.1.3 Factibilidad Bibliográfica

La presente investigación tiene factibilidad bibliográfica debido a que la información requerida se encuentra en libros, documentos científicos, tesis, revistas y documentos web.

4.2 SITUACIÓN ACTUAL DE LA EMPRESA

La empresa Electroservicios Querubín de la ciudad de Puyo, es una compañía dedicada al desarrollo de proyectos tecnológicos y venta de equipos en áreas que abastecen los mercados eléctricos, electrónicos y de comunicaciones. Desde el punto de vista de gestión de la empresa está organizada en la jerarquía mostrada en la Fig.4. 1.

La máxima unidad de gestión de la empresa está comprendida por la dupla de gerente y presidente, a éstos responden los departamentos de ventas, desarrollo tecnológico y administración de bienes.

El departamento de administración de bienes, es el encargado del área contable así como del manejo de activos de la empresa. El departamento de ventas mantiene un contacto directo con los clientes y los técnicos de instalación, quienes ejecutan la

mano de obra necesaria en los proyectos. El departamento de desarrollo tecnológico, es el encargado del diseño de proyectos eléctricos o de comunicaciones [37].

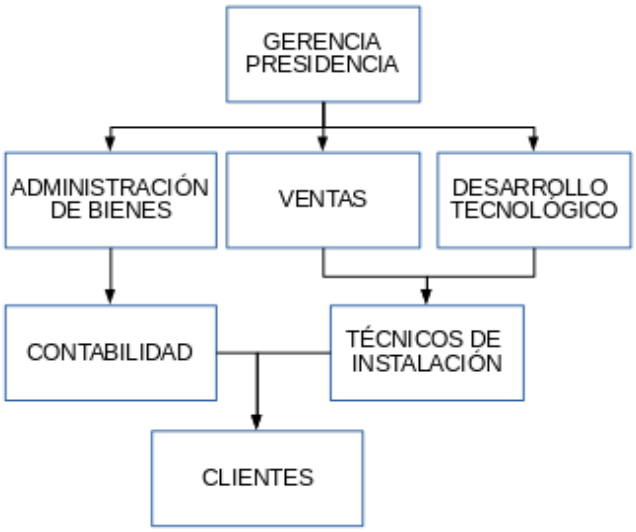


Fig.4. 1: Organigrama estructural de la empresa Electroservicios Querubín [37].

La empresa funciona en una construcción arquitectónica de una sola planta, la que se ilustra en la Fig.4. 2. La edificación está dividida por zonas en donde gerencia y presidencia comparten una misma oficina de forma similar a los departamentos de administración de bienes y contabilidad, estando todos los departamentos y la bodega de almacenamiento de equipos conectados mediante un pasillo.

El acceso a las distintas áreas de la empresa es controlado mediante personal de seguridad, y cada departamento de la misma tiene cerraduras comunes. Los empleados de la empresa tienen la llave del departamento al que pertenecen, sin embargo, algunos empleados de ventas y del laboratorio de desarrollo tecnológico requieren el ingreso a la bodega, el mismo que no tiene ningún registro o control de identificación.

La bodega de la empresa Electroservicios Querubín es un punto crítico en el análisis de seguridad física y económica para la compañía. En éste lugar se almacenan equipos electrónicos y materiales eléctricos de alto costo como: computadores, rollos

de cable, equipos de transmisión de datos inalámbricos, sistemas de comunicaciones de radio-frecuencia, entre otros.

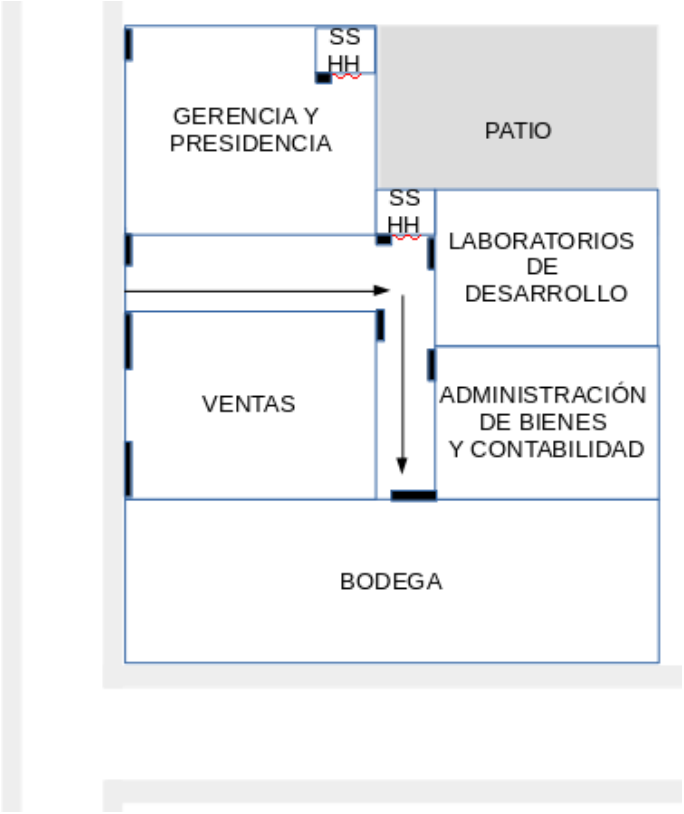


Fig.4. 2: Distribución de zonas de trabajo en la empresa de Electroservicios Querubín [37].

Debido a la sensibilidad económica que representa la bodega para la empresa, y tomando en cuenta las consideraciones de las normas IEC ISO 27001, aplicadas con un enfoque para que las personas propietarias de activos definan a ciertos usuarios, cada vez que son necesarios para acceder a la zona de almacenamiento de los activos (Bodega); se procedió con el área administrativa y de gerencia a establecer las siguientes requerimientos de acceso.

- El acceso al área de almacenamiento de activos debe ser restringido, permitiendo el paso solo a trabajadores de las áreas de administración de bienes, ventas y gerencia.
- El acceso a la bodega debe mantenerse bloqueado por defecto y de forma automática, garantizando el acceso solo a personas autorizadas.
- Por seguridad, el acceso al área de almacenamiento es restringido para un

horario comprendido entre las 22h00 y las 05h00, a excepción del Gerente.

- Todo acceso realizado a la bodega debe mantener un registro de horario y usuario.
- Se debe implementar un sistema de alertas de condiciones anormales de funcionamiento como: puerta forzada o puerta abierta sin autorización.

El sistema de control de acceso propuesto para la empresa de Electroservicios Querubín, es el mostrado en el diagrama de bloques de la Fig.4. 3 .

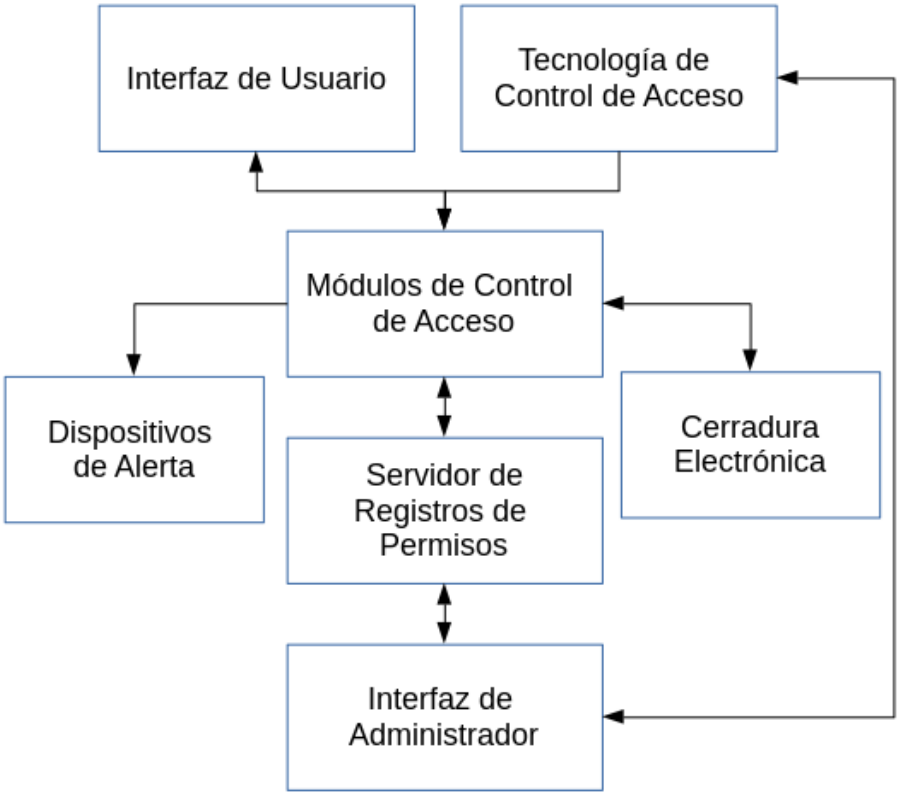


Fig.4. 3: Diagrama de bloques del sistema de control de acceso de la empresa de Electroservicios Querubín.

El sistema consta de 7 sectores diferenciados que son: Tecnología de control de acceso, una interfaz de usuario para crear funciones de control de acceso o registro de asistencia, el módulo de control de acceso que es una interfaz entre el identificador de iris, los actuadores del sistema y el servidor de registros y permisos. Finalmente se tiene una interfaz de administrador para configurar la gestión del sistema.

4.3 TECNOLOGÍAS DE CONTROL DE ACCESO

Los sistemas de control de accesos en el mercado mundial a los que se puede acceder sin restricciones legales en Ecuador funcionan mediante las tecnologías descritas en la Tabla4. 1 y la Tabla4. 2. En las tablas mencionadas la fiabilidad, facilidad de uso, prevención de ataques, aceptación del usuario, y estabilidad se evalúan de forma cuantitativa en donde los números cercanos a 0 evalúan las características de forma negativa, mientras que los cercanos a 10 simbolizan que la característica es positiva.

Tabla4. 1: Características de los sistemas de control de acceso convencionales. Basado en [21].

Tecnologías/ Características	**Proximidad**	**Clave**	**Banda magnética**	**Código de barras**	**Tarjetas con Chip**
Fiabilidad	4	3	4	2	7
Facilidad de Uso	9	6	9	9	9
Prevención de Ataques	8	8	8	8	8
Aceptación del Usuario	9	7	9	8	9
Estabilidad	10	8	10	8	10
Intrusivo	No	No	No	No	No
Identificación y Verificación.	Ambas	Ambas	Ambas	Ambas	Ambas
Interferencias	Campos electro-magnéticos	No	Campos electro-magnéticos	No	No

La Tabla4. 1 describe las características de controles de accesos convencionales, es decir de aquellos que utilizan datos u objetos externos a los usuarios para la autenticación, dentro de ésta categoría se determina que la fiabilidad de éstos sistemas se encuentra en valores cuantitativos que van desde media a baja fiabilidad; ésto, debido a que los objetos de identificación o claves pueden pasarse entre usuarios, perdiendo características de seguridad. Las tecnologías que funcionan por proximidad o banda magnética presentan desventajas en relación a interferencias a

campos electromagnéticos, con las demás características no se tiene inconvenientes, sin embargo no son utilizadas en el sistema de éste proyecto debido a su fiabilidad.

La Tabla4. 2 muestra las características de los sistemas de control de accesos que utilizan métodos biométricos de autenticación, en donde se observa que solo la tecnología de reconocimiento de voz posee una baja fiabilidad, mientras que los sistemas de reconocimiento de iris tienen la mayor fiabilidad ya que el porcentaje de falsas aceptaciones es de 1 en $1.5x10^6$. En referencia a la aceptación de los sistemas por parte del usuario, únicamente el reconocimiento de voz tiene un índice de alta aceptación, pero éste es descartado debido a su baja confiabilidad.

Tabla4. 2: Características de los sistemas de control de acceso biométricos. Basado en [21] [24]

Tecnologías/ Características	**Huella Dactilar**	**Iris**	**Geometría de la Mano**	**Facial**	**Voz**
Probabilidad de Error	1 en 10.000	1 en $1.5x10^6$ (en un ojo)	1 en 50.000	1 en 100.000	1 en 500
Facilidad de Uso	9	7	8	7	8
Prevención de Ataques	8	8	9	8	8
Aceptación del Usuario	8	6	6	7	9
Estabilidad	8	10	9	7	6
Intrusismo	Bajo	No	Bajo	No	No
Identificación y Verificación.	Ambas	Ambas	Identificación	Ambas	Ambas
Interferencias	Suciedad, heridas, asperezas, sequedad, edad	Iluminación inadecuada	Artritis, reumatismo, edad, lesiones varias de la mano	Iluminación inadecuada.	Campos sonoros, ruido sonoro ambiental

La estabilidad se refiere a las variaciones que la medida biométrica sufre en torno al transcurso del tiempo, en ésta característica, los sistemas que utilizan detección de huellas dactilares y detección de iris son los más estables en comparación al reconocimiento facial o geometría de mano.

Otro factor que interviene en un sistema de control de acceso efectivo, es la interferencia, la que provoca retardos en el tiempo de autenticación y en consecuencia, incomodidad a los usuarios; en éste aspecto los sistemas con detección de huella dactilar están sujetos a interferencias producidas por suciedad, heridas o asperezas del tejido epitelial; los métodos de geometría de la mano presentan inconvenientes cuando el usuario adquiere enfermedades degenerativas de los tejidos óseos o articulaciones de las manos o dedos y los sistemas de detección de iris y reconocimiento facial, están sujetos a sufrir interferencias de luminosidad.

Debido a las características mencionadas, se determina que la mejor tecnología a implementarse en el sistema de control de acceso para la empresa de Electroservicios Querubín, es la de reconocimiento de iris ya que es la tecnología de mayor fiabilidad por ser la tecnología con la menor probabilidad de error, con una dificultad de uso y aceptación de usuario intermedia, pero de alta estabilidad y pocas interferencias.

4.4 EQUIPOS DE RECONOCIMIENTO DE IRIS.

Los equipos que permiten implementar sistemas basados en reconocimiento de iris conocidos en el mercado internacional están listados en la Tabla4. 3, en el mercado local ecuatoriano, no se dispone de éste tipo de tecnologías, por lo que para éste proyecto, en la aplicación de sistemas con reconocimiento de iris en el país se considera la necesidad de importar los dispositivos.

