Universidad Nacional José Faustino Sánchez Carrión

Facultad de Ingeniería Industrial, Sistemas e Informática
Escuela Profesional de Ingeniería Electrónica

Diseño de un sistema control de acceso biométrico y la seguridad física de la Institución Educativa 20786, Vilcahuaura 2022

Tesis
Para optar el Título Profesional de Ingeniero Electrónico

Autores

Daniel Alexander Alcantara Coca
Kevin Alex Leandro Racacha

Asesor

Ing. Carlos Enrique Bernal Valladares

Huacho – Perú

2023

DISEÑO DE UN SISTEMA CONTROL DE ACCESO BIOMETRICO Y LA SEGURIDAD FISICA DE LA INSTITUCION EDUCATIVA 20786, VILCAHUAURA 2022

INFORME DE ORIGINALIDAD

15%	13%	2%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	3%
2	repositorio.ucv.edu.pe Fuente de Internet	1%
3	repositorio.unjfsc.edu.pe Fuente de Internet	1%
4	Submitted to Universidad Alas Peruanas Trabajo del estudiante	1%
5	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
6	Submitted to Universidad Nacional Jose Faustino Sanchez Carrion Trabajo del estudiante	1%
7	Submitted to Universidad Privada del Norte Trabajo del estudiante	<1%
8	repositorio.ucp.edu.pe Fuente de Internet	<1%

DISEÑO DE UN SISTEMA CONTROL DE ACCESO BIOMETRICO Y LA SEGURIDAD FISICA DE LA INSTITUCION EDUCATIVA 20786, VILCAHUAURA 2022

Bach. DANIEL ALEXANDER ALCANTARA COCA

Bach. KEVIN ALEX LEANDRO RACACHA

TESIS DE PREGRADO

ASESOR:

ING. CARLOS ENRIQUE BERNAL VALLADARES

UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

202

DEDICATORIA

Nuestra tesis la dedicamos principalmente a Dios, por darnos la fuerza necesaria para culminar esta meta. A los docentes que nos acompañaron durante nuestra preparación profesional. A nuestra familia, por todo su amor y por motivarnos a seguir hacia adelante.

Alcántara Coca Daniel

Leandro Racacha Kevin

AGRADECIMIENTO

A los docentes

"Sus palabras fueron sabias, sus conocimientos rigurosos y precisos, a ustedes mis profesores queridos, les debo mis conocimientos. Donde quiera que vaya, los llevaré presente en mi desarrollo profesional. Gracias por guiarnos en esta importante etapa de nuestra formación profesional, por su paciencia, por compartir sus conocimientos de manera profesional e invaluable, por su dedicación, perseverancia y tolerancia. De igual manera agradecer a nuestro asesor por su apoyo, compromiso y dedicación se logró culminar este trabajo."

A mis padres

"Ustedes han sido siempre el motor que impulsa mis sueños y esperanzas, quienes estuvieron siempre a mi lado en los días y noches más difíciles durante mis horas de estudio. Siempre han sido mis mejores guías de vida. Hoy cuando concluyo mis estudios, les dedico a ustedes este logro amado padres, como una meta más cumplida. Gracias por ser quienes son y por creer en mí. Especialmente a mis abuelos (Q.E.P.D.) quienes me motivaron a estudiar la carrera."

"Agradezco también a nuestra alma mater, la Universidad Nacional José Faustino Sánchez Carrión, por ser nuestra casa formadora, en especial a la Escuela de Ingeniera Electrónica."

"A la institución educativa que nos brindó la oportunidad de llevar a cabo el desarrollo de este trabajo de investigación."

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE CUADROS

RESUMEN

Título de la investigación: "Diseño de un sistema control de acceso biométrico y la seguridad física de la Institución Educativa 20786, Vilcahuaura 2022". **Objetivo:** Establecer la relación entre el sistema de control de acceso biométrico y la seguridad física en la institución educativa 20786, Vilcahuaura 2022. **Metodología:** El tipo de investigación fue no experimental, de nivel correlacional y enfoque mixto. **Hipótesis:** El sistema de control de acceso biométrico se relaciona con la seguridad física en la institución educativa 20786, Vilcahuaura 2022. **Población:** conformada por 25 personas, que representan los docentes que laboran en esta Institución Educativa, y que son ellos quienes tendrán la autorización de acceso a este ambiente y tendrán el registro de su huella dactilar. **Muestra:** Al ser la población menor de 50, se considerará la muestra también igual a 25 personas. **Instrumento:** Encuesta, para medir la relación entre la variable independiente y variable independiente. **Resultados:** Se observó que un 4% de docentes encuestados expresan un nivel medio en la variable Sistema de Control de Acceso Biométrico, y un 96% un nivel alto, en la institución educativa 20786 de Vilcahuaura. **Conclusión:** Existe una relación entre el sistema de control de acceso biométrico y la seguridad física en la institución educativa 20786, Vilcahuaura, basándonos en los resultados obtenidos mediante la prueba de correlación de Pearson que arrojo un valor de 0.754.

Palabras Claves: Control de Acceso, Biometría, Control de Acceso Biométrico, Seguridad Interna.

ABSTRACT

Research title: "Design of a biometric access control system and physical security of the Educational Institution 20786, Vilcahuaura 2022". **Objective:** Establish the relationship between the biometric access control system and physical security in the educational institution 20786, Vilcahuaura 2022. **Methodology:** The type of research was nonexperimental, correlative level and mixed approach. **Hypothesis:** The biometric access control system is related to physical security in the educational institution 20786, Vilcahuaura 2022. **Population:** made up of 25 people, representing the teachers who work in this educational institution, and it is they who will have the authorization of access to this environment and will have the record of their fingerprint. **Sample:** Since the population is under 50, the sample shall also be considered as 25 persons. Instrument: Survey to measure the relationship between the independent variable and the independent variable. **Results:** It was observed that 4% of teachers surveyed expressed an average level in the variable Biometric Access Control System, and 96% a high level, in the educational institution 20786 of Vilcahuaura. **Conclusion:** There is a relationship between the biometric access control system and physical security in the educational institution 20786, Vilcahuaura, based on the results obtained by the Pearson correlation test that yielded a value of 0.754.

Keywords: Access Control, Biometrics, Biometric Access Control, Internal Security.

INTRODUCCIÓN

"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" (Pérez, 2018, p.29). Pérez (2018) menciona que: "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" (p.34).

La investigación se ha estructurado de la siguiente manera: "En el I capítulo se tiene en cuenta el planteamiento del problema donde se hace la descripción de la realidad problemática, luego la formulación del problema con su respectivos objetivos de la investigación, tiene en cuenta Justificación de la investigación ,delimitaciones del estudio, viabilidad del estudio y las estrategias metodológicas, en el II capítulo, el marco teórico, que comprende los antecedentes del estudio, el cual tiene en cuenta las Investigaciones relacionadas con el estudio y otras publicaciones, en las bases teóricas hacemos el tratado de las Teorías sobre la variable independiente y dependiente , definiciones de términos básicos, Sistema de hipótesis y la operacionalización de variables, en el III capítulo, el marco metodológico que contiene el diseño de la investigación, la población y muestra, las técnicas de recolección de datos y las técnicas para el procesamiento de la información, el IV capítulo, que contiene los resultados y su respectiva contrastación de hipótesis, en el V capítulo, se tiene en cuenta la discusión de los resultados, en el VI, capítulo contiene las Conclusiones, recomendaciones y finalmente las referencias bibliográficas y sus respectivos anexos".

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

En la actualidad, la seguridad es un tema muy importante en sus distintos aspectos, ya sea al referirnos a la seguridad ciudadana, seguridad informática, seguridad laboral, etc. Siempre se busca nuevos métodos para poder prevenir accidentes o resguardar información, y en este sentido la tecnología juega un papel muy importante, ya que, gracias a sus avances, estos métodos de prevención o protección han ido mejorando con el tiempo, a tal punto de que ahora se pueden diseñar sistemas muy eficientes y con un alto nivel de confiabilidad.

Esta problemática de la seguridad se ve reflejada en todas las partes del mundo, y si nos referimos específicamente a empresas o instituciones ya sean públicas o privadas el panorama es el mismo, dentro de estas no solo existe la seguridad para los miembros que la componen, sino que también la seguridad en cuanto a la información, recursos o equipamiento que estas manejen, los cuales garantizan la estabilidad y el correcto desarrollo de la institución. Debido a esto, la implementación de un sistema que controle el acceso a estas áreas para cierto personal autorizado resulta indispensable. Los métodos tradicionales resultan ineficientes e inseguros para los intereses de la institución, tal es el caso, del acceso a los laboratorios de la Universidad Estatal Del Sur De Manabí o el ingreso del personal a la Empresa Electroservicios Querubín De La Ciudad De Puyo, ambos casos presentaban un problema en cuanto al control de acceso y la asistencia de sus miembros, ya que se aplicaba estos métodos tradicionales, que resultan vulnerables a suplantación o incluso alteración de la información que se desea

obtener. La implementación de un sistema adecuado basado en la tecnología de reconocimiento biométrico para ambos casos resulto en una solución viable y confiable para su propósito. De esto último, se debe destacar que si bien es cierto que la implementación del sistema pudo desarrollarse con otros tipos de tecnología ya sea por firma digital, por ejemplo, la aplicación de la biometría hace que este sistema sea más confiable, ya que se está trabajando con una característica única de la persona, lo cual eliminó los inconvenientes que se presentaban inicialmente. Es así como la biometría aprovecha una característica propia del ser humano (ya sea la huella digital, reconocimiento facial, patrones del iris, etc.) para poder realizar este tipo de sistemas, que pueden ir desde lo más simple como una cerradura electrónica, hasta sistemas muchos más complejos.