Los equipos que utilizan reconocimiento de iris para autenticación y pueden ser importados son: el Eyeswipe Nano, HBOX, Eyelock Nano NXT y el Myris. Todos los dispositivos mencionados tienen las mismas características de fiabilidad, el Eyeswipe Nano, HBOX, Eyelock Nano NXT, utilizan los mismos protocolos de

comunicación, que son protocolos especiales de sistemas de control de accesos como: Wiegand y Friend-toFriend (F2F). Debido a los costos y a la seguridad se selecciona el Eyeswipe Nano, como el sensor a utilizarse en el sistema, descartando los otros equipos de características superiores por su alto costo y el Myris por la baja seguridad ante vandalismos e incomodidad al ser un mecanismo manual.

Tabla4. 3: Características de los sensores de reconocimiento de iris. Basado en [24]

Sensores/ Características	**Eyeswipe-Nano**	**HBOX**	**NANO NXT**	**Myris**
Probabilidad de Error	1 en $1.5x10^6$ (por ojo)	1 en $1.5x10^6$ (por ojo)	1 en $1.5x10^6$ (por ojo)	1 en $1.5x10^6$ (en un ojo)
Distancia de reconocimiento	6-15 cm	1.5m a 2m V 30 cm H	6 - 30cm	12 - 17cm
Tiempo de reconocimiento	2 - 5 segundos	0.5 segundos	1-3 segundos	1-3 segundos
Modo de reconocimiento	Vídeo	Vídeo	Vídeo	Vídeo
Software de gestión	Propietario SSH	Propietario SDK optional	Propietario SDK optional	Propietario
Protocolos de Comunicación	Wiegand, F2F, OSDP, PAC, POE	Wiegand, F2F, OSDP, PAC, POE	Wiegand, F2F, OSDP, PAC, POE	USB
Número de Registros	10^4 Device $+10^6$ Server	$2x10^4$ Device $+10^6$ Server	10^4 Device $+10^6$ Server	10^3 Device 10^4 Server
Montaje y seguridad	Soporte de pared Alta	Soporte pared Alta	Soporte pared Alta	Manual/ Baja
Precio	$520	$3400	$1700	$400
Requiere Importación	Si	Si	Si	Si

4.5 IDENTIFICADOR DE IRIS EYESWIPE NANO

El identificador de iris Eyeswipe Nano mostrado en el proceso de registro de un

usuario en la Fig.4. 4, es un dispositivo de la empresa Eyelock, que identifica, registra y crea alertas de registros de autenticación de usuarios mediante la tecnología de reconocimiento de iris.

El dispositivo Eyeswipe Nano tiene un sistema operativo de propietario que procesa la información y determina si una plantilla detectada está registrada o no en su base de datos interna. El registro de usuarios en la base de datos del dispositivo, se realiza desde el programa Eyenroll, software entregado por el fabricante para la gestión de usuarios del sistema, que permite guardar tres características de cada usuario registrado (ÍD, Nombre, Apellido).

Fig.4. 4: Proceso interno del registro de un usuario en el Eyeswipe Nano.[24].

El identificador de iris se comunica por Ethernet con controladores que alojan servidores TCP/IP, permitiendo tener varios sensores de reconocimiento de iris conectados en red a un mismo controlador. El dispositivo tiene un servidor Avahi que permite conocer la dirección IP inicial mediante el envío de un broadcast.

Con la dirección IP del Eyeswipe es posible configurar las características específicas del dispositivo como su dirección IP, tono del sonido aceptación o negación de un registro, intensidad de luz de los LEDs indicadores de registro. También es posible configurar el dispositivo para que envíe los datos de los procesos de autenticación correctos a un servidor TCP/IP determinado. Para realizar todas estas

configuraciones, el Eyeswipe nos permite el acceso al sistema del identificador mediante un servicio ssh.

Una vez dentro del sistema Eyeswipe, existen dos ficheros que permiten configurar las características de mayor importancia para el sistema, los cuales son: la dirección IP, y la dirección y puerto del servidor al que el dispositivo debe enviar los datos cuando detecta “matches correctos”. Los archivos de configuración se observan en la Fig.4. 5

La dirección IP del dispositivo se configura de forma similar a un sistema Linux, en el directorio /etc/network/ se encuentra un fichero de nombre interfaces, el mostrado en la parte izquierda de la Fig.4. 5, en donde se especifica una dirección IP estática.

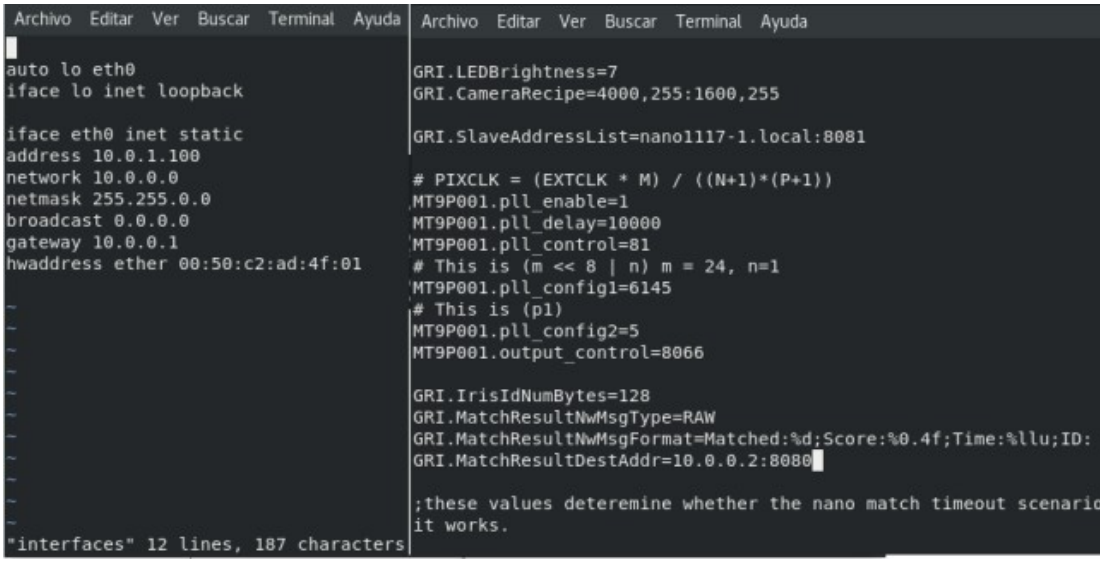


Fig.4. 5: Ficheros de configuración del Eyeswipe Nano.

Del lado derecho de la imagen se observa el fichero /root/Eyelock.ini, en la última línea de código válida visualizada, se especifica la dirección IP del servidor TCP/IP, que para el caso estará alojado en el módulo controlador, y tiene la dirección IP 10.0.0.2 y con un socket que estará examinando las peticiones del Eyeswipe en el puerto 8080.

4.6 INTERFAZ DE USUARIO

El sistema tiene la capacidad de crear registros de asistencia y habilitar el acceso a

las distintas áreas de la empresa a usuarios determinados, sin embargo ésta función no la puede realizar de forma autónoma el Eyeswipe Nano.
Para manejar las dos funciones, se requiere de una interfaz de selección que permita al usuario escoger una de las funciones. La función seleccionada es procesada por el módulo de control de acceso, creando los eventos necesarios para registrar la solicitud y activar los mecanismos de apertura de ser necesario.

La interfaz de usuario se diseñó bajo las normas NUREG- 0700 Rev. 2 que especifica las guías de revisión para el diseño de interfaces humano-sistemas. Las normas técnicas especifican el uso de colores, tamaño de letra, uso de abreviaciones, entre otras características para que la interfaz sea entendible y de fácil manipulación por parte del usuario.

Las especificaciones que se tomaron y que se adaptan al uso del sistema actual se detallan a continuación:

- Cuando el color se utiliza para la codificación, se debe emplear de forma conservadora y continua. El número de colores utilizado para la codificación debe mantenerse al mínimo necesario para proporcionar suficientemente información.
- Cuando un usuario debe distinguir rápidamente entre varias categorías discretas de datos, se debe usar un color único para mostrar los datos en cada categoría.
- Se deben usar colores más brillantes y / o más saturados cuando sea necesario llamar la atención del usuario sobre los datos críticos.
- Debe evitarse el azul puro sobre un fondo oscuro para texto, líneas finas o información de alta resolución
- Cuando la codificación por colores se utiliza para agrupar o resaltar los datos mostrados, todos los colores del conjunto deben ser fácilmente discriminables entre sí.
- El color rojo debe ser utilizado con preferencia para indicar estados de alarma, condiciones inseguras o peligrosas; el color verde indica condiciones satisfactorias, seguras o de normal funcionamiento, los colores azules claros u

oscuros se utilizan para dar avisos.

- Para discriminar colores sobre un fondo claro se debe utilizar tonos de rojo, amarillo oscuro, verde, y negro; y sobre fondos oscuros los tonos rojo, amarillo, blanco, azul desaturado y verde.
- Los símbolos deben ser legibles y fácilmente discriminables contra los colores de fondo en todas las condiciones de luz ambiental previstas.
- Se debe usar un máximo de tres niveles de tamaño. Las dimensiones principales del símbolo más grande deben ser al menos el 150 por ciento de la dimensión principal del símbolo más pequeño.
- Se deben proporcionar señales auditivas para alertar al usuario de situaciones que requieren atención, como una acción de entrada incorrecta o una falla de la HSI para procesar una entrada del usuario.
- La tasa máxima de actualización debe determinarse por el tiempo requerido para que el usuario identifique y procese la función modificada de la pantalla.
- El cambio de valores alfanuméricos que el usuario debe leer de manera confiable no debe actualizarse más de una vez por segundo
- Cuando la computadora genera una pantalla para actualizar los datos modificados, los elementos antiguos deben borrarse antes de agregar nuevos elementos de datos a la pantalla.
- Una organización de pantalla de visualización estándar debería ser evidente para la ubicación de varias funciones de HSI (como una zona de visualización de datos, zona de control o zona de mensaje) de una pantalla a otra.
- Las zonas funcionales de HSI y las características de visualización deben ser visualmente distintivas entre sí, especialmente para los elementos de comando y control en pantalla (que deben ser visiblemente distintos de todas las otras estructuras de pantalla).
- La polaridad de contraste de los caracteres superpuestos debe ser apropiada para el método de proyección
- Los números individuales en cualquier tipo de escala fija deben ser verticales.
- Las teclas de función son teclas individuales en un teclado o pad que están dedicadas a operaciones predefinidas particulares, como para abrir una pantalla predefinida

- Al definir abreviaturas que no son comunes para la población de usuarios, se debe usar una regla simple que los usuarios entiendan y reconozcan
- Las abreviaturas y los acrónimos no deben incluir la puntuación
- Cuando el usuario debe recordar los códigos arbitrarios, los caracteres se deben agrupar en bloques de tres a cinco símbolos, separados por un mínimo de un espacio en blanco u otro carácter separador, como un guion o una barra inclinada.
- Los valores numéricos normalmente deberían mostrarse en el sistema de números decimales
- Se debe mostrar un número en la cantidad de dígitos significativos requeridos por los usuarios para realizar sus tareas.
- Las pantallas numéricas deben acomodar el rango completo de la variable.
- Las pantallas digitales deberían cambiar lo suficientemente despacio para poder leerlas [38].

Tabla4. 4: Características técnicas de pantallas touch.

Pantalla/ Características	**LCD TFT 2.4” TOUCH V2.1**	**LCD 2.8” Shield V3**	**3.2” SMART SCREEN**	**NEXTION 2.4”**
Protocolo de comunicación	SPI+controlador HX8347D	SPI+controlador HX8347D	Serial/ SPI 802.11 b/g/ n/	USART
Memoria Integrada	No	No	80kb	Si
Tamaño	2.4” 240x320px	2.8” 240x320px	3.2” 240x320px	240x320px
Voltaje de Funcionamiento	3.3 – 5 Vdc	3.3 – 5 Vdc	4 – 5.5 Vdc	3.3 – 5 Vdc
Tipo de touch screen	Resistivo	Resistivo	Resistivo	Resistivo
Método de Programación	Requiere Microntrolador	Requiere Microntrolador	Requiere Microntrolador	Software Nextion
Precio (USD)	22	23	70	23

La interfaz de usuario es desarrollada en una pantalla touch, ya que presenta un ambiente más amigable con el personal, y en la actualidad los costos son

comparables a sistemas de teclados con LCD’s que resultan los más económicos. En la tabla Tabla4. 4 se observa las características de cuatro pantallas LCD touch, de la que se escoge la pantalla Nextion NX322T024 debido a su bajo costo, facilidad de programación e integración en circuitos con solo 4 cables (USART).

4.7 DISPOSITIVOS DE ALERTA

En sistemas electrónicos de seguridad se utilizan sirenas para enviar señales sonoras que identifican alertas, comunicando al personal la existencia de un posible atraco a los bienes protegidos. El sistema de control de acceso por reconocimiento de iris integra un procedimiento para activar una señal acústica en caso de que la puerta de la bodega sea forzada o se detecte una condición anormal de funcionamiento del sistema.

En la Tabla4. 5 se tienen algunos de los dispositivos más comunes utilizados en señalización acústica para seguridad, de los dispositivos en lista la Sirena MS-390 fue descartada ya que de acuerdo a la norma técnica NTE INEN ISO 7731:2014 en ambientes laborales no se debe exceder un nivel de señalización acústica de 118 dB además éste dispositivo es de un costo elevado en comparación a los demás.

Tabla4. 5: Características de sirenas para sistemas de seguridad.

Característica /Dispositivo	**Voltaje de Alimentación**	**Consumo de Corriente**	**SLP**	**Tonos**	**Precio (USD)**
DSC SD 20W	6-12 Vdc	500 mA	110 dB	Seguridad Continuo	13,40
DSC SD 30W	6-12 Vdc	1100 mA	118 dB	Seguridad Continuo	15,99
DSC SD 15W	6-12 Vdc	300 mA	90 dB	Seguridad Continuo	8,70
Sirena FPE. MS-390	12 Vdc/24Vdc	3000 mA	130 dB	Seguridad	59,00

El dispositivo seleccionado es la sirena DSC SD 30W que opera a un voltaje nominal

de 12 Vdc con un consumo de corriente de 1.1 amperios; ya que es el dispositivo que tiene el mayor nivel de presión sonora recomendado por la norma ISO 7731, sus características eléctricas no difieren en gran magnitud a los otros dispositivos y sus precios son comparables; además tiene integrado un tono para uso de alertas de seguridad.

4.8 CERRADURA ELECTRÓNICA

La cerradura electrónica es un dispositivo instalado en la puerta para que el sistema permita o bloquee el acceso a la bodega, en la Tabla4. 6 se muestra las características de distintas cerraduras de accionamiento eléctrico y magnético. Las cerraduras de accionamiento eléctrico son utilizadas en ambientes exteriores y tienen dificultades en funcionamiento conjunto con brazos neumáticos para el cierre de puertas, reflejándose en una baja garantía del cierre automático de la puerta después de un acceso, motivo por el que son descartados.

Las cerradura de accionamiento magnético MAG600S es el dispositivo seleccionado para el sistema; éste equipo ejerce una fuerza de retención de 600lb en la puerta, superior al Access PRO 350 aunque por un de precio ligeramente superior. La fuerza de retención es superior en más de cuatro veces el peso que un ser humano promedio puede levantar, por lo que el sistema se considera seguro.

Tabla4. 6: Características de cerraduras eléctricas/magnéticas de sistemas de seguridad

Dispositivo	**Voltaje de Alimentación**	**Consumo de Corriente**	**Fuerza de Soporte**	**Sensores**	**Precio (USD)**
Cougar Electric Lock	9 – 12 Vdc	2A	Mecánico	No	70
Viro 8972	12 Vac	2A	Mecánico	No	89
Access PRO MAG600S	12 Vdc 24Vdc	575mA 280mA	280Kgf 600lb	Door Open	43,75
Access PRO MAG350S	12 Vdc 24Vdc	350mA 175mA	180Kgf 350lb	Door Open	38,08

4.9 MÓDULO DE CONTROL DE ACCESO

El módulo de control de acceso es una interfaz central entre los actuadores, el Eyeswipe Nano, la interfaz de usuario, la cerradura y el servidor de registros. Éste módulo aloja un servidor TCP/IP que recibe los datos de autenticación del Eyeswipe y los pasa mediante un cliente web al servidor de registros, en donde se llevan a cabo los procesos de identificación, registros y asignación de permisos, devolviendo un valor de verificación al módulo de control para que éste tome decisiones en función del mismo.

El módulo de control de acceso contiene un Servidor TCP/IP y un Cliente web que deben programarse en un micro-controlador de altas características de procesamiento, debido a que se necesita obtener una respuesta rápida del sistema, además se requiere de una interfaz de comunicación con la red de área local e interfaz serie para la pantalla seleccionada.

Tabla4. 7: Características de circuitos y tarjetas electrónicas de desarrollo.

Circuito Integrado	Frecuencia de Operación	Interfaces de Comunicación	Interfaces GPIO	Interfaces Analógicas	Precio (USD)
PIC18F2550	0 - 48 MHz	MSSP, EUSART, SPI, I2C, USB	22	10	$7+15 (Mod. Eth.)
PIC18F4550	0 – 48 MHz	MSSP, EUSART, SPI, I2C, USB	30	13	$10+15 (Mod. Eth.)
PIC16F887	0 – 20 MHz	MSSP, EUSART, SPI, I2C	30	13	$9+15 (Mod. Eth.)
Arduino Uno	16 MHz	USART, SPI, I2C	14	6	$13+15 (Mod. Eth.)
At-Mega 328p	16 MHz	USART, SPI, I2C	23	7	$7+15 (Mod. Eth.)
ESP8266-12E	80 / 160 MHz	USB-RS232, 2USART, 2SPI, I2C, 802.11	13	1	$11+0 (WIFI)
DOIT ESP32	2x 80/240 MHz	USB-RS232, 3USART, 2SPI, 2I2C, 802.11, 802.3	26	8	$13+0$ (WIFI)

En la Tabla4. 7 se detalla las características más relevantes de los micro-controladores y tarjetas electrónicas de desarrollo que pueden ser utilizadas como el cerebro del módulo de control. El dispositivo seleccionado es la tarjeta de desarrollo DOIT ESP32 de Espressif, debido a que incluye una pila para comunicación Wifi, es un dispositivo con un micro-procesador de 2 núcleos que trabajan hasta 240 MHz y es de bajo costo.

El módulo de control de acceso está diseñado en base al esquema del circuito mostrado en la Fig.4. 6, en donde se tiene un puerto de comunicaciones serie para el control de la pantalla, un puerto para la activación de 2 sirenas de hasta 1.5 A con una tensión de alimentación de 12Vdc, y un puerto para la detección de señales digitales de 12Vdc.

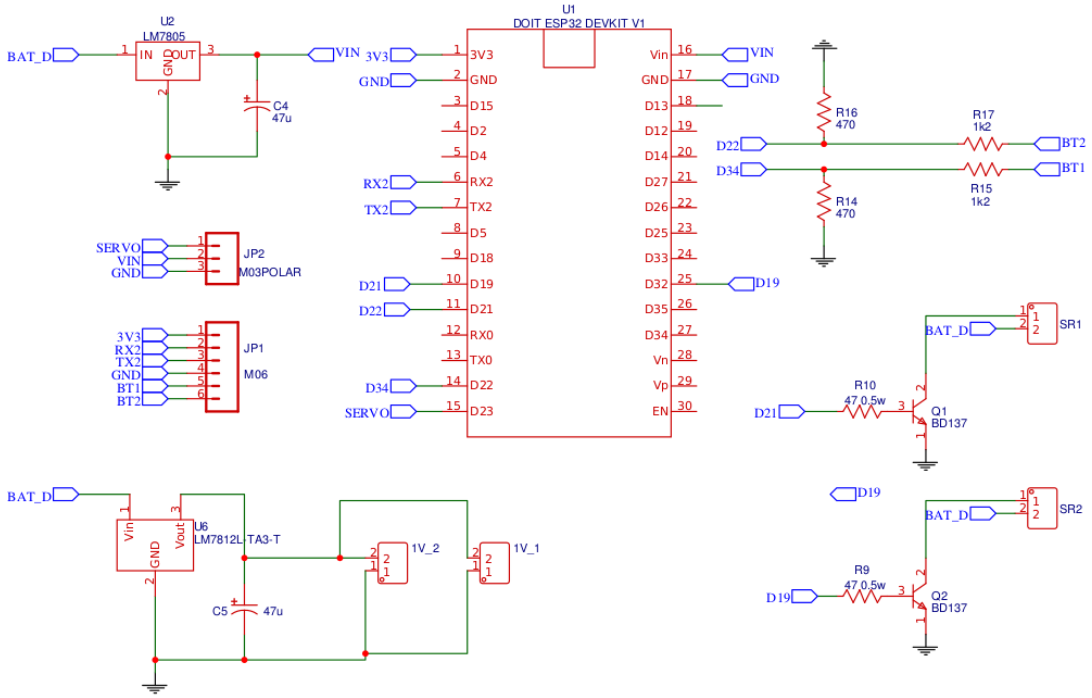


Fig.4. 6: Circuito de módulo de control de acceso.

El circuito es alimentado con un regulador de carga de baterías, funcionando como respaldo de alimentación del módulo de control de acceso, la corriente recomendada para el controlador de carga es de 3A, que es una corriente ligeramente superior a la

corriente de consumo de los principales elementos electrónicos alimentados por módulo de control, mostrados en la Tabla4. 8.

El módulo de control de acceso trabaja al voltaje suministrado por la tarjeta de control de carga que es de 12Vcd, por lo que se utilizan sirenas electrónicas, las mismas tienen un rango de consumo de corriente que va desde los 500mA a los 1100mA, y un rango de voltajes de funcionamiento desde los 6Vdc a los 12 Vdc, motivo por el que se diseña la tarjeta electrónica para que soporte sirenas a 12 Vdc y 1100 mA. Para la activación de las sirenas una señal digital enviada por el DIOT-ESP32 que es de 3.3 Vdc, activa un transistor BD135, permitiendo el encendido de la sirena.

Tabla4. 8: Consumo de corriente de los principales elementos conectados al módulo de control.

Elemento del Módulo	**Corriente de Consumo**		**Voltaje de Funcionamiento**	
	Mínimo	Máximo	Mínimo	Máximo
DIOT-ESP32	10 uA	200mA	5 Vdc	9 Vdc
Cerradura Magnética	300 mA 150 mA	300mA 150 mA	12 Vdc 24 Vdc	12 Vdc 24 Vdc
Pantalla	90 mA	500 mA	3.3 Vdc	5 Vdc
Sirena	500 mA	1100 mA	6 Vdc	12 Vdc
Corriente Total		2100 mA		

El transistor seleccionado trabaja con una corriente de colector de 1.5 A, voltaje colector-emisor de 45 V, un voltaje base emisor de encendido de 1V y una tensión máxima de emisor base de 5Vdc, por lo que es adecuado como interfaz de encendido de la sirena y la cerradura magnética.

El transistor trabaja en la región de saturación por lo que las resistencias de base R9 y R10 deben limitar la corriente de base para evitar daños al transistor y garantizar la saturación del mismo. La corriente de base de los transistores Q1 y Q2 deben estar en el rango establecido por la ecuación 4.1, en donde la corriente de base máxima del transistor es de 500mA, la corriente de colector 1100 mA y el la ganancia del

transistor (βcd) es 25.

$$500\,mA \geq I_B \geq \frac{I_{Csat}}{\beta_{cd}} \qquad 4.1$$

$$500\,mA \geq I_B \geq \frac{1.1\,A}{25} \qquad 500\,mA \geq I_B \geq 44\,mA$$

El valor de la resistencia de base se calcula con la ley de Ohm para el voltaje base-emisor aplicado por el DIOT-ESP32 a la resistencia de base del transistor, para el caso de corriente máxima y mínima, mostrado en la ecuación 4.2. Para evitar daños al transistor y garantizar que el mismo trabaje en la región de saturación, la resistencia de base R_b tiene que ser mayor a 4,6 y menor a 52,7 ohmios, seleccionando para el diseño una resistencia de 47 ohmios.

$$\frac{3.3\,V - Vbe}{500\,mA} \leq R_b \leq \frac{3.3\,V - Vbe}{44\,mA} \qquad 4.2$$

$$\frac{3.3-1}{500\,mA} \leq R_b \leq \frac{3.3-1}{44\,mA} \qquad 4{,}6\,\Omega \leq R_b \leq 52{,}7\,\Omega$$

Los sensores digitales para pulsadores son alimentados desde un regulador de tensión de 12Vdc a 1A, para que la tarjeta DIOT-ESP32 interprete las señales de éstos sensores, es necesario implementar un divisor de tensión que convierta los valores de 12Vdc a un mínimo de 3Vdc y un máximo de 3.6 Vdc y a una corriente inferior a 200mA; que son los valores lógicos y físicos que utiliza el ESP32. El divisor de tensión es el mostrado en la ecuación 4.3, en donde resolviendo se determina que el valor R_{14} debe ser por lo menos 2.33 veces mayor a R_{15} y no superar 3 veces el módulo de R_{15} .

$$3v \leq \frac{12v * R_{14}}{R_{15} + R_{14}} \leq 3.6 \qquad 2.33\,R_{14} \leq R_{15} \leq 3\,R_{14} \qquad 4.3$$

La corriente del divisor de tensión no debe ser mayor a 200mA por tanto se seleccionan las resistencias R_{14} y R_{15} de tal forma que cumpla esta

condición, tomando valores de resistencias superiores a 100Ω, para condiciones de diseño se establece a R_{15} en 300 Ω por lo que R_{14} tiene que estar entre 770 y 900 Ω, tomando para el diseño una resistencia de 820Ω, ya que es un valor de resistencia comercial.

En la Fig.4. 7 se muestra el diagrama de las conexiones de los elementos del sistema de control de acceso de la empresa Electroservicios Querubín, en donde se observa las conexiones cableadas e inalámbricas del módulo de control. El módulo de control de acceso se conecta de forma cableada a la pantalla, el detector de iris y el sistema de alimentación, los mismos que se instalan dentro de una caja de seguridad con normas de seguridad IP4.

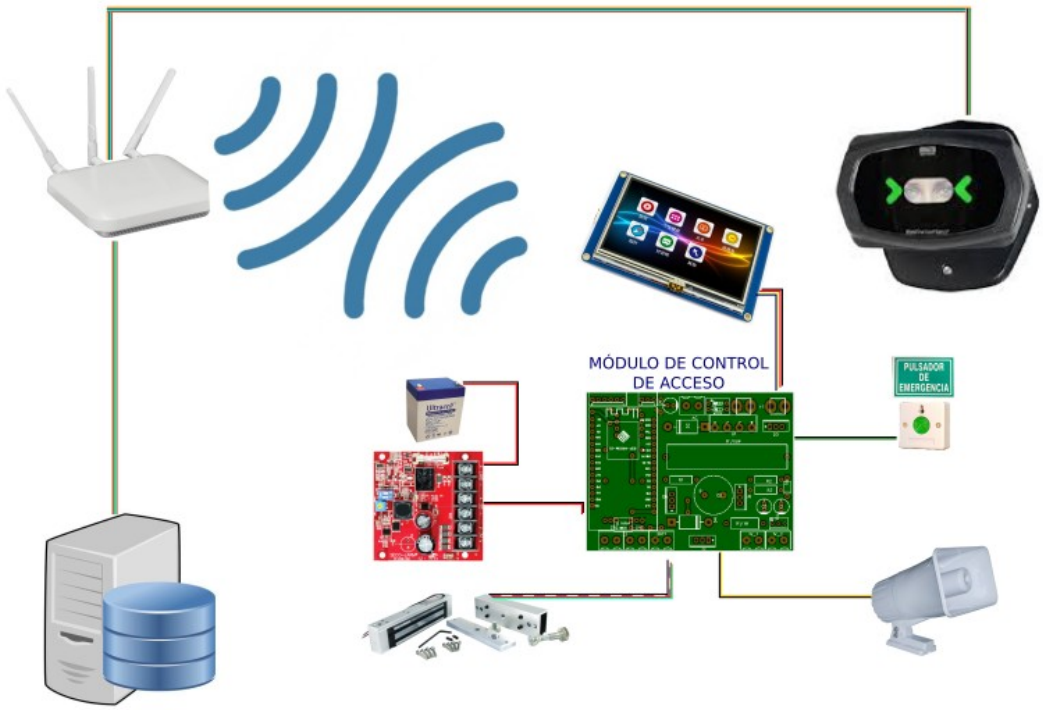


Fig.4. 7: Diagrama físico del sistema de control de acceso.