En el Perú, la tecnología biométrica no es un concepto que se maneja en esta última década, sino que más bien se remonta a finales de la década de los 90 cuando la Superintendencia Nacional de los registros públicos (SUNARP) comenzó a utilizar la biometría para realizar la verificación de identidad en sus usuarios cuando iban a realizar sus registros, más adelante se empezó a emplear en el rubro de la identificación pero de uso exclusivo de los índices de ambas manos, posteriormente este tipo de tecnología seria adoptado por la RENIEC cuya función era la de encargarse de la identificación de personas en el Perú, pero no sería hasta mediados de 2010 en donde este organismo actualizaría su tecnología para lanzar el DNI electrónico tomando como muestra las huellas dactilares de los 10 dedos y además se implementó las características del rostro de las personas. Con el pasar de los años este tipo de tecnología se ha vuelto muy cotidiana y una de las formas de identificación más confiable en el

país no solo en el campo de la identificación personal sino que también llevándose al campo de gestión de control de acceso como una nueva forma de validación de datos en diversos establecimientos, como aeropuertos, hospitales, complejos del estado, empresas privadas, instituciones educativas, oficinas, bancos e inclusive llegando a formar parte de la vida de las personas; implementándolas de manera innovadora en los hogares en forma de cerraduras inteligentes y control de acceso, en los teléfonos inteligentes en forma de sensores incorporados para el desbloqueo de las diferentes funciones, todo esto en consecuencia de la inseguridad que azota el país. Es por ello que se ha encontrado en este tipo de tecnología una forma de salvaguardar datos, información y materia valiosa. Esto sobre todo en empresas que trabajan con maquinaria, equipos, instrumentos y datos que no pueden estar expuestos o al alcance de cualquier persona ajena o no autorizada para el manejo y manipulación de estos bienes clasificados, ya que estos riesgos podrían estar sujeto a robos o perdida de material física o virtual sumamente importante.

Actualmente la Institución Educativa 20786, posee diversas áreas donde se encuentran materiales educativos indispensables para el correcto aprendizaje de los alumnos, tal es el caso del Centro de Recursos Tecnológicos o la Biblioteca de esta Institución Educativa, es aquí donde se resguarda los recursos de apoyo más importantes como las computadoras, tablets, equipos de sonido y libros; los cuales son usados tanto por los docentes como por los alumnos cuando son necesarios. Cabe resaltar que el acceso a este ambiente debería estar restringido solo al personal autorizado, tal es el caso, de los docentes que laboran en esta Institución Educativa quienes al mismo tiempo permitirán el acceso a los alumnos que necesitan utilizar estos recursos educativos.

El ingreso no autorizado podría ocasionar la perdida de estos materiales educativos o dañarlos, recayendo toda la responsabilidad sobre el docente a cargo de estos ambientes, sin embargo, la consecuencia más grave es dejar a los alumnos sin recursos de estudio, privándolos de la tecnología que actualmente se ha vuelto tan útil e indispensable para un mejor aprendizaje, esto significaría también que los docentes no contarían con estas herramientas que ayudan a transmitir mejor sus enseñanzas.

Es por ello que consideramos que es de suma importancia un método de seguridad para la gestión de acceso al Centro de Recursos Tecnológicos de esta Institución Educativa, de esta forma planteamos el hecho de implementar un sistema de control de acceso biométrico para la seguridad interna de este ambiente como medida de precaución a posibles problemas con graves consecuencias a corto y mediano plazo.

Esto con el fin de salvaguardar los bienes materiales con los que cuenta la institución educativa y que son de alto valor para la enseñanza de sus alumnos, capacitación de los docentes y personal administrativo. De esta manera también se tendrá un estricto control a cerca de las personas que tienen acceso al uso de estos materiales.

1.2. Formulación del problema

1.2.1. Problema general

- ¿Qué relación existe entre el sistema de control de acceso biométrico y la seguridad física en la institución educativa 20786, Vilcahuaura 2022?

1.2.2. Problemas específicos

- ¿Qué relación existe entre el sistema de identificación y la seguridad física en la institución educativa 20786, Vilcahuaura 2022?

- ¿Qué relación existe entre las características físicas y la seguridad física en la institución educativa 20786, Vilcahuaura 2022?

- ¿Qué relación existe entre el registro y autenticación y la seguridad física en la institución educativa 20786, Vilcahuaura 2022?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

- Establecer la relación entre el sistema de control de acceso biométrico y la seguridad física en la institución educativa 20786, Vilcahuaura 2022.

1.3.2. Objetivos específicos

- Establecer la relación entre el sistema de identificación y la seguridad física en la institución educativa 20786, Vilcahuaura 2022.

- Establecer la relación entre las características físicas y la seguridad física en la institución educativa 20786, Vilcahuaura 2022.

- Establecer la relación entre el registro y autenticación, y la seguridad física en la institución educativa 20786, Vilcahuaura 2022.

1.4. Justificación

1.4.1. Justificación metodológica

Esta investigación aportara la experimentación, descripción, análisis e interpretación de los procesos que se podrían seguir para darles una alternativa de solución en cuanto al área de recursos tecnológicos educativos de la institución educativa, todo mediante un control de acceso biométrico con el uso de huella dactilar, por lo que los principales beneficiados serían todos los integrantes de esta Institución Educativa, ya que evitara daños o perdidas de los recursos educativos importantes para la Institución, el cual podría ocasionar molestias a los docentes y alumnos que dependen de estos recursos para el normal desarrollo de sus clases.

1.4.2. Justificación social:

Como sabemos el control de acceso es un aspecto muy importante al momento de tener protegida cierta área en donde se encuentran objetos, maquinas e instrumentos, ya que de esta manera se garantiza la seguridad de

estos mediante una estricta selección de personal autorizado para el ingreso y manipulación de los mismo sin tener que correr demasiados riesgos.

1.5. Delimitación

- Nuestro estudio se centrará en la problemática que podría causar la falta de un control de acceso en la seguridad física de los recursos tecnológicos educativos que se encuentran almacenados en el Centro de Recursos Tecnológicos perteneciente a esta Institución Educativa.
- La delimitación temporal, está comprendida entre diciembre de 2022 y marzo de 2023 tiempo en el cual se desarrolla la presente investigación

1.6. Viabilidad

- Los investigadores con los conocimientos adecuados para llevar a cabo la investigación.
- Para el tema central de la investigación se cuenta con el acceso suficiente a la información primaria como internet, libros, revistas, etc.
- Se cuenta con el tiempo suficiente para el desarrollo de la investigación.
- Se cuenta con el medio de transporte necesario para llegar a la Institución Educativa.
- Los investigadores cuentan con los recursos económicos suficientes para realizar el estudio.
- Los recursos necesarios fueron adquiridos a través de recursos propios, El lector de biométrico dactilar, microcontrolador, keypad, LCD, se

conseguirán mediante tiendas online ya que de esta forma se disminuye un porcentaje de los precios que se presentan de forma local. Para esta investigación se cuenta con el permiso de la directora a cargo de esta Institución Educativa.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes del estudio

2.1.1. Antecedentes internacionales

Vallejo y Carrera (2017), realizaron la tesis de pregrado titulada "Implementación de un sistema biométrico de huellas dactilares para el control de asistencia estudiantil en la Escuela de Ingeniería Industrial de la Facultad de Mecánica". Realizada con apoyo de la Escuela Superior Politécnica de Chimborazo. Riobamba, Ecuador. "El objetivo general fue Implementar un sistema biométrico de huellas dactilares para el control de asistencia estudiantil en la Escuela de Ingeniería Industrial de la Facultad de Mecánica" (p.19). "La población fue de 330 estudiantes matriculados de los cuales se consideró una muestra de 178 estudiantes con un nivel de confianza del 95%" (p.81). "La técnica utilizada fue la encuesta y el instrumento el cuestionario" (p. 80). "Los resultados señalan que el 94% de los estudiantes están de acuerdo con el cambio de registro de asistencia a uno automatizado, el 6% restante considera que debe ampliarse el margen de tiempo" (p.84); respecto inconvenientes en cuanto al uso del sistema, el 96% de los estudiantes no han tenido inconvenientes (p.84); respecto a la eficiencia del sistema implementado, el 97% de los estudiantes considera que si es eficiente (p.85). La conclusión señala que existe una gran aceptación del sistema implementado ya que se obtuvo un resultado mayor al 90% en todas las interrogantes propuestas en el cuestionario.