El cableado necesario para el pulsador de emergencia y la cerradura magnética también es instalado bajo normativas IP4. El sensor de iris tiene una conexión Ethernet con un Access Point de la empresa, a donde se conecta también una

computadora de escritorio que hace las funciones de servidor. Finalmente el Access Point facilita la conexión de datos al módulo de control de acceso mediante Wifi.

4.10 SERVIDOR DE REGISTROS Y PERMISOS

El Servidor de Registros y Permisos es el núcleo del sistema que está diseñado en un servidor LAMP, servidor de código abierto que integra las características de gestión del sistema operativo Linux, servicios web de Apache, programación bajo lenguaje PHP y gestión de base de datos con MySql. El conjunto LAMP analiza el tráfico proveniente del módulo de control de acceso de acuerdo al diagrama de flujo de la Fig.4. 8. Al iniciar el servidor de registros se abre un socket en el puerto 80, el mismo que atiende las peticiones de los clientes de registro y hora, solicitadas desde el módulo de control de acceso.

Primero se consulta la existencia de un cliente "registros", en el caso de existir se obtiene de la petición por medio del protocolo HTTP(POST), el tipo de registro solicitado y un código que identifica al usuario. Con el código de usuario se consulta en la base de datos el nivel de acceso asignado a la persona que se está identificando, o la existencia de la misma en la base. Si el usuario no existe se retorna un mensaje de error al Módulo de Control de Acceso, registrando el evento en la base de datos.

En el caso de que la información del usuario esté en la base de datos, se analiza el tipo de petición recibida, si se trata de una petición de nómina de asistencia, se registra el evento en la base de datos y se retorna al Módulo de Control de Acceso (cliente) una respuesta de proceso correcto. Si el tipo de evento solicitado es de acceso, se utiliza el nivel de accesibilidad devuelto de la base de datos para determinar si tiene permiso o no para acceder al departamento solicitado, retornando en cada caso una respuesta de conceder o denegar acceso hacia el cliente y registrando el evento en la base de datos.

Si no existe un cliente registros, el sistema pasa a analizar la existencia de un cliente

hora mediante el protocolo HTTP(POST) y de ser el caso solo retorna la hora actual del sistema. Si no existen clientes web que soliciten una sincronización (hora), registro de asistencia o solicitud de acceso, el sistema analiza las solicitudes de nuevos registros de usuarios mediante el gestor de base de datos phpMyAdmin.

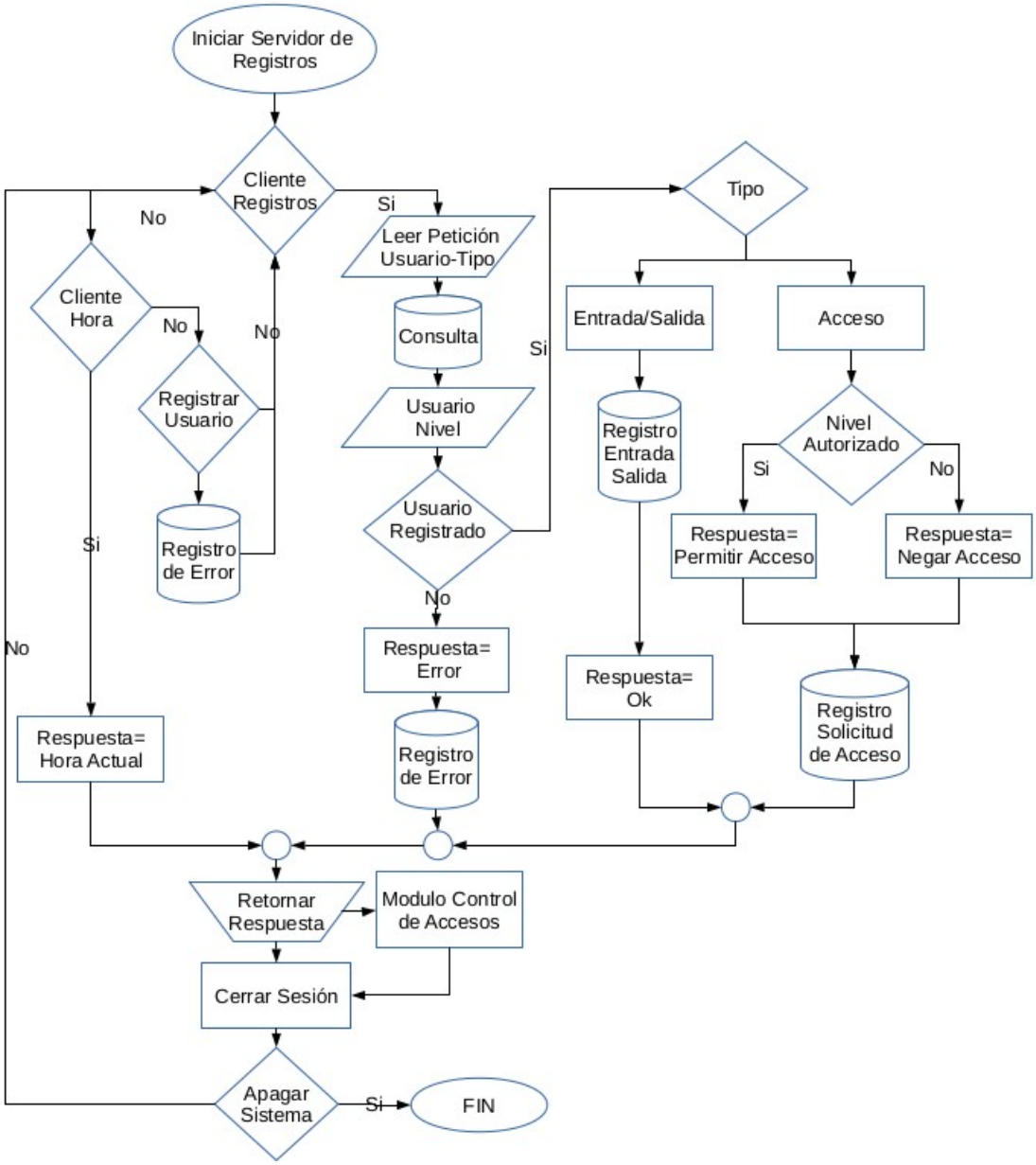


Fig.4. 8: Diagrama de flujo del programa del servidor de registros.

El servidor de registros, instalado en una máquina virtual del servidor local de la empresa, maneja tres funciones principales, dos están programadas en distintos

ficheros de lenguaje PHP v7 y la tercera función utilizada para el registro de nuevos usuarios es administrada con el software Eyenroll.

La primera función ubicada en la dirección web http://IP_SERVER/AccessControl/recepcionPost.php analiza las peticiones de acceso o registro de entrada y salida; la segunda función ubicada en la dirección web http://IP_SERVER/AccessControl/horaActual.php permite sincronizar el tiempo del servidor con el módulo de control de acceso, mostrando en la pantalla del usuario la hora actual del sistema.

El fichero recepciónPost.php escucha las peticiones realizadas por el módulo de control de acceso cuando verifica un match del detector de iris, recibiendo como datos el ÍD del usuario y el tipo de solicitud correspondiente a registro de asistencia o solicitud de acceso a la bodega. Al recibir una solicitud se verifica la existencia del usuario en la base de datos del sistema, si el usuario se encuentra registrado se continúa con el proceso de autenticación mediante los datos devueltos, caso contrario se envía un reporte de error a la pantalla Nextion, registrando el evento en la base de datos.

El proceso de autenticación continúa evaluando el tipo de solicitud realizado, en caso de una solicitud de registro de asistencia se procede almacenando la información en la base de datos y notificando el correcto registro al usuario en la pantalla Nextion. En la solicitud de acceso se evalúa el nivel de acceso del usuario determinando desde la base de datos el departamento en el que trabaja, así a los usuarios de los departamentos de administración de bienes, ventas y gerencia se les autoriza el acceso mientras que a los demás se les bloquea.

Todo intento de acceso o registro solicitado por el módulo de control de acceso al servidor queda almacenado, notificando si fue exitoso o no e incluyendo la fecha y hora de la solicitud.

4.11 INTERFAZ DE ADMINISTRADOR

La Interfaz de Administración del sistema consiste en el grupo de gestión de base de datos que provee phpMyAdmin. En el sistema se crea la base de datos AccessControl que contiene tres tablas: Horarios, Registros y Usuarios, además de un usuario MySql con permisos de lectura y escritura para Administración de la Base de datos. Para el diseño de la interfaz de administración también se utilizaron las Normas NUREG- 0700 Rev. 2 que especifica las guías de revisión para el diseño de interfaces humano-sistemas (HSI) especificadas en el apartado de interfaz de Usuario.

La tabla Usuarios contiene 7 campos relacionados a la información de los usuarios, y son los siguientes:

1. **ÍD.-** Es un identificador único para cada trabajador de la empresa, creado en un formato de cuatro caracteres, dos numéricos y dos alfanuméricos. El ÍD debe ser registrado en el Eyeswipe Nano y en la tabla Usuarios para el correcto funcionamiento. El ÍD es una clave primaria para identificar a los usuarios y crear relaciones con la tabla registros.
2. **CI.-** Es el número de cédula de identificación, creado en un formato de 10 caracteres numéricos.
3. **Nombre.-** Son los nombres completos del usuario.
4. **Apellido.-** Son los apellidos del usuario.
5. **Level.-** Es el nivel de acceso designado a los usuarios del sistema, los trabajadores de las áreas de administración de bienes y ventas tienen un nivel de acceso 5, gerencia un nivel de Acceso 10, y los demás departamentos un nivel de acceso 0.
6. **HorarioM.-** Es el horario matutino asignado al usuario mediante una relación con la tabla Horarios.
7. **HorarioV.-** Es el horario vespertino asignado al usuario mediante una relación con la tabla Horarios.

La tabla Registros almacena la información de todos los eventos producidos en el sistema así como: ingresos, salidas, registros extraoficiales, accesos correctos y accesos errados. Ésta tabla utiliza 4 campos que almacenan la siguiente información:

1. **Número.**- Es el número de identificación del registro
2. **ÍD.-** Es el ÍD de identidad del usuario.
3. **TipoR.**- Es el tipo de registro realizado, corresponde a un código alfanumérico de 4 dígitos, relacionado a clave principal de la tabla horarios en donde se crea registros extras para los eventos de acceso.
4. **Fecha.-** Es la información de fecha y hora actual del sistema al momento de realizar el registro.

La tabla horarios crea horarios establecidos para el ingreso y salida del personal de la empresa, también establece identificaciones del tipo de registro realizado para el caso de eventos de acceso o registros extraoficiales. Ésta tabla tiene los siguientes campos relacionados a:

1. **ÍD_R.**- Es un código alfanumérico de cuatro dígitos que identifica el tipo de horario o registro (Matutino, Vespertino, Acceso)
2. **Ingreso.**- Es la hora máxima establecida para el ingreso del personal.
3. **Salida.**- Es la hora mínima establecida para la salida del personal.
4. **LímiteIn.**- Es el rango de tiempo en minutos establecido para el inicio de registro de entrada antes de la hora máxima.
5. **LímiteSa.-** Es el rango de tiempo en minutos establecido para el inicio de registro de salidas después de la hora mínima.
6. **Días.**- Son los días en los que se debe manejar el horario.

Para el registro de las identificaciones de acceso y extraoficiales, todos los campos distintos al ÍD_R se llenan con ceros o nulos.

Las consultas personalizadas y el cruce de información entre tablas se realizan mediante la relación de la Fig.4. 9. En la relación de tablas, los tipos de horarios son

creados en la tabla Horarios y compartidos a las tablas Usuarios y Registros, también ésta última tabla utiliza los datos del ÍD de usuario para el almacenamiento de los mismos; ésto para evitar la redundancia de información.

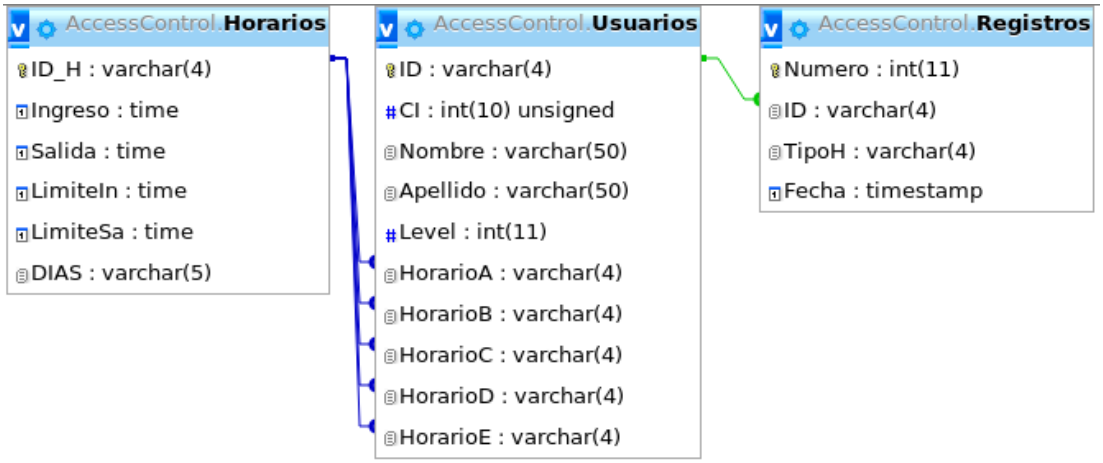


Fig.4. 9: Relaciones de las tablas de la base de datos AccessControl.

4.12 PRESUPUESTO

Los elementos necesarios para la implementación del sistema en la empresa de Electroservicios Querubín de la ciudad de Puyo se muestra en la Tabla4. 9, de acuerdo a los precios establecidos del mercado ecuatoriano.

El salario del ingeniero que realiza el servicio de instalación es el correspondiente al salario mínimo sectorial entregado por el ministerio del trabajo para el año 2018, correspondiente a servicios relacionados con Hardware y Software. El presupuesto total requerido para la instalación del sistema es de 1230.03 dólares.

El precio del diseño se estableció a partir del costo hora-hombre, de acuerdo a los criterios que recomienda la Organización Mundial de la Propiedad Intelectual (OMPI) para medir los esfuerzos necesarios requeridos para completar una tarea. El total de horas hombre en un proyecto se obtiene multiplicando el número de personas asignadas al mismo por el tiempo total que lleva completarlo. Así, para el presente proyecto se estima un promedio de 20 horas semanales durante seis meses con dos investigadores, teniendo un total de 960 horas-hombre. Multiplicando el total de

horas-hombre por el salario mínimo por hora para el diseño de proyectos de software, electrónicos y de telecomunicaciones (2.60), establecido por la tabla de salarios mínimos sectoriales para el 2018 en Ecuador se tiene que el costo total del diseño es de 20502 USD.