Arteaga (2018), realizó la tesis titulada “Implementación De Un Control De Acceso Utilizando Sistema Biométrico Para El Laboratorio De Electrónica Y Robótica De La Universidad Estatal Del Sur De Manabí”. Realizada con apoyo de la Universidad estatal del sur de Manabí. Jipijapa, Manabí, Ecuador. “El objetivo general fue desarrollar un control de acceso utilizando sistema biométrico para el laboratorio de robótica y electrónica de la Universidad Estatal del Sur de Manabí” (p.17). “La metodología utilizada para el desarrollo de este trabajo tuvo un enfoque cualitativo y cuantitativo, en el cual, se realizó una investigación para llevar a cabo la elaboración de encuestas aplicadas a la población potencialmente beneficiada” (p.46). “La población fue de 166 personas entre estudiantes y maestros, decidiéndose trabajar con la población completa. Las técnicas utilizadas fueron la encuesta y la entrevista, y el instrumento utilizado es el cuestionario. Los resultados de las encuestas señalan que 73% de los estudiantes consideran que las medidas de seguridad que se manejan en el laboratorio de robótica y electrónica no son las adecuadas” (p.54); “el 58% de ellos considera que la seguridad mejoraría con la implementación del control de acceso” (p.55); “el 90% considera que es conveniente que se use la huella dactilar para ingresar al laboratorio” (p.57); “y el 100% de la muestra tomada considera que si es necesario que en laboratorio de robótica se realice un sistema de control y gestión del personal. En conclusión, se desarrolló un control de acceso utilizando sistema biométrico para el laboratorio de robótica y electrónica de la Universidad Estatal del Sur de Manabí, se Identificó los procedimientos de seguridad utilizados en el laboratorio de electrónica y

robótica, y se Determinó los parámetros técnicos necesarios para la instalación de un control de acceso biométrico en el laboratorio de electrónica y robótica" (p.88).

Pérez (2018), realizo la tesis titulada "Sistema De Control De Acceso Por Reconocimiento De Iris Para El Ingreso De Personal A La Empresa Electroservicios Querubín De La Ciudad De Puyo". "Realizada con el apoyo de la Universidad Técnica de Ambato. Ambato, Ecuador. El objetivo general fue 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" (p.23). El trabajo de investigación se realizó bajo los conceptos de investigación aplicada. No se requería población ni muestra debido a las características de la investigación. Los instrumentos utilizados fueron tablas comparativas y fichas de observación. Los resultados obtenidos durante las 4 semanas de prueba del sistema se observó una reducción del porcentaje de errores del 10.09% al 3.63%, dicha reducción es producto de la adaptación del usuario al sistema (p.79), posterior al periodo de pruebas, luego de 14 días se obtuvo un promedio de 5.74 segundos en la que el sistema ejecuta una petición (p.80). En conclusión, "la facilidad de uso de un sistema de control de acceso incrementa el grado de aceptación de los usuarios, el nivel de seguridad en la empresa se incrementa con la implementación del control de acceso por identificación de iris" (p.81).

Fernández (2017), realizo la tesis titulada “Sistema De Control De Acceso Basado En La Tecnología De Autenticación Biométrica Por Huella Dactilar Para El Instituto Técnico Comercial - La Paz”. Realizada con el apoyo de la Universidad Mayor de San Andrés. La paz, Bolivia. “El objetivo general Diseñar un sistema de acceso basado en la tecnología de autenticación biométrica de huella dactilar, para el control de asistencia, registro de Docentes y Administrativos, y su posterior almacenamiento en una base de datos del Instituto Técnico Comercial La Paz” (p.15). “La metodología hace referencia al diseño metodológico experimental. La técnica utilizada es la experimentación” (p.18). “Los resultados obtenidos en las pruebas de funcionamiento, indican que se diseñó un prototipo funcional de un sistema de Control de acceso basado en la tecnología de autenticación biométrica por huella dactilar para el Instituto Técnico Comercial La Paz. En conclusión, el diseño y la implementación de un prototipo de hardware para la adquisición y lectura de huellas dactilares, el diseño de la interfaz gráfica de usuario, usando Windows Forms, el diseño de la base de datos en SQL resulto ser un sistema funcional alcanzando las expectativas iniciales” (p.102).

Montaña (2017). Realizo la tesis titulada “Sistema de identificación mediante huella digital para el control de accesos a la Universidad Libre Sede Bosque Popular simulado en un entorno web”. Realizada con el apoyo de la Universidad Libre Sede Bosque Popular, Bogotá, Colombia, 2019. El presente proyecto tiene por objetivo general, “Desarrollar un sistema de identificación por huella digital para control de accesos de la universidad libre sede bosque popular

simulado en un entorno web" (p.20). Es una investigación de tipo tecnológica-aplicada, y se usó el instrumento de la encuesta (p.22). Se obtuvo como resultado que, en base a la encuesta realizada se obtuvo como resultado que el 100% de los encuestados considera que la implementación de este sistema es necesario y esencial (p.56). Se puede concluir, la comunidad estudiantil de la universidad libre sin importar el género, desean sentirse seguros con sus objetos personales, dentro de las instalaciones de la sede bosque popular de la universidad libre. Se hace necesario que la institución implemente un sistema de control de accesos que sirva como colaboración a la celaduría, con el fin de tener control de las personas que ingresan y que salen de la sede (p.57).

2.1.2. Antecedentes Nacionales

Guerra y Jiménez. (2021), "Aplicación de reconocimiento biométrico por huella dactilar y su influencia en la seguridad lógica en SEDAPAL", Universidad César Vallejo, Callao – Perú. "El objetivo general de esta tesis se basa en determinar de qué manera influye la aplicación de reconocimiento biométrico por huella dactilar en el control de acceso en SEDAPAL" (p.25). "La metodología que se emplea en este trabajo fue aplicada debido a que el problema estaba establecido y fue reconocido por los investigadores y de nivel experimental" (p.77). "La población estuvo conformada por el equipo de servicios y clientes especiales perteneciente a la gerencia comercial de SEDAPAL, para la muestra se seleccionó a 52 trabajadores del equipo de

servicios y clientes especiales de la gerencia comercial, para la recolección de datos se empleó la técnica de la encuesta por ser de carácter masivo" (p.79). "Los resultados indican que efectivamente el reconocimiento biométrico por huella dactilar si tiene influencia en la auditoria de seguridad en SEDAPAL" (p. 131). En conclusión, "la aplicación de reconocimiento biométrico por huella dactilar si influye en la seguridad lógica en SEDAPAL, donde el contraste usando la prueba de rangos con signos de Wilcoxon, la cual es una prueba empleada en variables cualitativas ordinales para muestras relacionadas, resulto con un nivel de significación de 0,000 menor que 0,05, quedando rechazada la hipótesis nula y aceptando la alterna" (p.139).

Sotelo (2020). "Diseño de un prototipo de control de acceso basado en tecnología biométrica de huella dactilar, lector de barras y RFID". Universidad Tecnológica del Perú, Lima – Perú. "El objetivo general de esta tesis es esbozar un arquetipo de control de acceso fiable para la identificación peatonal y vehicular basado en tecnología biométrica de huella dactilar, lector de barras y RFID" (p.17). "La metodología que se empleado en este trabajo es del tipo experimental ya que la estructura de trabajo se dividió en 3 principales aspectos, diseño, desarrollo e integración y validación" (p.38). En los resultados se obtuvo que "en la primera etapa se logró la identificación del trabajador mediante la lectura de su huella dactilar y la verificación de los datos fueron correctos" (p.92) y para la segunda etapa "se logró la identificación del trabajador mediante la lectura de su documento de identidad y la verificación de sus datos fueron

correctos" (p.93). En conclusión, "para esta tesis se logró esbozar un prototipo de control de acceso confiable para la identificación exacta del personal militar y civil que laboran en el centro de informática y estadística (CINFE) cotejando la identificación de cada uno de ellos con la lectura de la huella dactilar, lectura del código de barras y la lectura de la tarjeta RFID" (p.95).

San Martin (2019). "Diseño e implementación de un sistema de control de acceso por biometría", Universidad Tecnológica del Perú, Lima – Perú. Este trabajo tiene por objetivo general el "diseñar e implementar un sistema de control de acceso por medio de características biométricas" (p.3). La metodología que se empleó para esta tesis se pudo deducir que fue experimental ya que contaron con una etapa de prueba de equipos previa a la implementación en campo. Los resultados arrojan que los problemas con las lecturas de huellas durante las pruebas fueron nulos y que de esta manera se aseguran de que solo puedan ingresar al taller las personas registradas en la base de datos (p.45). En conclusión, "se logró cumplir el objetivo ya que se diseñó e implemento un sistema de control de acceso que, a través del análisis de las características biométricas de los usuarios, mejora la seguridad del taller" (p.47).

Ccamerccoa. (2020). "Implementación de un sistema automatizado para gestionar la seguridad de accesos en viviendas juliaqueñas mediante aplicativo móvil e internet de las cosas", Universidad Peruana Unión, Juliaca – Perú. "El objetivo general de este trabajo es implementar un sistema automatizado para

gestionar la seguridad de accesos en viviendas juliaqueñas mediante aplicativo móvil e internet de las cosas" (p.24). La metodología que se utilizó en el trabajo en la parte de aplicación fue la de Mobile-Den cada una de las fases y para el hardware se empleó la metodología waterfall que se desempeña en forma cascada (p.72). Como resultado se obtuvo que una vez instalado el software y el hardware se puso a prueba por el periodo de un mes y no se obtuvieron fallas, cumpliendo con su objetivo de reforzar la seguridad registrando solo a usuarios autorizados, actualizando datos y fechas (p.135). En conclusión, "se consiguió mostrar todo lo que se quería obtener en el proyecto enfocándose en la aplicación y en el hecho de incrementar la seguridad de la vivienda en donde se implementó el sistema" (p.138).

Menéndez. (2019). "Propuesta para el diseño de un sistema de validación y autentificación biométrico dactilar para la asociación guadalupana", Universidad Tecnológica del Perú, Lima – Perú. "El objetivo general de esta tesis es diseñar un sistema de validación y autenticación biométrico dactilar para mejorar el control de acceso de la asociación guadalupana" (p.14). "La metodología que emplea es de la forma empírica aplicando el método Scrum debido a que este proyecto es de corto plazo" (p.26). Los resultados arrojaron que con este proyecto se podría llevar un mejor control de la asociación guadalupana mejorando así la seguridad mediante los dispositivos biométricos. En conclusión, "la asociación guadalupana no cuenta con un sistema que ayude a

gestionar los ingresos de los trabajadores y asociados ni tiene como identificarlos" (p.69).

2.2 Bases Teóricas:

2.2.1 Sistema de control de acceso

Este sistema regula o controla quién o qué puede tener acceso ciertas áreas o recursos, en este sentido, Pérez (2018), menciona que:

> "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" (p.29).

De lo expuesto, se puede concluir que un sistema de control de acceso hace referencia a un mecanismo que opera en función de la identificación de un usuario, al cual se le permitirá o no el acceso a un área generalmente restringido (determinado por la institución o empresa), es decir, acceder a ciertos recursos ya sean lógicos o físicos, que solo están disponibles para cierto personal autorizado. Para que este sistema pueda discriminar correctamente a que usuarios se les permitirá el acceso, hace uso de la tecnología, para lo cual, existe una variedad de métodos que se pueden utilizar para poder obtener los datos necesarios del usuario a identificar, sin embargo, es necesario considerar la precisión y confiabilidad del método que se utilizara, ya que si bien todos

pueden cumplir con el objetivo del sistema, no todos pueden garantizar una identificación segura, debido a su nivel de vulnerabilidad frente a fraudes o suplantaciones de identidad.

Entonces, debido a la necesidad del sistema de identificar la credencial del usuario, se vuelve necesario que esta debe ser intransferible, como en el caso de un sistema de control de acceso biométrico.

Con todo lo mencionado hasta ahora, es fácil deducir que este sistema está enfocado en evitar la violación de seguridad hacia alguna área en específico (proteger recursos importantes) además de poder tener un monitoreo o control de aquellos que hayan tenido acceso a estas áreas. Es así que, "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" (Pérez, 2018, p.29). Con todas las características antes mencionadas la aplicación de esta tecnología se vuelve muy importante y hasta indispensable para las empresas, entidades o instituciones, ya que son estas las que poseen recursos muy importantes para su correcto desarrollo, los cuales deben estar disponibles solo para cierto personal autorizado. Además, la combinación o integración apropiada de los elementos electrónicos o tecnológicos que compongan este sistema puede reducir costos, tales como, componentes de seguridad o personal de seguridad que se encargue de esta actividad; de modo que, solo se tiene un pago por cada sistema que se implemente, y también el costo de su mantenimiento (preventivo y correctivo) resulta inferior al salario de un personal de seguridad.

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" (Pérez, 2018, p.29). Esta gestión de acceso es la que permitirá el ingreso a un limitado grupo de usuario, concediéndoles el derecho al acceso a los recursos o servicios restringidos, y claro se le deniega al resto, para ello la gestión maneja los siguientes conceptos básicos, según Pérez (2018):

> "Acceso, nivel y alcance de la funcionalidad de un servicio o área que un usuario está autorizado a utilizar. Identidad, información que define el dominio de las personas reconocidas por la organización. Derechos, 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" (p.29).

Estos sistemas independientemente de su configuración o tipo de control que utilice, se encargan de otorgar la autorización a los usuarios para el acceso de ciertas áreas, por lo general para la protección de objetos de valor, o como los ya mencionados recursos indispensables para alguna empresa o institución, pero también a zonas donde el nivel de peligro es más elevado o con más incidencia de accidentes, lugar donde solo el personal capacitado tenga el acceso, protegiendo así la seguridad de la propia persona o usuario.

2.2.3 Tipos de control de acceso

"Los sistemas de control de acceso de personal, representan la tecnología con más demanda en el mercado para seguridad de áreas restringidas" (Pérez, 2018, p.32). El desarrollo de la tecnología avanza mucho cada año, trabajando con los correctos sistemas mecánicos, el personal adecuado, dispositivos modernos y nuevas tecnologías, han hecho posible ahora obtener sistemas o procesos de control automatizados en su totalidad. En este sentido, es importante identificar correctamente el área donde se va a instalar este sistema, de modo que, se pueda seleccionar la tecnología más adecuada para su correcto funcionamiento, es por ello que los controles de acceso se dividen en 2 tipos:

- Control de acceso físico: Referido a la restricción de acceso hacia áreas físicas, como pueden ser viviendas, edificios o ambientes dentro de estos, básicamente podríamos referirlo al tipo de seguridad más común en cualquier ambiente donde nos encontremos. Es así que, "Históricamente, esto se pudo conseguir de forma parcial mediante la implementación de llaves y cerraduras. Cuando una puerta está bloqueada, tan solo una persona que posea la llave adecuada tiene la potestad de entrar" (Arteaga, 2018, p.27). De lo mencionado, es el método de seguridad clásico que se usa en cualquier parte para controlar el acceso a ciertos ambientes, sin embargo, es evidente el gran problema que presenta este método, su vulnerabilidad se refleja en el hecho de que, si bien las cerraduras solo poseen una llave maestra, nada quita el hecho de la facilidad con la que esta puede ser copiada o incluso extraviarse, lo que ocasiona que se tenga que hacer un cambio de cerradura.

Siempre se busca maneras de poder corregir estos inconvenientes, y tener un mejor control de acceso físico, de modo que, ahora hay diversos métodos que nos permiten realizar esta actividad de forma segura, pudiendo ser logrado por un ser humano (personal de seguridad) o por medios tecnológicos.

- Control de acceso lógico: "El control de acceso electrónico emplea computadoras para solucionar las limitaciones de las llaves y cerraduras convencionales. Se puede utilizar una amplia gama de credenciales para reemplazar las llaves mecánicas" (Arteaga, 2018, p.28). De lo mencionado, este tipo sistema se enfoca en la integración de componentes por medio de una computadora o algún controlador, donde haciendo uso de un software adecuado se puede tener un mejor control, obteniendo mayor información en cada operación del sistema como la fecha, hora, autorización, entre otros. Es decir, independientemente de la credencial que se utilice para identificar al usuario que intenta tener acceso, se contara con un registro de su autorización de ingreso, además del tiempo en la cual se le permitió o denegó el acceso. Adicionalmente, estos tipos de sistemas cuentan con alarmas que se activaran cuando se intente forzar el acceso de modo ajeno a como está configurado.

2.2.4 Componentes de un sistema de control de acceso

Todo sistema de control de acceso posee elementos fundamentales para su correcto funcionamiento, estos determinaran su nivel de confiabilidad, seguridad y precisión. Es así que, según Pérez (2018):

"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" (p.34).

Entonces, según lo mencionado hay conceptos importantes a tener en cuenta dentro de este tipo de sistemas, por lo cual, tomando de referencia un sistema de control de acceso tipo lógico, el cual es precisamente es tema del presente trabajo de investigación, se pueden considerar los siguientes componentes fundamentales:

- **La Credencial,** es el modo o mecanismo por el cual se identificará al usuario que desea tener acceso, de aquí es donde se podrá obtener la información que se requiera para poder verificar la identidad del usuario y otorgarle o no el acceso. Entonces, se refiere a algo que una persona posee o sepa, como puede ser alguna tarjeta de identificación, clave secreta, algún rasgo físico de la persona (biometría), firma, entre otros.
- **Lector,** equipo o dispositivo encargado de adquirir la información contenida en la credencial para la identificación del usuario. La información se procesa y posteriormente se envía al controlador del sistema (interno o externo), donde se verificará la identificación, para otorgar o no el acceso correspondiente.
- **Servidor,** elemento que se encarga de almacenar la información de todo el sistema, que va desde los usuarios registrados, el nivel de acceso de

los mismos, intentos de acceso sean exitosos o no, señal de alarma, etc. Es así que, el servidor almacenara todos los eventos que puedan ocurrir durante el funcionamiento del sistema.

- **Controlador,** representa el cerebro del sistema, encargo de la ejecución de acciones correspondientes en base a la información que proporciona el resto de elementos, por lo que, proporcionara el acceso en base a la identificación del usuario, su nivel de acceso, la zona donde desee ingresar, la hora en que lo haga o eventos producidos anteriormente. Entonces, el controlador permanece en constante comunicación con el servidor para obtener dicha información.
- **Mecanismo de Apertura**, representa el dispositivo final del sistema, permite la apertura o bloqueo de la puerta del área donde se desea acceder, mediante señales eléctricas que son enviadas por el controlador luego de verificar la identidad del usuario.
- **Alimentación del sistema**, referido a la energía que necesita el sistema para funcionar correctamente, algo a tener en cuenta que los distintos elementos del sistema (circuitos electrónicos) se alimentan con distintos niveles de voltaje, por lo que, esto conlleva a tener que acondicionar circuitos adicionales para poder lograr esta regulación al nivel correcto de voltaje que se requiera, además, se debe considerar que pueden existir cortes de energía, lo que nos lleva tener que implementar un sistema de respaldo para evitar que el funcionamiento del sistema de control de acceso se detenga.

Hasta ahora se ha hecho mención de todos los elementos que se requieren para poder abrir la "puerta" y acceder al ambiente deseado, por otro lado se debe tener en cuenta algún mecanismo que nos permita salir del ambiente, para ello se puede considerar dispositivos como algún pulsador o botón que permita la apertura de la puerta, o incluso el uso de un sensor para la detección del individuo, es decir, la puerta se abrirá automáticamente cuando el usuario se acerque a esta.