Tabla4. 9: Presupuesto requerido para la instalación del Sistema de Control de Acceso.

Item	**Descripción**	**Cantidad**	**Unidad**	**Precio Unitario $**	**Precio Total $**
1	Sensor Eyelock Eyeswipe Nano	1	c/u	520.00	520.00
2	Pantalla Nextion NX3224T024	1	c/u	23.00	23.00
3	Sirena DSC SD 30W	1	c/u	15.99	15.99
4	Cerradura Acces Pro MAG600S	1	c/u	43.75	43.75
5	Regulador de Tensión LM7805	1	c/u	0.50	0.50
6	Resistencia de 820 Ω	2	c/u	0.10	0.20
7	Resistencia de 330 Ω	2	c/u	0.10	0.20
8	Capacitor de 47uF	2	c/u	0.23	0.20
9	Regulador de Tensión LM7812	1	c/u	0.50	0.50
10	Resistencia de 47Ω	2	c/u	0.10	0.20
11	Transistor BD135	2	c/u	0.37	0.74
12	Puertos de conexión Molex kk	2	c/u	0.80	1.60
13	Puertos de conexión 2p Bornera	5	c/u	0.23	1.15
14	Espadines header female	1	c/u	0.50	0.50
15	Regulador de carga de baterías	1	c/u	34.00	34.00
16	Módulo DIOT-ESP32	1	c/u	13.00	13.00
17	Baquelita 8.5x10 cm^2	1	c/u	0.78	0.78
18	Estaño	2	metros	2.70	5.40
19	Ácido clorhídrico	1	onza	1.80	1.80
20	Switch de encendido	1	c/u	0.33	0.33
21	Cable UTP CAT. 6	20	metros	0.87	17.40
22	Servicio de Instalación	1	mes	417	417
	Subtotal				1434.24
	IVA 12%				131.79
	Total				1230.03

4.13 FUNCIONAMIENTO DEL SISTEMA.

A continuación se realiza una presentación del funcionamiento del sistema de control de acceso por reconocimiento de Iris desde la perspectiva del usuario y administrador, también se presenta una evaluación estadística de la seguridad y comodidad del sistema. En el Anexo 1 se visualiza las imágenes del prototipo diseñado.

4.13.1 Enfoque desde el Usuario.

El enfoque del funcionamiento del sistema desde la perspectiva del usuario en el proceso de autenticación para solicitar un registro o acceso, se canaliza desde las funciones de la interfaz gráfica de la pantalla Nextion visualizada en la Fig.4. 10. En la pantalla inicial se tiene un panel que permite seleccionar la función de acceso o registro e indica la hora actual del sistema sincronizado con el servidor.

Fig.4. 10: Funciones de la interfaz gráfica del usuario.

El diseño del software que controla la interfaz gráfica del sistema en la pantalla Nextion se desarrolló bajo las recomendaciones de la norma ISO 9241, que especifica criterios ergonómicos para oficinas con terminales visuales. La interfaz es creada con una organización jerárquica, colocando la información o controles dentro de categorías lógicas. También, se presenta y oculta la información y los controles

según el contexto en el que se encuentra el sistema; así se busca encontrar la distribución de los elementos más adecuada a fin de que las personas ejecuten sus actividades eficientemente.

En la pantalla uno, al seleccionar la opción de registro se muestra la pantalla dos que tiene un panel de selección entre registro de entrada o salida. Al seleccionar la opción de ingreso o salida del panel dos o el de acceso del panel uno, el usuario debe proceder a autenticarse en el sensor de Eyelock.

El sensor identifica al usuario cuando éste ubica su mirada en dirección a un espejo del sensor, a una distancia aproximada entre 6 y 20 centímetros como se muestra en la Fig.4. 11. Cuando la autenticación es correcta el sensor activa un tono sonoro y torna las luces a color verde para notificar al usuario que el proceso de identificación fue exitoso.

Fig.4. 11: Uso del sensor de Reconocimiento de iris Eyeswipe-Nano[24].

En el proceso de autenticación la pantalla muestra el panel tres de la Fig.4. 10, esperando una respuesta del sensor. En los procesos exitosos la pantalla cambia de forma temporal al panel 4A indicando al usuario que se ha realizado el registro en la base de datos, en el caso de solicitud de acceso se abre la cerradura magnética. Si el usuario no se encuentra registrado, se muestra el panel de error 4B durante un

periodo de dos segundos.

En el caso de accesos no autorizados o cuando no se establece conexión son el servidor de registros, determinando que el registro o solicitud no se ejecutó de forma correcta, se muestra temporalmente en pantalla el panel de error 4C. Después de mostrar en pantalla los mensajes de los procesos de autenticación exitosos y erróneos, se regresa de forma automática al panel 1.

El proceso de autenticación se basa en el diagrama de la Fig.4. 12, el sistema utiliza las librerías de OpenCV orientadas a visión por computadora para generar los distintos procesos de forma automática.

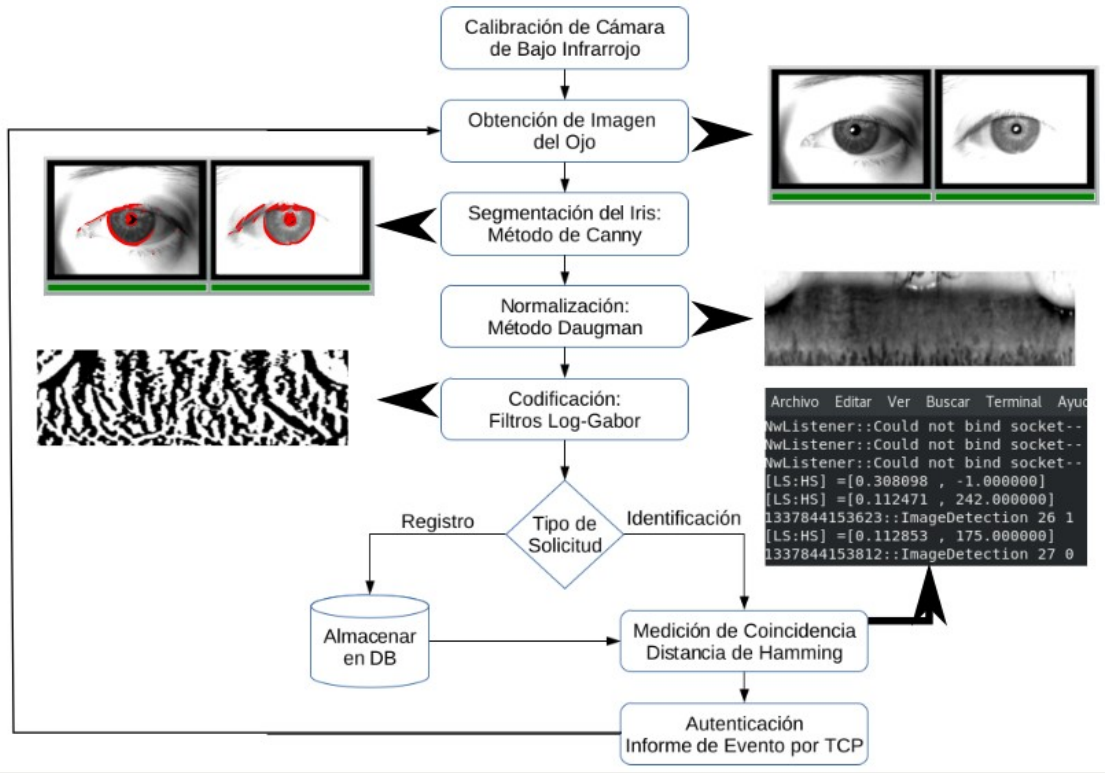


Fig.4. 12: Proceso de Autenticación de usuarios por reconocimiento de iris.

De forma inicial, al encender el dispositivo, se calibra internamente una cámara de bajo infrarrojo para adaptarse a las condiciones de luminosidad del ambiente, también se configuran los controladores del sistema que permiten adquirir imágenes,

establecer una comunicación ethernet y controlar el generador de tonos y los LEDs. En el proceso de autenticación o registro de nuevos usuarios se obtiene una imagen tomada por la cámara de infrarrojo cercano, a la que se aplica el método de Canny para detectar los bordes y de ésta forma segmentar el iris.

Al iris segmentado se aplica el algoritmo de Daugman mostrado en la ecuación 4.4

$$max_{(r,x_0,y_0)}\left|G_\sigma(r)*\frac{\delta}{\delta r}\oint_{r,x_0,y_0} I\frac{(x,y)}{2\pi r}ds\right| \qquad 4.4$$

Donde:
I (x, y) es la imagen del ojo,
r es el radio para búsquedas sobre la imagen (x, y),
G (r) es una función de suavizado de mediante un filtro de Gauss.
x_0, y_0 Son las coordenadas centrales de la imagen.

El operador busca en el dominio (x; y) de la imagen el máximo valor en la derivada parcial borrosa con respecto al radio creciente r, de la integral de contorno normalizada de I (x;y) a lo largo de un arco circular ds de radio r y coordenadas centrales (x_0, y_0). El símbolo * denota la convolución entre G (r) y el resultado de la derivada.

El algoritmo comienza a buscar en la imagen sobre el dominio (x, y) empezando desde la pupila, para detectar el cambio de los valores máximos de píxel, que ocurren cuando se pasa de la pupila a la esclerótica.

De forma posterior al resultado obtenido se le aplica la transformada de Hough expresada en la ecuación 4.5, que es una técnica de extracción de características utilizada en análisis de imágenes, visión por computadora y procesamiento de imágenes digitales para encontrar todo tipo de figuras que puedan ser expresadas matemáticamente, tales como rectas, circunferencias o elipses.

$$(x-x_i)^2+(y-y_i)^2=r_i^2 \quad 4.5$$

Donde:

(xi, yi) son coordenadas centrales,

r es el radio.

En general, y el ojo sería modelado por dos círculos, pupila y limbo (región del iris), y dos parábolas, párpados superiores e inferiores. El algoritmo comienza a detectar los párpados desde la dirección horizontal, luego detecta la pupila y el límite del iris por la dirección vertical.

Para finalizar la normalización se transforma las coordenadas cartesianas de la imagen resultante a coordenadas polares de la forma especificada en las ecuaciones 2.1 y 2.2

El proceso de codificación utiliza los filtros de Log-Gabor generando un mapa de bits en forma de matriz, que se almacena en la base datos interna del dispositivo, teniendo la capacidad de almacenar hasta 10.000 registros; ésto cuando se realiza un nuevo registro de usuario. Para el proceso de autenticación se compara los datos de la matriz obtenida con las almacenadas mediante la distancia de Hamming. Si el resultado de la distancia de Hamming calculada en cierta comparación es menor a 0.3, implica una autenticación correcta y se envía la información del usuario autenticado (Nombre_Apellido Código)a un servidor TCP.

4.13.2 Enfoque de Administración.

El administrador del sistema debe registrar a los usuarios en el servidor de registros y en la base de datos interna del Eyeswipe Nano, asegurando que la información sea la misma. El registro de los usuarios en el sensor de iris se realiza con el software Eyenroll, facilitado de forma gratuita por la misma empresa distribuidora de Eyelock; la base de datos de Eyenroll permite registrar tres campos alfanuméricos, éstos son utilizados para el nombre, cédula e ÍD de usuario.

En el servidor de registros, el administrador ingresa un nuevo usuario mediante la interfaz web mostrada en la Fig.4. 13 (2). En la información ingresada en la tabla, el ÍD de usuario es utilizado para sincronizar los datos del Eyeswipe y los permisos entregados por el servidor. En adición el administrador puede crear horarios en el formulario de la Fig.4. 13 (1) para regir las nóminas de asistencia, facilitando el cálculo de sanciones económicas por atrasos o faltas. La tabla registros es actualizada de forma por software cuando se detecta un evento de registro o acceso.

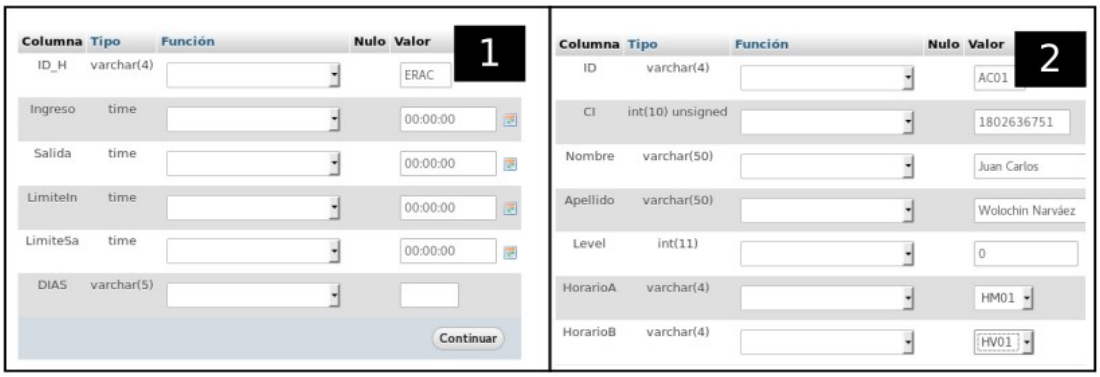


Fig.4. 13: Interfaz gráfica de gestión de la base de datos del servidor de registros

	Numero	ID	TipoH	Fecha
Editar Copiar Borrar	283	01	IMO1	2018-04-13 13:24:36
Editar Copiar Borrar	284	01	IMO1	2018-04-13 13:24:38
Editar Copiar Borrar	285	01	SOAC	2018-04-13 13:25:00
Editar Copiar Borrar	286	03	SOAC	2018-04-13 13:25:24
Editar Copiar Borrar	287	03	SMO1	2018-04-13 13:29:02
Editar Copiar Borrar	288	03	SMO1	2018-04-13 13:29:22
Editar Copiar Borrar	289	01	SSNN	2018-04-13 13:37:05
Editar Copiar Borrar	290	01	SSNN	2018-04-13 13:37:11

Fig.4. 14: Sección de respuesta a la consulta devuelta de la tabla registros.