2.2.5 Tipos de información de autenticación

Existen 3 tipos de información para poder realizar la autenticación del usuario, Arteaga (2018), menciona las siguientes:

- "Algo que el usuario conoce, por ejemplo, una contraseña, o PIN" (p.29).
- "Algo que tiene el usuario, como una tarjeta inteligente o un llavero" (p.29).
- "Algo que el usuario es, como la huella dactilar, verificado por medición biométrica" (p.29).

Entonces en base a estas características, tenemos:

- Acceso por Contraseñas o PIN, del tipo más común para poder tener a cualquier tipo de información (físico o informático), este sistema funciona en base al ingreso de esta clave o contraseña al controlador para poder verificar su identidad, por medio de algún tipo de teclado numérico o alfanumérico. Entonces, esto implica que cada usuario posea una clave única para ingresar, y si bien resulta en un sistema

económico y simple, el problema que presenta es su bajo nivel de seguridad, ya que, nada evita que esta información sea filtrada y conocida por otros individuos que no tienen la autorización necesaria, perdiendo la confiabilidad en el método que este tipo de sistema utiliza.

- Tarjeta Magnéticas, son objetos físicos que se utilizan para poder brindar la información que necesita el sistema y verificar su identidad, estos dispositivos son de un material de PVC o polyester, y adicionalmente poseen una banda magnética donde se almacena la información que necesita el sistema pero codificada, de modo que, al pasar la tarjeta por el lector correspondiente, se procederá con la decodificación de este información y su posterior validación para que el sistema apertura o mantenga bloqueada la puerta. Este tipo resulta más seguro debido a la dificultad que existe para poder copiar la información contenida en la barra magnética, además, es económico y de rápido acceso, sin embargo, su problema radica en la perdida de información debido a la fricción generada al momento de usar la tarjeta, lo que gradualmente va degradando la barra magnética, alterando la información original.
- Tarjetas Inteligentes, es similar al sistema anterior mencionado en cuanto a composición y funcionamiento. La diferencia radica en que esta lleva la información en un microprocesador integrado capaz de realizar algunos cálculos adicionales, además, no todas requieren de hacer contacto con el lector para ingresar la información.

- Medición Biométrica, método de seguridad moderno que ya se pueden encontrar en muchos dispositivos tecnológicos como los celulares, que permiten tener una verificación de identidad más segura, ya que, este sistema consiste en reconocer alguna característica física de la persona para validar acceso, siendo este un método más seguro y confiable, ya que estas características son únicas en la persona y no se pueden imitar.

2.2.6 Definición de la biometría

Se define a la Biometría como la tecnología que se encarga de la extracción o reconocimiento de las características físicas únicas del ser humano, con el objeto de poder garantizar la seguridad a través de sistemas o mecanismos de control de acceso. Tal como mencionan Guerra y Jiménez. (2021), "La biometría se conceptualiza como una tecnología de reconocimiento de patrones únicos e intransferibles, los cuales tienen un enfoque de seguridad a través de mecanismos como el control de acceso" (p.34). De lo mencionado podemos entender que la biometría se encuentra muy relacionado al tema de seguridad, algo bastante importante y necesario en cualquier entorno donde se utilice o maneje información o recursos valiosos, disponibles solo para un grupo determinado de individuos autorizados. Por lo que, se hace necesario la autentificación exacta, confiable y precisa de aquel que desea tener acceso a dichos recurso. Esto sobre todo se ve reflejado en las empresas u organizaciones, ya que, estas poseen recursos o activos importantes para su correcto desarrollo y crecimiento, que necesitan ser protegidos en todos sus aspectos, entonces, es aquí donde la biometría se vuelve un punto

central para que esto se cumpla; ya sean factores internos o externos que busquen atentar contra estos activos podría afectar de gran manera los objetivos de la empresa.

2.2.7 Tipos de biometría

La biometría basa es una técnica en medir o identificar rasgos biológicos de la persona, los cuales son únicos y los diferencia de los demás; este grupo de características resultan difíciles de perder, perdurables con el tiempo e intransferibles, y estas a su vez se dividen en 2 grupos, según Cadillo (2018, p.30) y Vallejo y Carrera. (2017, p.21):

- **Rasgos Fisiológicos o Estáticos,** referido a las características físicas de la persona, inalterables y que se presentan en todas las personas, entre los más importantes tenemos:
  - ✓ **Huella Dactilar,** método de identificación más antiguo usado para reconocer personas en el ámbito forense y policial, esta característica es singular en las personas, ya que incluso los gemelos idénticos no la comparten. Su medición requiere de muchos recursos tanto de procesamiento como de almacenamiento, sin embargo, es considera un sistema económico, confiable, y sencillo de usar, también, su nivel de exactitud es muy elevada, lo que resulta en uno de los sistemas más utilizados actualmente.
  - ✓ **Reconocimiento de Iris,** método referido al sentido de la vista del ser humano, haciendo uso del órgano ojo, más específicamente toma la

información de los patrones del iris que se encuentra en esta, este rasgo es muy distintivo en cada persona. Es evidente que requiere la participación de la persona, quien deberá acercarse al sensor encargado de escanear el ojo y tomar la información, y si bien el proceso no representa ningún riesgo para la salud de la persona, la tecnología que utiliza es cara, además, hay sistemas menos intrusivos y con una mejor efectividad en base al precio que tienen.

- ✓ **Reconocimiento de la voz,** resulta de una combinación de características físicas y de conducta de la persona, ya que, si bien está presente en la mayoría de las personas y usado a diario, pero no resulta invariable en el tiempo, dado que, se ven influenciadas por la edad, alguna condición médica o el estado emocional de la persona en un determinado momento. El proceso de reconocimiento se dificulta por el ruido externo presente en el ambiente, así como la calidad de la muestra de voz que se tome, por lo que, el resultado que devuelve es la que tenga un mayor grado de similitud entre una lista de candidatos. Además, se debe considerar la facilidad con la que puede ser imitada y su dificultad al distinguir una voz de otra. Sin embargo, esta característica es bastante aceptable y accesible.
- ✓ **Reconocimiento de la retina,** es una técnica muy segura que hace uso del patrón vascular presente en la retina de la persona, estas son invariantes a lo largo del tiempo, a la vez que son únicas en cada persona al igual que con la huella digital. Su nivel de seguridad radica

en la dificultad para poder replicar estos patrones (venas), sin embargo, requiere la presencia del usuario y cierto nivel de contacto con el sensor encargado de tomar la muestra, es así que la aceptación del usuario está condicionada.

- ✓ **Reconocimiento Facial,** como su nombre lo indica analiza los rasgos presentes en el rostro del individuo, el cual se realiza mediante programas que realizan complejos análisis numéricos de la imagen que se tome, además, el registro puede ser algo tardado, ya que requiere tomar varias fotografías que serán almacenadas para poder realizar la comparación respectiva, cuando el usuario desee validar su identificación.

- **Rasgos conductuales o dinámicos,** son rasgos basados en la conducta del ser humano, lo cual se puede considerar variante con el tiempo a diferencia de los rasgos físicos, entre los más comunes están:
  - ✓ Pulsaciones del tecleado, técnica que se basa en la singularidad de la persona para escribir haciendo uso del teclado, la cual varía entre cada persona, pero no exactamente única. Se mide por medio de la fuerza que se aplique, la velocidad con la que se presionan las teclas y la duración por cada pulsación. Los factores que influyen en la permanencia del patrón de tecleo son la habilidad, alguna condición médica, tipo de teclado o algún daño ocurrido en el mismo. Esta técnica resulta ser económica, ya que el gasto radica más que todo en el software encargado de realiza el reconocimiento.

- ✓ **Firma,** uno de los rasgos más comunes para la identificación de la persona, dado que la forma de firmar resulta característico de la persona, aunque con pequeñas variaciones en la mismas pero con la suficiente repetición se puede crear un patrón valido para validar la identidad del individuo, sin embargo, pueden existir firmas con variaciones significativas en cada repetición, además de que la firma puede variar a lo largo del tiempo y verse influenciada por el estado de la persona (físico o emocional).
- ✓ **Escritura,** técnica similar a la firma, resulta característico en cada persona y variable con el tiempo. Sin embargo, está sujeta a falsificaciones.

2.2.8 Elección de rasgo biométrico

Al momento de realizar un sistema de reconocimiento biométrico, uno de los factores más importantes a considerar es cuál es el rasgo biométrico más apropiado para cumplir con los objetivos que se deseen, para ello se puede considerar la capacidad de discriminar a un individuo de otro.

Sin embargo, Vallejo y Carrera. (2017) menciona "Para elegir un método adecuado se tiene que tomar en cuenta otros factores externos como el nivel de seguridad requerido, costo del sistema, tiempo de respuesta necesario entre otros factores" (p.22). Entonces, de lo mencionado por el autor, se concluye que se debe tener una descripción detallada de los sistemas biométricos existentes, identificar las características mencionadas y además tener en cuenta que cada sistema posee

debilidades y fortalezas que influyen mucho la confiabilidad del sistema en el entorno donde se va a implementar. Adicionalmente, su funcionamiento se basa en 3 principios fundamentales comunes para todos los sistemas, y tal como lo menciona Vallejo y Carrera. (2017, p.23):

- Todas disponen de un mecanismo automático, el cual se encargará de la detección y captura de la información que necesita el sistema para la validar la identidad del individuo en base a sus características biométricas.
- Todas disponen de la técnica de normalización de la imagen capturada, lo cual implica en ajustar las dimensiones de la imagen a un valor estándar establecido, sin alterar alguna característica importante de la imagen, luego de cual se almacenará y se realizará la comparación adecuada con los datos almacenados en la base datos y así validar su identificación.
- Todas disponen de una interfaz de comunicación, necesaria para mantener la comunicación entre los distintos elementos que integran este sistema.