La información de la base de datos es visualizada mediante consultas realizadas en phpMyAdmin, debido a las tablas relacionadas se puede personalizar los datos que se

quieren obtener de las consultas, sin embargo la información principal está dentro de la tabla Registros. En la Fig.4. 14 se muestra una sección de una consulta realizada a la tabla registros, en donde se le solicita que retorne toda la información.

Como ejemplo de análisis se toma el registro 287 y se determina que pertenece al usuario con ÍD 03, quien realizó una solicitud de acceso correcta (SOAC) un día 04 de abril de 2018 a las 13 horas 25 minutos y 24 segundos.

4.13.3 Resultados

La confiabilidad del sistema se evaluó mediante dos programas de análisis de tráfico de red: Wireshark y Net Analizer, determinando la seguridad del mismo frente a ataques de Hacking. Los programas capturan los paquetes transmitidos entre el servidor, el módulo de control y el Eyeswipe, permitiendo visualizar los datos transmitidos entre ellos al producirse un proceso de autenticación, cuando se solicita un acceso a la bodega de la empresa que responde con una autorización exitosa.

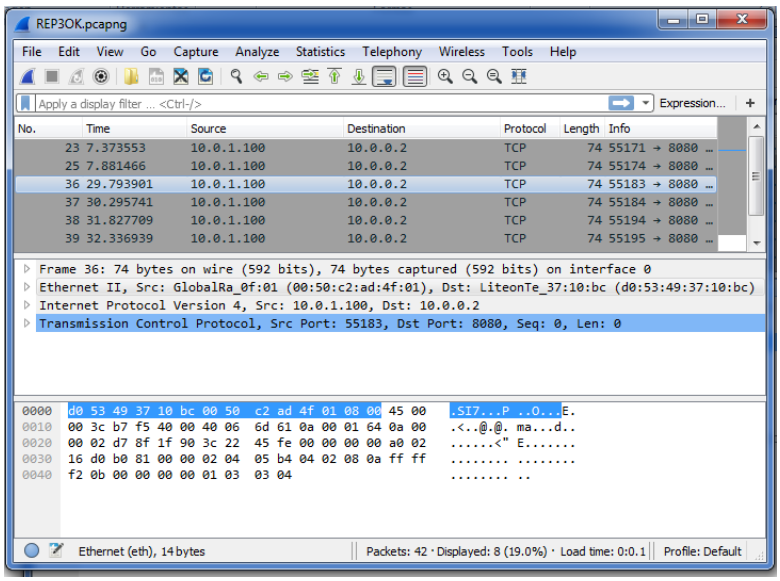


Fig.4. 15: Captura de paquetes en el envío de datos entre el Eyeswipe y el Módulo de Control en una autenticación.

En la Fig.4. 15 se observa el paquete de datos enviado desde el Eyeswipe-Nano hacia el Módulo de Control de Acceso capturado por el software Wireshark cuando se

produce un “match”.

El puerto destino utilizado para la transmisión de datos es el 8080, la información es transmitida utilizando el protocolo TCP y un protocolo de cifrado de la información entre terminales; evitando de ésta manera la posibilidad de capturar la trama específica que se envía para la apertura de puertas.

El software Wireshark, no pudo capturar el tráfico de red entre el Módulo de Control de Acceso y el Servidor, sin embargo utilizando Net-Analizer es posible capturar las tramas de las peticiones POST, realizadas mediante el protocolo HTTP.

Fig.4. 16: Captura de datos de la cabecera HTTP enviada de Módulo de Control de Acceso al Servidor.

En la Fig.4. 16 en la trama de color azul se observa los datos capturados por el software Net-Analizer correspondiente a la cabecera HTTP enviada desde el Módulo de Control de Acceso al servidor para consultar en la base de datos el nivel de

accesibilidad de un usuario (Daniel Alvarado).

En color rojo me detalla la respuesta que el servidor entrega al Módulo de Control de Acceso, devolviendo el valor del nivel de accesibilidad en una cabecera de respuesta de conexión exitosa de una petición HTTP.

Los datos mostrados en la imagen de la Fig.4. 16 son de una captura de prueba realizada como muestra de la forma de transmisión de datos que sucede entre el Servidor y el Módulo sin encriptar. Para establecer un nivel de mayor seguridad los datos correspondientes al nombre de usuario y código de usuario son encriptados con un código base de 64 bits y una palabra clave de 16 bytes, teniendo como resultado las tramas de petición y respuesta mostradas en la Fig.4. 17, en donde el nombre el nombre de usuario y código solo pueden interpretarse en el receptor, donde se tiene el algoritmo de desencriptado.

Fig.4. 17: Captura de datos de la cabecera HTTP enviada de Módulo de Control de Acceso al Servidor con datos encriptados.

4.13.4 Análisis de Resultados

En la Fig.4. 18 se observa un análisis del porcentaje de falsas negaciones del sistema en función del tiempo, realizada en pruebas de funcionamiento durante las cuatro primeras semanas después de la instalación del prototipo. En la primera semana el porcentaje de errores es del 10.09%, en la segunda semana se reduce el porcentaje de error al 6.1%, la tercera al 4,17% y finalmente en la cuarta semana el error se reduce hasta el 3.63%. La reducción del porcentaje de error se determina como una causalidad de la adaptación del usuario al sistema, determinando que el usuario se familiariza con el sistema.

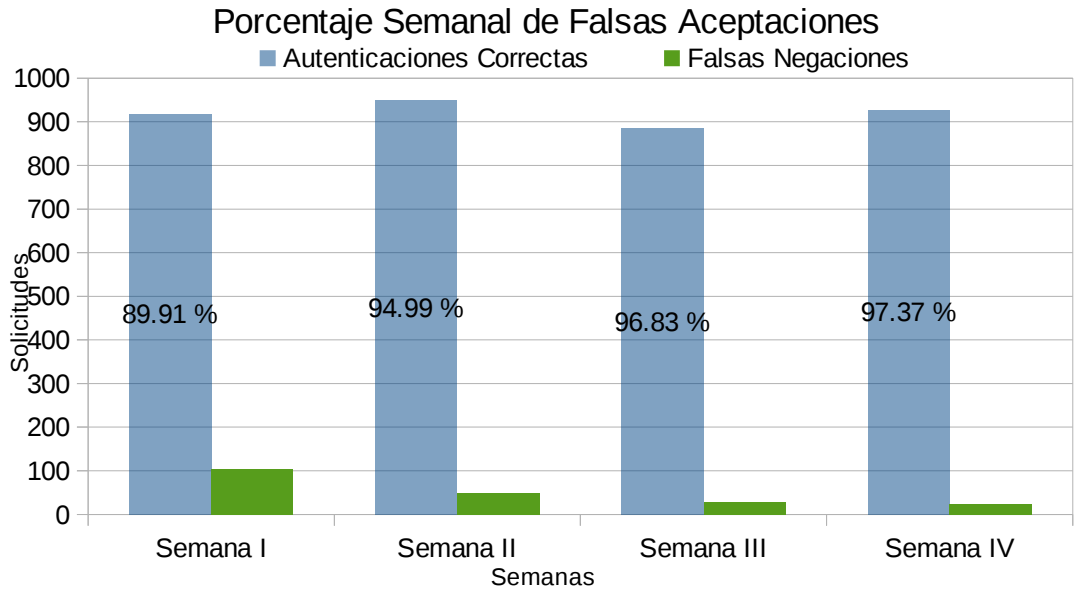


Fig.4. 18: Porcentaje semanal de falsas negaciones del sistema

Después de las cuatro semanas de prueba se evaluó el tiempo que le toma a un usuario ejecutar una petición de acceso, para el efecto se programó en el módulo de control de acceso un timer que mide el tiempo desde que el usuario inicia la solicitud de acceso presionando el botón en la pantalla táctil, hasta cuando el servidor LAMP retorna la respuesta de consentimiento o negación.

En la Fig.4. 19 se observa el tiempo promedio medido durante 14 días posteriores a las cuatro semanas de pruebas y adaptación de los usuarios, que le toma al sistema ejecutar una petición de acceso. El tiempo medio que le toma al sistema varía entre 4 y 7 segundos teniendo un valor promedio general de 5.74 segundos.

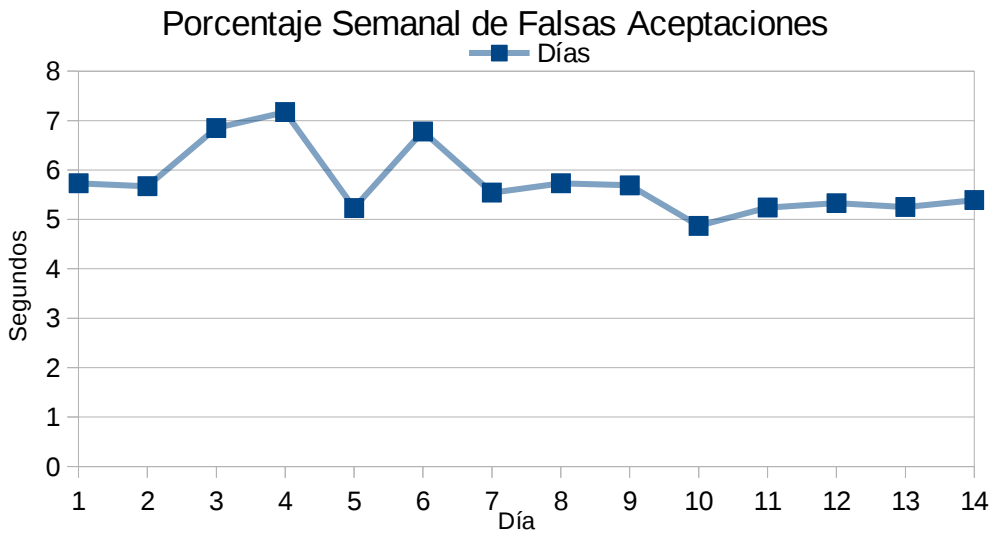


Fig.4. 19: Tiempo promedio de ejecución de peticiones de acceso del sistema

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Los sistemas de autenticación que utilizan patrones físicos del iris o retina son los más fiables en referencia a seguridad de identificación debido a que su probabilidad de error en falsas aceptaciones está alrededor de 6.7×10^{-7} cuando se utiliza un ojo y elevándose de forma cuadrática al utilizar los dos.

- La facilidad de uso de un sistema de control de acceso incrementa el grado de aceptación de los usuarios, el uso de micro-controladores de de 32 bits a una frecuencia de oscilación de 160MHz, considerados de alta velocidad de procesamiento, reduce el tiempo de operación, teniendo como resultado mayor comodidad del usuario. Los micro-controladores utilizados de forma externa al identificador de iris, permiten obtener datos suficientes para migrar de forma parcial el sistema hacia funciones diseñadas en software libre, facilitando el desarrollo y mejora de la aplicación y reduciendo los costos de implementación.

- El porcentaje de falsas aceptaciones en la prueba del sistema es 0%, estableciendo así la alta confiabilidad del mismo. El porcentaje promedio de falsos rechazos es del 5.51%, teniendo a reducir en función del tiempo, debido a la adaptación del usuario al sistema. Así en un periodo de pruebas de 4 semanas el porcentaje de falsos rechazos se reduce en un 7,46% con la

tendencia a estabilizarse en un promedio de error en el margen de 3% y 4%.

- El nivel de seguridad en la empresa se incrementa con la implementación del control de acceso por identificación de iris. El registro de accesos permite obtener información de fecha y hora de ingresos a las instalaciones, que ante la identificación de posibles pérdidas, facilita la revisión de vídeo de seguridad mediante el sistema de monitoreo por cámaras, teniendo mayor probabilidad de identificar al posible responsable.

5.2 RECOMENDACIONES

- Debido a que los equipos de identificación de iris son de alto costo, la implementación de un sistema con esta tecnología representa grandes inversiones económicas, por lo que se debe utilizar sistemas de control de acceso biométricos de detección de iris solo en zonas donde se requiere un alto control de seguridad.

- Mantener una condición de iluminación adecuada y constante en el punto de funcionamiento del equipo de reconocimiento de iris con la finalidad de mejorar la estabilidad del equipo de reconocimiento de iris. Mantener el equipo lejos de fuentes de luz infrarroja (solar) para evitar interferencias.

- En las grandes empresas, donde se requiere que un identificador de iris autentique a más de mil usuarios se debe utilizar sensores con un tiempo de reconocimiento menor a un segundo. A un menor tiempo de reconocimiento el grado de aceptación de usuario al sistema se incrementa.

- Las instalaciones y cableado de todos los equipos utilizados en el sistema de control de acceso deben utilizar protección de componentes eléctricos y electrónicos basadas de forma mínima en normas IP4, para entregar protección al sistema ante condiciones ambientales de polvo, agua y asegurar la infraestructura ante ataques de vandalismo.

Bibliografía

[1] L. DELCAMPO, T. ROJO (2016) "Seguridad en América", México, [online] Disponible:http://www.seguridadenamerica.com.mx/noticias/de-consulta/articulos-destacados-de-seguridad/23986-tendencias-en-control-de-acceso, Último Acceso:15 Nov. 2017.

[2] DOINTECH SAS (2015) "Automatización Seguridad y Control", Bogotá - Colombia, [online] Disponible:http://www.dointech.com.co/control-personal.html, Último Acceso:15 Nov. 2017.

[3] Z. V. VARGAS VERGARA, "Sistema de Control de Acceso y Monitoreo con la Tecnología RFID para el departamento de Sistemas de la Universidad Politécnica Salesiana Sede Guayaquil" , Guayaquil-Ecuador, Julio 2013.

[4] J. J. SAAVEDRA GUADA, "Diseño e Implementación de un Sistema de Control de Acceso" , Sartenejas-Venezuela, 2006.

[5] D. A. CADENA MORÁN, "Diseño e Implementación de un Sistema de Control e Inventario Electrónico a Través de la Internet Basado en la Tecnología RFID para los Laboratorios del DEEE-ESPE" , Sangolquí-Ecuador, 2011. Disponible: https://repositorio.espe.edu.ec/bitstream/21000/4697/2/T-ESPE-032816-A.pdf, 15 Nov. 2017.

[6] J. A. ALVARADO SÁNCHEZ, "Sistema de Control de Acceso con RFID" , México D. F., Enero 2008. Disponible: https://www.cs.cinvestav.mx/TesisGraduados/2008/tesisJorgeAlvarado.pdf, 15 Nov. 2017.

[7] A. J. BALSERO MENESES, "Diseño e Implementación de un Prototipo para el Control de Acceso en la Sede de Ingeniería de la Universidad Distrital Francisco José de Caldas Mediante el Uso de Torniquetes Controlados por Carnet con Tecnología NFC y Lector Biométrico de Huella Dactilar" , Bogotá-Colombia, 2016. Disponible: http://repository.udistrital.edu.co/bitstream/11349/3430/1/VargasGarciaCristianGerman2016.pdf, 15 Nov. 2017.

[8] J. E. VELÁSQUEZ VALENCIA, A. A. LINARES JARAMILLO, "Soluciones Inteligentes para el Control de Acceso Físico Mediante el uso de Tecnología

Biométrica" , Pereira, 2013. Disponible: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4090/0053682V434.pdf, 15 Nov. 2017.

[9] J. J. GARCÍA GARRIGOS, "Sistema de Autenticación Biométrica de Huella Dactilar asistido por Interfaz de Voz para el Control de Accesos" , Valencia-España, Noviembre 2006. Disponible: https://www.researchgate.net/profile/Juan_Garcia_Garrigos/publication/259705766_Sistema_de_Autenticacion_Biometrica_de_Huella_Dactilar_asistido_por_Interfaz_de_Voz_para_el_Control_de_Accesos/links/02e7e52d69a04f3a57000000/Sistema-de-Autenticacion-Biometrica-de-Huella-Dactilar-asistido-por-Interfaz-de-Voz-para-el-Control-de-Accesos.pdf, 15 Nov. 2017.

[10] JAIME R. MICHILENA, ESTEFANÍA G. TORRES, "Sistema Electrónico para Control de Acceso de Personas por Reconocimiento de Huella Dactilar, con Autenticación Remota en Base de Datos a través de una WLAN" , Ibarra-Ecuador, Agosto 2012. Disponible: http://repositorio.utn.edu.ec/bitstream/123456789/1060/2/04%20RED%20015%20Art_Sistema_electronico_Tenc.pdf, 15 Nov. 2017.

[11] J. E. GUTIERREZ RICARDO, "Estudio de Factibilidad para el Control de Acceso Biométrico, en una Empresa Empleando Lectores de Huella Digital" , Bogotá-Colombia, 2007. Disponible: http://repository.lasalle.edu.co/bitstream/handle/10185/2158/T91.07%20G985e.pdf?sequence=1, 15 Nov. 2017.

[12] M. S. GARCÍA VÁZQUEZ, A. A. RAMÍREZ ACOSTA, "Avances en el Reconocimiento de Iris: Perspectivas y Oportunidades en la investigación de Algoritmos Biométricos", Revista Computación y Sistemas Vol. 16 No 3,,267-276.

[13] A. BROCHERO ÁLVAREZ, S. LÓPEZ ORTIZ, M. GONZÁLEZ CASTRILLÓN, H. WILLIAM PEÑUELA, "Sistema de Lectura y Análisis de Iris" , , Oct. 2014.

[14] S. YONEKURA BAEZA, C. PÉREZ FLORES, "Evaluación y Mejora de un Sistema de Reconocimiento de Iris a Distancia Utilizando Cámara de Alta Resolución" , 2014.

[15] P. TOMÉ GONZÁLEZ, "Reconocimiento Automático de Patrones de Iris" , , Jun. 2018.

[16] TECNO SEGURO MAGAZIN DIGITAL (2018) "¿Qué es un Sistema de Control de Acceso? ", [ONLINE] Disponible: https://www.tecnoseguro.com/faqs/control-de-acceso

[17] ITIL, OFFICE OF GOVERMMENT COMMERCE, " Operación del Servicio", The Stationary Office,2009,237

[18] J. VAN BON, A. JONG, A. KOLTHOF, M. PIEPER, R. TJASSING, A. VEEN, T. VERHEIJEN, " Operación del Servicio Basada en ITIL V3- Guía de Gestión", Van Harren Publishing,2008,pp. 113-115

[19] J. RODRÍGUEZ FERNANDEZ, " Circuito Cerrado de Televisión y Seguridad Electrónica", Paraninfo,2013,pp. 122-128

[20] A. D. AVILÉS SALAZAR, K. L. COBEÑA MITE, L. CÓRDOVA RIVADENEIRA, "Diseño e Implementación de un Sistema de Seguridad a través de Cámaras, Sensores y Alarma, Monitorizado y Controlado Telemétricamente para el Centro de Acogida PATIO Mi Pana, Perteneciente a la Fundación Proyecto Salesiano" , 2015.

[21] Cuadernos de Seguridad (Abril 2017) "Sistemas de Control de Accesos y sus Componentes", [ONLINE] Disponible: https://cuadernosdeseguridad.com/2017/04/sistemas-control-accesos-componentes-lsb/#, Último Acceso:16 Ago 2018 .

[22] A. MORA PÉREZ, I. IBARRA BERROCAL, L.OJADOS GONZALES, "Gestión de la Prevención. Control de Accesos" , , 2016. http://repositorio.upct.es/bitstream/handle/10317/5636/tfm-mor-ges.pdf?sequence=3, .

[23] E. CASTRO LÓPEZ, L. JIMÉNEZ ORTEGA, M. RODRÍGUEZ PÉREZ, "Control de Acceso y Seguridad por Código de Barras" , , 2005 México D.F.. http://tesis.ipn.mx/handle/123456789/23.

[24] EYELOCK, " Tecnología avanzada de autenticación de irispara empresas, gobiernos y consumidores.", ,2016,1-2

[25] L. FLORIAN CRUZ, R. CARRANZA ATHÓ, "Reconocimiento del Iris", Tóp. Esp. Proc. Gráfico, Trujillo-Perú,2006,pp. 3-7.

[26] LUCAS D. TERISSI, LUCAS CIPOLLONE, PATRICIO BALDINO, "(Mar. 2006), “Sistema de Reconocimiento de Iris”", Revista Argentina de Trabajos Estudiantiles, Vol. 1 No 2,, pp. 1-4.

[27] M. GONZÁLEZ URBANO, "“Reconocimiento de Iris”", Tesis de Ingeniería, Universitat de Barcelona, Barcelona-España,

[28] R. SÁNCHEZ REILLO, "El Iris Ocular como Parámetro para la Identificación

Biométrica" , Sep. 2000.

[29] J. F. CANNY, "“Finding edges and lines in images,” " , , 1983. , .

[30] R. C. GONZÁLEZ R. E. WOODS, "Tratamiento Digital de Imágenes", . Wilmington, Delware: Addison-Wesley / Diaz de Santo,1996,

[31] J. G. DAUGMAN, "High confidence visual recognition of persons by a test of statical independence", IEEE Transactions On Pattern Analysis and Machine Intelligence, vol. 15, no. 11,Nov. 1993.

[32] D. GABOR, "Theory of communication", J. Institute ofElectrical Engineer, vol. 93,,pp. 429–459, 1946.

[33] O. A. SÁNCHEZ MACHADO, J. R. GONZÁLEZ GONZÁLEZ, "Control de Acceso Basado en Reconocimiento de Iris", Corporación Universitaria Tecnológica de Bolívar, Cartagena de Indias,2003,pp. 27, 45-48.

[34] FINEPRINT (2015) "Ssitemas Electrónicos", Disponible: http://iesodrapisuerga.centros.educa.jcyl.es/sitio/upload/SISTEMAS_ELECTRONICOS.pdf, Último Acceso: 16 Ago. 2018 .

[35] R. COBO () "El ABC de la Automatización", Disponible: http://www.aie.cl/files/file/comites/ca/abc/hmi.pdf, Último Acceso:16 Ago. 2018.

[36] RNDS () "Instalación de Cerraduras Electromagnéticas", Disponible:http://www.rnds.com.ar/articulos/045/rnds_164w.pdf, Último Acceso:16 Ago. 2018.

[37] General Villamil S/Ny Francisco de Orellana Puyo-Ecuador, "Electroservicios Querubín".

[38] M. S. GARCÍA VÁZQUEZ, A. A. RAMÍREZ ACOSTA, "Avances en el Reconocimiento de Iris: Perspectivas y Oportunidades en la investigación de Algoritmos Biométricos", devGuide.net Ltd,2012,99

ANEXOS

Anexo 1: Imágenes del Prototipo del Sistema de Control de Acceso.

En la Ilustración 1 se muestra distintas situaciones de funcionamiento del sistema de reconocimiento de iris en el sistema de control de acceso. En la Ilustración 1(1) se observa el sensor Eyeswipe cuando no se ha establecido una conexión de red, en el caso dado, aún al estar energizado, el sensor no enciende las luces. La Ilustración 1(2) es un ejemplo del funcionamiento cuando el detector de iris genera un error en el reconocimiento del usuario; el error es producido por un movimiento indebido en el momento de la lectura y los LEDs del Eyeswipe se tornan de color rojo.

En la Ilustración 1(3) se observa el Eyeswipe en etapa de reconocimiento; cuando el detector de iris determina la presencia de un sujeto y empieza a procesar la información del iris, la luz de los LEDs se torna de color azul. La Ilustración 1(4) muestra al sensor en el caso de un "match", que es el evento dónde la autenticación se da de forma correcta y el usuario finalmente es identificado; en ésta condición las luces de los LEDs se vuelven de color verde.

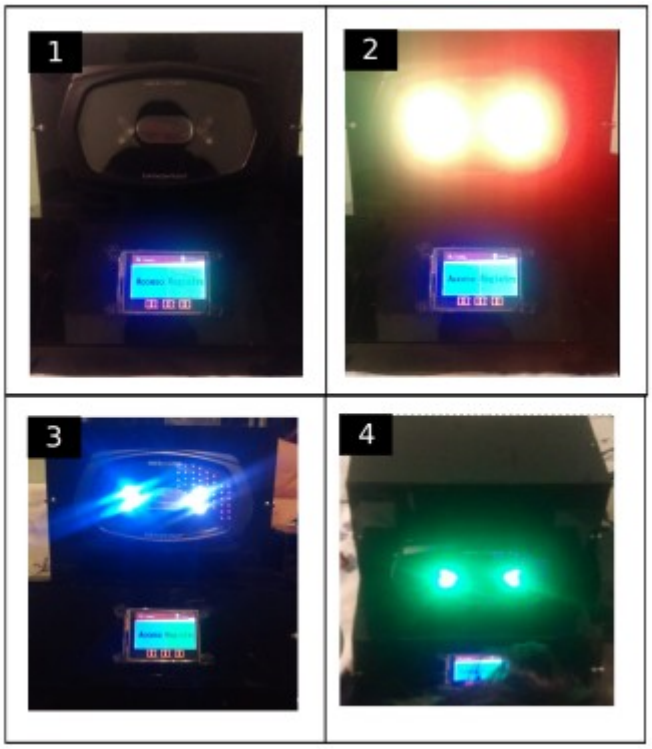


Ilustración 1. Imágenes del sensor de reconocimiento de iris para el Sistema de Control de Acceso.

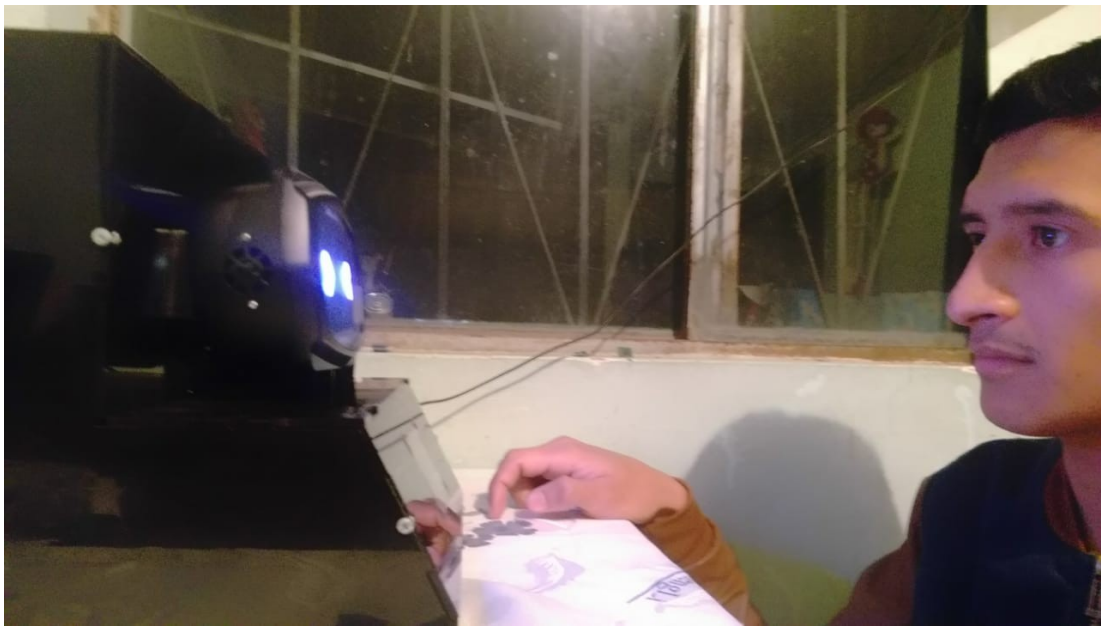


Ilustración 2 Inicio del proceso de autenticación

Ilustración 3 Proceso de reconocimiento.

En la *Ilustración 2 se observa el inicio de un proceso de autenticación de un usuario, el mismo ubica su rostro a una distancia entre los 50 y 70cm de distancia del dispositivo, localizando sus ojos de forma ortogonal al sensor de iris. En la Ilustración 3 se observa el proceso de reconocimiento, en el que por unos pocos segundos las luces del equipo toman un color azul hasta llegar a la Ilustración 4 en donde de forma final se identifica al usuario generando el "match".*

Ilustración 4. Usuario Identificado.

Anexo 2: Software del módulo de control de acceso.

El software del Módulo de Control de Acceso es programado en el IDE de Arduino, el mismo está compuesto por métodos que permiten la ejecución de procesos como clientes y servidores web. A continuación se explica las funciones implementadas en el software que rige el sistema desde los módulos de control de accesos.