2.2.9 Sistema de reconocimiento biométrico

Con base en la definición de la biometría, este tipo de sistema se encarga de la identificación de personas por medio del reconocimiento de algún rasgo físico o de conducta única en cada persona. En este sentido, para Guerra y Jiménez. (2021):

“El reconocimiento biométrico en combinación con componentes sistematizados que proporciona una estructura de seguridad fortificada conducente a la autenticación univoca de individuos, debido a que esta no depende de factores que puedan ser extraviados o hurtados, sino que funciona como un mecanismo individual e intransferible propio de cada persona.” (p.37).

En base a lo mencionado por el autor, un sistema de reconocimiento biométrico, hace referencia a un sistema de seguridad que diferencia de los métodos tradicionales enfocados a este fin, resulta mucho más confiable y preciso por estar diseñado a partir de elementos modernos que hacen posible la efectividad y robustez del sistema, logrando que difícilmente sea vulnerado. El sistema utiliza como credencial de identificación una característica única e intransferible en cada persona, es aquí donde radica su fortaleza y que en combinación con la tecnología adecuada se puede obtener una correcta validación de identidad de cada usuario registrado.

En este proceso de validación o autenticación de la identidad de la persona, también es necesario el uso de los componentes adecuados para lograr tal fin. De manera general este proceso comienza por la adquisición o captura del rasgo biológico que se analizara, esto se logra mediante un dispositivo lector capaz de realizar la lectura y adquisición correspondiente, luego de esto, en base a la configuración dada al sistema o al procedimiento que se realice se procede a guardar la información en la base de datos que se tenga, o sino, tomar una decisión en base a la información obtenida validando o no la identidad del usuario.

El proceso del sistema se basa en el reconocimiento es decir, en volver a conocer al usuario que ya estaba registrado en el sistema (base de datos), por lo que, el proceso

se resume en autenticar o validar si la muestra que se está analizando ya se ha registrado o no; este proceso se puede realizar de 2 maneras, por medio de la identificación o la verificación, la primera resulta en proceso más tardado porque necesita comparar la información que se recoge de la persona (muestra) con cada registro que tenga dentro de su base de datos del sistema con el objetivo de encontrar alguna similitud con alguna de estas y así devolver un resultado; la verificación implica el ingreso de alguna clave o credencial adicional junto con la muestra del rasgo biológico, de modo que, se tenga que comparar la muestra ingresada solo con el registro que se tenga almacenado bajo el patrón de la clave ingresada, lo que resulta en proceso más simple y rápido. Entonces, esta es otra de las consideraciones a tener en cuenta al momento de diseñar este tipo de sistema, ya que dependerá del objetivo que se busque y de los recursos disponibles para el desarrollo de este sistema. Sin embargo, como lo menciona Arteaga (2018) "Ejecutar una consulta de identificación en una base de datos biométrica con millones de registros también se ha vuelto mucho más rápido con el desarrollo de máquinas de computación avanzadas" (p.33), esto nos indica que la tecnología moderna ha hecho que este sistema haya conseguido considerables mejoras tanto en su capacidad de almacenamiento como el procesamiento, logrando que sea más eficiente.

Dentro del proceso de reconocimiento pueden darse 2 casos en particular, el falso rechazo o la falsa aceptación, y tal como su nombre lo indica, ocurre cuando rechaza erróneamente a un usuario que se encuentre registrado en la base datos, o por el otro lado se acepte a un usuario que no se encuentre registrado, respectivamente. Estos casos pueden presentarse sobre todo cuando la persona ha sufrido alguna condición

que haya alterado el rasgo biológico que el sistema necesita para reconocerlo; además, cada uno de estas situaciones pueden ser representados como parámetros porcentuales que permitirán conocer o definir la exactitud del sistema, ya que básicamente mide la cantidad de errores que ha tenido el sistema durante su funcionamiento en un cierto periodo de tiempo.

De todo lo mencionado, los sistemas biométricos representan un gran avance en la forma de identificar o autenticar a una persona, su eficiencia y rapidez han significado un gran impacto en todo el mundo, llegando a resultar necesario para muchas empresas o instituciones para evitar algún tipo suplantación con sus empleados o clientes.

2.2.10 Estructura general de un sistema biométrico

Partiendo de la definición de un sistema, el cual se refiere a un conjunto de elementos que tienen una relación o trabajan en conjunto para lograr un objetivo en común, en este sentido, la inclusión de la biometría implica tener conjunto de elementos destinados a reconocimiento de una persona a través de la medición de los patrones únicos presentes en las características biológicas que cada uno posee, para ello es necesario considerar elementos destinados a la captura de la muestra, el procesamiento de la misma y su posterior almacenamiento, para que luego puedan ser comparados con nuevas muestras ingresadas y así identificar a la persona. Entonces, estos sistemas se enfocan en el mapeo de un rasgo biológico en particular, pero solo uno de ellos, aunque todos funcionan bajo este mismo principio apoyándose en la tecnología.

Debido a la naturaleza de este proceso, es importante destacar algunos puntos clave en su desarrollo, tal como menciona Guerra y Jiménez. (2021, p.36):

La calidad de la captura, elemento que es brindado por el individuo, resultando en la parte determinante del proceso, sin embargo, está sujeto diversas interferencias ya sea por causas externas como la humedad o suciedad, entre otros; o por el mal posicionamiento de la persona al momento de tomar la muestra. El pre procesado, elemento que se encarga de poder corregir los errores o degradación en la muestra que se pueda presentar por los factores anteriormente mencionados. Umbral de decisión, nivel de calidad requerido de la muestra, para poder ser comparada con los datos que se tengan almacenados.

2.2.11 Requerimientos de un sistema biométrico

La confiabilidad de este tipo de sistema se basa en la elección adecuada del rasgo biológico a analizar, pero, estas deben cumplir con ciertos requisitos, y tal como mencionan Vallejo y Carrera. (2017, p.26) y Fernández (2017, p.21):

- Unicidad: Los patrones o características del rasgo debe ser única e irrepetible en la persona, es decir, 2 personas no deben poseer el mismo rasgo, la probabilidad es baja.
- Universalidad: El rasgo debe estar presente en todas las personas.
- Permanencia: Este rasgo no debe variar con el tiempo o a corto plazo.
- Cuantificación: El rasgo debe poder ser medida cuantitativamente.

En base a estas condiciones, debe considerarse que no todos los rasgos poseen las mismas ventajas o la facilidad con la que son obtenidas, entonces, su elección

dependerá del nivel de seguridad que se requiera, la disponibilidad de recursos y los costos que estos impliquen.

2.2.12 Huella dactilar

Rasgo fisiológico del ser humano más utilizado para la identificación de la persona, su uso se remonta desde el ciclo XIX, donde su análisis se realizaba de forma visual capturándose haciéndose uso de la tinta y papel, para su posterior almacenamiento; desde entonces hasta la actualidad el proceso se ha automatizado gracias a los avances tecnológicos, por lo que el procedimiento se vuelve más confiable, rápido y preciso. Y su propio desarrollo también ha resultado muy útil y una opción importante en los campos de la seguridad, civil, forense y policial.

Este rasgo fisiológico resulta ser único en cada persona, y su patrón es formado por las células epiteliales presentes en los dedos, los cuales son formados desde los primeros meses de formación del feto y se mantienen hasta la defunción de la persona, por lo que, este rasgo determina la identidad de cada persona de modo que ninguna otra posee el mismo patrón ya sea entre familiares o incluso gemelos idénticos.

De esto último es donde radica la ventaja para sus distintas aplicaciones, además, de su sencillez en su uso, resultan económicos y no son invasivos con el cuerpo.

Entonces conceptualmente tenemos que la huella dactilar es la impresión visible del patrón de formado por las crestas del dedo sobre una superficie en particular, es así que, según Vallejo y Carrera. (2017, p.23):

- Huella latente, marcas producidas por el contacto del dedo sobre una superficie debido al sudor o la grasa de la piel, estas marcas permanecen ocultas, y no se pueden apreciar a simple vista.
- Huella dactilar positiva, impresión de la huella sobre una superficie haciendo uso de una sustancia adicional.
- Huella dactilar negativa, impresión de la huella sobre una superficie blanda, capaz de registrar el relieve del patrón.

El patrón característico de cada huella recibe el nombre de minucias, que son precisamente esas particularidades los que generan la forma de la impresión dejada por el dedo.

2.2.13 Elementos de la huella dactilar

Para el desarrollo o diseño de un sistema biométrico basado en huella dactilar es importante conocer los elementos que la componen, estas se refieren a los tipos de minucias que se pueden encontrar en las huellas, de esta manera tenemos un mejor entendimiento del proceso que se debe seguir el sistema para lograr la autenticación de la persona, y son las siguientes:

- Cresta, relieves o curvas formado por las líneas o segmentos del dedo.
- Bifurcación, división de la cresta en 2.
- Divergente, dos crestas que se mantienen paralelas y en algún punto llegan a separarse.
- Valles, espacio formado por la separación entre 2 crestas paralelas.

2.2.14 Reconocimiento de huellas dactilares

Con base en lo mencionado a cerca de las huellas dactilares, el reconocimiento de las mismas resulta en uno de los métodos más utilizados y conocidos, debido a su alto nivel de aceptación. Además, cumple con todos los requerimientos de un sistema de reconocimiento biométrico eficiente, desde el punto de la universalidad es un rasgo fisiológico que poseen todas las personas, aunque con ciertas excepciones en casos donde las personas hayan sufrido algún daño o condición que impida obtener su huella dactilar (quemaduras, amputaciones, entre otros). Respecto a la unicidad, la huella dactilar es única en cada persona, que no se repite incluso entre familiares o gemelos idénticos. La huella también es permanente o invariable con el tiempo, ya que se mantiene desde la formación del feto hasta incluso después de la defunción de la persona, sin embargo, sigue sujeta a que la persona haya sufrido alguna condición mencionada anteriormente, que impida la medida correcta de la muestra. Es cuantificable, ya que se puede tomar una imagen de la muestra y con la correcta aplicación de software puede transformarse a un conjunto de valores numéricos.

El rendimiento del sistema se enfocara en cómo se implementan las diversas partes que hacen posible el funcionamiento correcto del sistema, y que son la fase de captura, extracción de los datos, comparación con los datos almacenados, etc. Estos elementos requieren de un software, por lo que, dependen mucho del algoritmo con la que son diseñados para poder obtener mejores resultados en el menor tiempo posible, por otro lado, para la obtención de la muestra se hace uso de los sensores encargados de esta tarea los cuales tendrán un nivel de calidad en la obtención de este.

En base todo a estos puntos mencionados se obtendrá un cierto nivel de aceptabilidad, y así como menciona Guerra y Jiménez (2021) "(…) la mayoría de opiniones respecto al reconocimiento de huellas dactilares resultan ser muy favorables" (p.41). En conclusión, esta técnica de reconocimiento de personas resulta en una de las más utilizadas para implementación de sistemas biométricos encargados de la identificación de personas.

2.2.15 Componentes de un sistema biométrico dactilar

Cuando nos referimos a la arquitectura de un sistema, se habla de representación en su conjunto, lo cual incluye los componentes de hardware y software que necesitaran para lograr su objetivo, y la manera de cómo estos se relacionan entre sí, ya sea en base a su funcionalidad o la arquitectura propia que posee cada uno de estos, y al mismo tiempo de cómo estas interactúan con el ser humano. Entonces, tal como menciona Arteaga (2018) "los diferentes sistemas de reconocimiento biométrico pueden tener diferentes conjuntos de sensores, subsistemas y algoritmos para lograr el objetivo de reconocimiento y coincidencia de patrones específicos" (p.43). Entonces, independientemente de sistema biométrico que se vaya a utilizar, el procedimiento que se sigue es el mismo, con variación en el tipo de componentes que permitan lograr su objetivo.

Todo comienza con la adquisición de la muestra, lo que representa una imagen digital de la huella que se va a analizar, el cual puede ser obtenido por medio de un dispositivo denominado sensor o lector de huella dactilar, luego, esta imagen será procesado adecuadamente para crear una "plantilla", el cual contendrán un conjunto

de puntos que representan las minucias características de la muestra tomada. De lo mencionado, podemos determinar que este lector de huella es parte vital del sistema ya que los elementos siguientes dependerán de la información que obtenga. La calidad de los sensores ha aumentado junto al avance de la tecnología, a pesar de ello ciertas condiciones pueden ocasionar algún tipo de error al momento de tomar la muestra, es por ello, que los elementos posteriores a este se encargaran de poder corregir estas deficiencias.

- Procesamiento de Imagen, debido a que la obtención de la muestra por medio del sensor puede tener ciertas deficiencias por ciertos factores comprometiendo la calidad de la imagen, es necesario la inclusión de un algoritmo (software) que se encargue de poder mejorar o compensar las deficiencias en la imagen, de modo que, pasen a la siguiente etapa de extracción de minucias con la mayor calidad posible, esto garantiza un buen rendimiento del sistema además de su robustez, para poder obtener el mejor resultado posible para la verificación de la identidad.
- Extracción de minucias, para esta etapa el método más usado es la de número de cruce (CN), respecto a esto Arteaga (2018) menciona que,

"Este método implica el uso de la imagen del esqueleto donde el patrón de flujo del caballete está conectado por ocho. Las minucias se extraen escaneando el vecindario local de cada píxel de la cresta en la imagen usando una ventana de 3 x 3."

Este método sigue un algoritmo basado en el análisis de los pixeles de la imagen obtenida como muestra, sin embargo, este método puede incluir algunas

falsas minucias debido a alguna deficiencia o ruido que haya estado presente en la imagen original, por lo que, resulta necesario una etapa o subsistema adicional de procesamiento de imagen, encargado de poder validar las minucias obtenidas, como el algoritmo Tico y Kuosmanen, el cual basa su funcionamiento a partir de dos conjuntos de minucias, los cuales serán analizados punto a punto, para posteriormente determinar si se trata del mismo dedo o no. Para ello es necesario 2 etapas adicionales. Una primera etapa de alineación, donde a partir del cálculo de la similitud de las crestas de cualquier minucia de la imagen, si resulta mayor a un umbral establecido se procede a transformar cada conjunto de puntos en un nuevo sistema de coordinación. Una segunda etapa de emparejamiento, donde haciendo uso de un algoritmo de coincidencia elástica para hacer el conteo de cada par de minucias que coincidan, dicha coincidencia se genera a partir de que ambas compartan similitud en su posición y dirección.

2.2.16 Técnicas de reconocimiento dactilar

Por lo general estas técnicas se enfocan en la comparación de la imagen que se adquiere como muestra y la que se tenga almacenada (registro), la imagen que se captura se encuentra en escala de grises, de esta manera se puede lograr que esta imagen se encuentre con la orientación y posición correcta para realizar la comparación.

Las técnicas utilizadas para realizar este proceso son:

- Técnicas basadas en minucias, esta técnica hace uso de las minucias que se encuentran dentro de la huella dactilar, registrando tanto su

forma como la posición del mismo, y en consecuencia se establecen como mediciones, entonces, este método requiere que luego de la obtención de la muestra se identifiquen las minucias correspondientes y sus mediciones correspondientes, para ello es necesario que sigan ciertos pasos, el cual comienza con la toma de la muestra de la huella, luego del cual se le aplicara una normalización en las dimensiones de la imagen, a fin de evitar problemas al momento de hacer la verificación, y posteriormente identificar las minucias correspondientes en base a las consideraciones apropiadas.

- Técnica basada en correlación, esta técnica no usa solamente las minucias para hacer las comparaciones, sino que hace uso de la información completa de toda la estructura de las crestas. De esta manera, la comparación se realiza con el cálculo del nivel de correlación que exista entre 2 imágenes de huella dactilar. En este sentido Cadillo (2018), asegura que "el grado de similitud entre dos huellas se basa en que la correlación espacial entre dos imágenes se hace máxima cuando las dos imágenes son idénticas" (p.53). De lo mencionado, podemos concluir que, si 2 imágenes pertenecen a la misma huella, el grado de similitud debe ser la máxima, sin embargo, esto no siempre ocurre debido a diversos factores que pueden afectar al nivel de correlación, como los que se mencionan a continuación:
    - ✓ Cierto desfase o desplazamiento que puede existir entre las imágenes, como consecuencia de la obtención de la muestra.

- ✓ Así como el desplazamiento una imagen, puede darse el caso de que la imagen tenga una rotación respecto a la otra.
- ✓ Ciertas deformaciones no lineales de la piel (arrugas) puede impedir la correcta alineación de las imágenes, disminuyendo considerablemente el valor de la correlación.
- ✓ La calidad de la imagen también puede interferir en la detección de los patrones que se necesita para proceder con la correlación.

2.2.17 Seguridad física

Tal como hace mención Pampa y Lozano (2020) "Protección de las instalaciones físicas contra sabotaje o accidentes provocados por la presencia de personas no autorizadas o mal intencionadas". Entonces, de lo mencionado por el autor la seguridad física se refiere a las amenazas y riesgos que enfrentan las instalaciones o los bienes, por lo que surge la necesidad de poder implementar planes o métodos destinados a la prevención o limitación de los resultados negativos producto de las acciones dañinas en contra de su seguridad. Para este fin se vuelve necesario la inclusión de sistemas de control de acceso, capaces de mantener un monitoreo automatizado de las personas que tengan acceso a estos ambientes o bienes, esta seguridad se puede reforzar con cámaras de vigilancia o con un personal especializado de seguridad. Esta definición puede llegar a extenderse a la protección de un mayor tipo de daños externos como pueden ser los factores climáticos (Fernández, 2017).