El código mostrado a continuación es el encabezado para configuración del dispositivo a programar y creación de variables locales y globales. Se incluye la librería "Wifi" para el manejo de las funciones de conectividad de Arduino con Wifi, y la librería "HardwareSerial.h" que es una librería exclusiva del módulo ESP32 que permite manejar los puertos de comunicaciones serie. En HardwareSerial MySerial(1); se especifica que se utilizará el puerto USART 1 para controlar la pantalla. Se crean variables de control de tiempo, que permiten ejecutar funciones periódicas y se establece variables con los datos de la red inalámbrica.

```
#include <WiFi.h>
#include <HardwareSerial.h>
#include <Ticker.h>
HardwareSerial MySerial(1);
Ticker reloj;
const char* ssid= "INTERNET CNT";
const char* password = "";
const char* host = "10.0.0.200"; // Direccion ip del Servidor Remoto
byte leernextion[7];
WiFiServer server(8080);
IPAddress ip(10, 0, 0, 2);
IPAddress dns(10, 0, 0, 1);
IPAddress gateway(10, 0, 0, 1);
IPAddress subnet(255, 255, 0,0);
```

En el método de configuración setup de Arduino, se configura los pines de entrada y salida para leer los sensores, activar sirenas y cerraduras. De forma posterior se establece la conexión inalámbrica, se inicializa el servidor y se asigna la función relojActual a una ejecución periódica a una frecuencia de 1HZ.

```
void setup() {
pinMode(2, OUTPUT);
pinMode(5, OUTPUT);
pinMode(15, OUTPUT);
```

```
pinMode(4, OUTPUT);
ledcSetup(0, 50, 10);
ledcAttachPin(5,0);
ledcWrite(0,32);
MySerial.begin(9600, SERIAL_8N1, 16, 17);
WiFi.config(ip, dns, gateway, subnet);
WiFi.begin(ssid, password);
        while (WiFi.status() != WL_CONNECTED) {
        delay(250);
        digitalWrite(2,HIGH);
        delay(250);
        digitalWrite(2,LOW);
        }
digitalWrite(2,HIGH);
server.begin();
reloj.attach(1, relojActual);
}
```

En el método de peticionPost, se se crea una trama que permite ejecutar una petición como cliente web. La función recibe los datos de match del Eyeswipe que son id, nombre, apellido y los concatena en una variable con la estructura adecuada para ejecutar una petición POST del protocolo HTTP.

```
void peticionPost(char* id, char* nombre, char* apellido, char* idxx){
char outbuf[500];
char trama[500];
char* cabeceraPost= "POST /AccessControl/recepcionPost.php HTTP/1.1\r\n"
"Host: 10.0.0.200\r\n"
"Connection: close\r\nContent-Type: application/x-www-form-urlencoded\r\n"
"Content-Length: %u\r\n\r\n"
"%s";
sprintf(trama,"ID=%s&Nombre=%s&Apellido=%s&tipoRegistro=%s",id,nombre,apellido,idxx);
sprintf(outbuf,cabeceraPost,strlen(trama),trama);
enviarPeticion(outbuf); }
```

En la función principal del programa (loop) se obtienen los datos provenientes del puerto serie o se evalúa la existencia de solicitudes, en cualquiera de los casos se toman los datos, ya sea de la pantalla en el caso de comunicación serie, o del cliente en el caso de WiFi, se desentrama y se pasa a la función específica solicitada por el usuario.

```
char* tiporegistro="";
byte i=0;
```

```
byte f=0;
void loop() {
if(f==3){
leernextion[0]=0;
leernextion[4]=0;
leernextion[5]=0;
leernextion[6]=0;
i=0;
f=0;
 }
            while (MySerial.available()) {
            leernextion[i]= MySerial.read();
            if(leernextion[i]==0xFF)
            f++;
            i++;
            }
            i=0;
            if ((leernextion[4]==0xFF)&&(leernextion[5]==0xFF)&&(leernextion[6]==0xFF)){
            if(leernextion[1]==0){// PAGINA 0
            tiporegistro="SOAC";
            }else{
            switch (leernextion[2]) // BOTONES
            {
            case 1:
            tiporegistro="IN";
            break;
            case 2:
            tiporegistro="SA";
            break;
            default:
            tiporegistro="SSNN";
            break;
            }
            }
            pantallaProceso();
}else if((leernextion[0]==0x66)&&(leernextion[1]==0x0)&&(leernextion[2]==0xFF)){
 tiporegistro="";
 }
```

```
WiFiClient client = server.available(); //DATOS PROVENIENTES DE EYELOCK
if (client) {
String nombre = "";
String id = "";
String apellido= "";
byte getdata=0;
while (client.connected()) {
if (client.available()) {
 char c = client.read();
 if (c=='I'&& getdata==0)
 getdata=1;
  if (c==' ' && getdata!=0 ){
 getdata ++;
 }else if(c=='|'){
 getdata=0;
 break;
}
 switch (getdata) {
 case 1:
 nombre+=c;
 break;
 case 2:
 id+=c;
 break;
 case 3:
 apellido+=c;
 break;
 } }}
char nombrec[nombre.substring(3).length()+1];
char apellidoc[apellido.substring(1).length()+1];
char idc[id.substring(1).length()+1];
nombre.substring(3).toCharArray(nombrec,nombre.substring(3).length()+1);
apellido.substring(1).toCharArray(apellidoc,apellido.substring(1).length()+1);
id.substring(1).toCharArray(idc,id.substring(1).length()+1);
client.stop();
peticionPost(idc,nombrec,apellidoc, tiporegistro);
}
tiempoOpen1(); //Temporizador de puerta
```

```
}
```

En el método de tiempoOpen es un temporizador que mantiene la cerradura de la puerta abierta quitando la energía a la cerradura cuando se solicita un acceso correcto. Al terminar el tiempo del temporizador energiza nuevamente la cerradura, permitiendo que la puerta quede bloqueada.

```
unsigned int tiempo=0;
void tiempoOpen1(){
 if (tiempo!=0){
 tiempo++;
 if (tiempo==500000){
 ledcWrite(0,32);
 tiempo=0;
 }}}
```

En el método de enviarPeticion() conecta al servidor y a la base de datos para obtener una respuesta que especifica el nivel de acceso de un usuario, o si este se encuentra registrado o no.

```
void enviarPeticion(char* data) { //CONEXIÃ“N CON BASE DE DATOS
WiFiClient client;
if (client.connect(host, 80)) {
client.print(data);
unsigned long timeout = millis();
while (client.available() == 0) {
if (millis() - timeout > 5000) {
client.stop();
return;
}
}
String line;
while(client.available()){
line=client.readStringUntil('\n');
}
if(tiporegistro!=""){
if(tiporegistro=="SOAC"){// CÃ³digo de acceso, en line se devuelve el nivel
if (line=="10"){
ledcWrite(0,80);
tiempo++;
pantallaOk();
}else {
if (line=="NR"){
```

```
pantallaNoreg();
delay(500);
}
pantallaAcnegado();
}
}else if (tiporegistro=="IN"||tiporegistro=="SA"){
if (line=="OK")
pantallaOk();
else
pantallaNoreg();
}
tiporegistro="";
}else {
pantallaNofuntion();
}
}else{
pantallaErr();
return;
}}
```

En el método de pantallaProceso(), muestra en la pantalla Nextion la fase de proceso.

```
 void pantallaProceso(){
 MySerial.print("page 2");
 fintramaNextion();
 MySerial.print("tm0.tim=25000");
 fintramaNextion();
 MySerial.print("tm1.tim=500");
 fintramaNextion();
 MySerial.print("tm2.tim=800");
 fintramaNextion();
 }
```

En el método de pantallaOk, muestra en la pantalla Nextion el mensaje OK.

```
 void pantallaOk(){//AGRUPAR
 MySerial.print("page 2");
 fintramaNextion();
 MySerial.print("t0.txt=");
 MySerial.write(0x22);
 MySerial.print("OK");
 MySerial.write(0x22);
```

```
 fintramaNextion();
 MySerial.print("t0.bco=1419");
 fintramaNextion();
  timerPag2();
 }
```

En el método de pantallaErr, muestra en la pantalla Nextion el mensaje ERR.

```
void pantallaErr(){ //AGRUPAR
 MySerial.print("page 2");
 fintramaNextion();
 MySerial.print("t0.txt=");
 MySerial.write(0x22);
 MySerial.print("ERR");
 MySerial.write(0x22);
 fintramaNextion();
 MySerial.print("t0.bco=63780");
 fintramaNextion();
 timerPag2();
 }
```

En el método de pantallaAcnegado, muestra en la pantalla Nextion el mensaje de Acceso denegado.

```
 void pantallaAcnegado(){ //AGRUPAR
 MySerial.print("page 2");
 fintramaNextion();
 MySerial.print("t0.txt=");
 MySerial.write(0x22);
 MySerial.print("ACC NEG");
 MySerial.write(0x22);
 fintramaNextion();
 MySerial.print("t0.bco=63780");
 fintramaNextion();
 timerPag2();
}
```

En el método de pantallaNoreg, muestra en la pantalla Nextion el mensaje NOREG, sucede cuando el usuario no se encuentra registrado en la base de datos.

```
 void pantallaNoreg(){ //AGRUPAR
 MySerial.print("page 2");
 fintramaNextion();
 MySerial.print("t0.txt=");
 MySerial.write(0x22);
```

```
MySerial.print("NO REG");
MySerial.write(0x22);
fintramaNextion();
MySerial.print("t0.bco=63780");
fintramaNextion();
timerPag2();
}
```

En el método de pantallaNofunction, muestra en la pantalla Nextion un mensaje de que no se ha seleccionado una función para el registro o acceso.

```
void pantallaNofuntion(){ //AGRUPAR
MySerial.print("page 2");
fintramaNextion();
MySerial.print("t0.txt=");
MySerial.write(0x22);
MySerial.print("NO PRESS");
MySerial.write(0x22);
fintramaNextion();
MySerial.print("t0.bco=63780");
fintramaNextion();
timerPag2();
}
```

En el método de fintramaNextion() es una cadena de datos que se debe enviar a la pantalla Nextion al final de cada trama.

```
void fintramaNextion(){
MySerial.write(0xff);
MySerial.write(0xff);
MySerial.write(0xff);
}
```

En el método de timerPag2, activa en la pantalla un timer de control que evita bucles infinitos.

```
void timerPag2(){
MySerial.print("tm0.tim=2000");
fintramaNextion();
MySerial.print("tm1.tim=5000");
fintramaNextion();
MySerial.print("tm2.tim=5000");
fintramaNextion();
}
```

En el método de relojActual() es una función que conecta con el servidor mediante una petición GET

del protocolo HTTP para sincronizar la hora mostrada en la pantalla Nextion con la hora del sistema del Servidor.

```
void relojActual(){
char outbuf[500];
char trama[500];
char* cabeceraPost= "POST /AccessControl/horaActual.php HTTP/1.1\r\n"
 "Host: 10.0.0.200\r\n"
"Connection: close\r\nContent-Type: application/x-www-form-urlencoded\r\n"
 "Content-Length: %u\r\n\r\n"
 "%s";
 sprintf(trama,"");
sprintf(outbuf,cabeceraPost,strlen(trama),trama);
WiFiClient client;
if (client.connect(host, 80)) {
client.print(outbuf);
unsigned long timeout = millis();
while (client.available() == 0) {
if (millis() - timeout > 5000) {
client.stop();
return;
}
}
String hora;
while(client.available()){
hora=client.readStringUntil('\n');
}
escribirHora(hora);
}else{
pantallaErr();
return;
}}
```

En el método de escribirHora(), muestra en la pantalla Nextion la Hora del sistema.

```
 void escribirHora(String data){
 MySerial.print("t1.txt=");
 MySerial.write(0x22);
 MySerial.print(data);
 MySerial.write(0x22);
 fintramaNextion(); }
```

Anexo 3: Software del Servidor de Registros.

El código mostrado a continuación pertenece al fichero recepcionPost.php, que es una página web programada en php que recibe los datos del usuario desde Arduino por medio de una petición POST. Los datos recibidos corresponden al ID de usuario con el que se ejecuta una consulta en la base de datos, devolviendo una respuesta a Arduino con el valor del nivel de acceso, err, o regok.

```
<?php
$id=$_POST['ID']; //control de grabado de datos
$apellido=$_POST['Apellido'];
$nombre=$_POST['Nombre'];
$tipo=$_POST['tipoRegistro'];
date_default_timezone_set('America/Guayaquil');
$hora= date('H:i:s');
$enlace = mysql_connect("localhost", "root", "Ytjda3toGe") or die ("Error de Login");
mysql_select_db("AccessControl",$enlace) or die ("Error de ConexiÃ³n con la Base de Datos2");
switch ($tipo){
case "IN"://INGRESOS
if ($hora>'07:30:00'&&$hora<'12:00:00'){
$tipo = 'IM01';
} else if ($hora>'13:30:00'&&$hora<'18:00:00'){
$tipo ='IV01';
}else{
$tipo = 'IE01';}
$consulta = "select * from Usuarios where ID='$id'";
$resultado=mysql_query($consulta, $enlace);
$cluster=mysql_fetch_array($resultado);
if($cluster['CI']!=''){
echo 'OK';
}else{
echo 'NR';
}
break;
case "SA"://SALIDAS //preguntar por registro
if ($hora>'08:00:00'&&$hora<='14:00:00'){
$tipo = 'SM01';
}else if ($hora>'14:00:00'&&$hora<'19:00:00'){
$tipo ='SV01';
}else{
$tipo = 'SE01';
}
$consulta = "select * from Usuarios where ID='$id'";
$resultado=mysql_query($consulta, $enlace);
$cluster=mysql_fetch_array($resultado);
if($cluster['CI']!=''){
echo 'OK';
}else{
echo 'NR';
}
break;
case 'SOAC':
$consulta = "select * from Usuarios where ID='$id'";
$resultado=mysql_query($consulta, $enlace);
$cluster=mysql_fetch_array($resultado);
$nivel=$cluster['Level'];
```

```
if ($nivel!='')
echo $nivel;
else
echo 'NR';
break;
default:
$tipo ='HENR';
break;
}
$sql="INSERT INTO Registros (Numero,ID,TipoH) VALUES (0,'".$id."','".$tipo."')";
$resultado2 =mysql_query($sql, $enlace);
?>
```

El fichero horaActual.php es un fichero programado en php que ejecuta una página web que devuelve a Arduino la hora actual del sistema.

```
<?php
date_default_timezone_set('America/Guayaquil');
$hora= date('H:i:s');
$minutoAnadir=0;
$segundos_horaInicial=strtotime($hora);
$segundos_minutoAnadir=$minutoAnadir*60+2;
$nuevaHora=date("H:i:s",$segundos_horaInicial+$segundos_minutoAnadir);
echo $nuevaHora;
?>
```