2.3. Definición de términos básicos:

- ✓ Falso Rechazo/Aceptación. “Se produce cuando el sistema rechaza a un usuario autorizado o acepta a uno no autorizado. Se cuantifica mediante la probabilidad (porcentaje) de falsos rechazos o falsas aceptaciones”.
- ✓ Pixel. “Es la parte más pequeña de una imagen al que se puede aplicar individualmente un color o una intensidad o que se puede diferenciar de los otros mediante un determinado procedimiento”.
- ✓ Imagen Digital. “Una imagen digital se compone de una agrupación de píxeles, cada uno con un valor de intensidad o brillo asociado. Una imagen digital se representa mediante una matriz bidimensional, de forma que cada elemento de la matriz se corresponde con cada pixel en la imagen”.
- ✓ Minucias. “Aparición de singularidades en las líneas, como puntos de bifurcación, cercado, unión, terminación, etc.”.
- ✓ Algoritmo. “Conjunto ordenado de operaciones sistemáticas que permite hacer un cálculo y hallar la solución de un tipo determinado de problemas”.
- ✓ Control: “Método para manejar el estado de un aparato, máquina o proceso”.
- ✓ Sensor: “Elemento que permite medir diversas señales, por ejemplo, presión, temperatura, nivel, presencia”.
- ✓ Transmisor: “Capta la variable del proceso por medio del sensor y transmite una señal normalizada a distancia”.

2.4. Hipótesis e investigación

2.4.1. Hipótesis general

- El sistema de control de acceso biométrico se relaciona con la seguridad física en la institución educativa 20786, Vilcahuaura 2022

2.4.2. Hipótesis específicas

- El sistema de identificación se relaciona con la seguridad física en la institución educativa 20786, Vilcahuaura 2022

- Las características físicas se relacionan con la seguridad física en la institución educativa 20786, Vilcahuaura 2022

- El registro y autenticación se relaciona con la seguridad física en la institución educativa 20786, Vilcahuaura 2022

2.5. Operacionalización de las variables

Las variables de investigación se presentan a continuación:

- **Variable 1:** Sistema de control de acceso biométrico
- **Variable 2:** Seguridad física

2.5.1 Matriz de Operacionalización de variables.

Cuadro 1.

Matriz de Operacionalización de variables

VARIABLE	DEFINICION CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	INSTRUMENTO
Sistema control de acceso Biométrico	Es un sistema de identificación, el cual haciendo uso de las características físicas únicas del ser humano tiene el objetivo de realizar el registro y autenticación de personas para el ingreso o salida de un lugar o área en particular.	Sera medido a través de su relación con la seguridad física y la aceptación de la institución estatal.	X.1 Sistema de identificación	X.1.1. Tipos X.1.2. Nivel de confiabilidad X.1.3. Costo	Encuesta basada en la escala de Likert para medir la relación entre las variables
			X.2 Características físicas	X.2.1 Rasgos Únicos X.2.2 Dificultad de detección.	
			X.3 Registro y autenticación	X.3.1 Cantidad de usuarios X.3.2 Tiempo de respuesta X.3.3 Automatizado	
Seguridad Física.	La seguridad física es el conjunto de mecanismos y acciones que buscan la identificación y prevención de riesgos o situaciones riesgosas, con el propósito de brindar protección a algún recurso o bien material.	Sera medido a través de su relación con el sistema de control de acceso biométrico.	Y.1 Mecanismos	Y.1.1 Tipo. Y.1.2 Fiabilidad. Y.1.3 Complejidad.	
			Y.2 Riesgos	Y.2.1 Amenaza. Y.2.2 Vulnerabilidad.	
			Y.3 Protección	Y.3.1 Nivel de seguridad. Y.3.2 Técnica.	

Nota: Elaboración propia.

CAPÍTULO III: METODOLOGÍA

3.1 Diseño metodológico

3.1.1 Diseño de la investigación

Dado que se tiene como objetivo determinar la relación que existe entre el control de acceso biométrico y la seguridad física de la Institución Educativa 20786, la investigación será de tipo aplicada, con nivel correlacional, ya que se usará el conocimiento científico, para la formulación de problemas e hipótesis, con el objetivo de poder resolver algún problema existente en la sociedad. (Ñaupas, Mejía, Novoa y Villagómez, 2014, p.93).

Con un diseño metodológico no experimental correlacional, dado que lo se busca es, "(…) establecer el grado de correlación o de asociación entre una variable (X) y otra variable (Z) que no sean dependientes una de la otra." (Ñaupas, Mejía, Novoa y Villagómez, 2014, p. 343)

3.1.2 Enfoque de Investigación

Este trabajo de investigación se llevará a cabo bajo el planteamiento metodológico del enfoque Mixto, debido a que por temas de adaptación es el que mejor encaja con las definiciones y necesidades de la problemática.

Al respecto el enfoque mixto, "pretende conjugar los procedimientos de la investigación cuantitativa con los de la investigación cualitativa, en el convencimiento de que el reduccionismo, el extremismo en la investigación no conducen a nada bueno." (Ñaupas, Mejía, Novoa y Villagómez, 2014, p. 99)

Teniendo ya definido nuestro enfoque mixto se procede a utilizar la técnica de la encuesta para obtener datos medibles sobre la relación que existe entre el control de acceso biométrico para los docentes y la seguridad física de los recursos educativos de la Institución Educativa 20786 Vilcahuaura.

3.2 Población y muestra

3.2.1 Población

Para definir el concepto de población, nos basaremos en las palabras de Ñaupas, Mejía, Novoa y Villagómez (2014) que nos mencionan que "la población es el conjunto de individuos personas o instituciones que son motivo de investigación." (p.246).

La población de estudio estará conformada por 25 personas, que representan los docentes que laboran en esta Institución Educativa, y que son ellos quienes tendrán la autorización de acceso a este ambiente y tendrán el registro de su huella dactilar.

Luego, respecto a la muestra del estudio, Córdova (2017) precisa que: "Cuando la población es relativamente pequeña no es recomendable extraer de ella una muestra, es preferible realizar el estudio en toda la población. Pero en este caso se denomina simplemente "Grupo de estudio", ya que no hay población sin muestra ni muestra sin población" (p.103)

En conclusión, en el presente proyecto de investigación se trabajara con un grupo de estudio de 25 personas, que representan a los docentes que laboran

en esta institución educativa.

3.2.2 Muestra

Para este trabajo de investigación se utilizará un muestreo no probabilístico del tipo muestreo por accidente, ya que según Ñaupas, Mejía, Novoa y Villagómez (2014) en este tipo de muestreo "el investigador escoge los individuos de la muestra según las circunstancias de mayor facilidad […] se escogerá la muestra entre las personas que están más al alcance del investigador" (p.254). Esto debido a que se les pedirá la colaboración de los docentes que laboran en esta Institución Educativa forme parte de la experimentación.

3.3 Técnica para la recolección de datos

Podemos decir que la técnica de recolección de datos es la herramienta con la sustentaremos los resultados al final de la investigación, para lo cual ya teníamos decidido cuál sería la herramienta que nos ayudaría en el trabajo.

Utilizaremos la encuesta como técnica de recolección de datos para la presente investigación.

3.3.1 Instrumentos para la recolección de datos

Para esta investigación hemos seleccionado una encuesta con preguntas cerradas como instrumento de recolección de datos y nos basaremos en la escala de Likert.

Podemos definir el escalamiento de Likert según Hernández (2014) como:

"Consiste en un conjunto de ítems presentados en forma de afirmaciones o juicios, ante los cuales se pide la reacción de los participantes. Es decir, se presenta cada afirmación y se solicita al sujeto que externe su reacción eligiendo uno de los cinco puntos o categorías de la escala. A cada punto se le asigna un valor numérico. Así, el participante obtiene una puntuación respecto de la afirmación y al final su puntuación total, sumando las puntuaciones obtenidas en relación con todas las afirmaciones" (p.238).

Para evaluar la relación que existe entre el control de acceso biométrico y la seguridad física de la Institución Educativa se llevara a cabo un cuestionario tomando el modelo o estructura Likert. Este cuestionario estará compuesto por 15 ítems, que corresponden a 6 dimensiones:

- Sistema de identificación
- Características físicas
- Registro y autorización
- Mecanismos
- Riesgos
- Protección

Para poder evaluar cada una de las dimensiones cogimos las opciones ya preestablecidas que nos brinda el escalamiento de Likert para puntuar nuestro cuestionario, estas son:

- Totalmente de acuerdo (5)
- De acuerdo (4)
- Neutral (3)
- En desacuerdo (2)
- Totalmente en desacuerdo (1)

En cuanto a las puntuaciones para la escala de Likert se obtienen sumando los valores alcanzados respecto de cada frase. Para nuestro caso el número de ítems es 16 por lo que puntuación mínima posible es 16 y la máxima es de 80. Mientras más baja sea la puntuación el encuestado tendrá una actitud que tiende a estar en desacuerdo con lo que se planteara.

3.4 Técnicas para el procesamiento de la información

Para la investigación que estamos llevando a cabo se utilizara la técnica de la estadística descriptiva, para Ñaupas, Mejía, Novoa y Villagómez (2014) la estadística descriptiva tiene:

"Como objeto fundamental, procesar, resumir y analizar un conjunto de datos obtenidos de las variables estudiadas. Estudia un conjunto de medidas o estadígrafos mediante los cuales es posible comprender la magnitud de las variables estudiadas, como las medidas de tendencia central y las medidas de dispersión".

Herramientas de procesamiento de datos.

Para llevar a cabo la organización, presentación y tabulación de datos que se tendrán por el cuestionario que se hará a cada uno de los docentes de la Institución Educativa 20786, Vilcahuaura y se utilizará el programa SPSS V26.

3.5 Matriz de consistencia

Cuadro 2.

Matriz de Consistencia: "DISEÑO DE UN SISTEMA DE CONTROL DE ACCESO BIOMETRICO Y LA SEGURIDAD FISICA DE LA INSTITUCION EDUCATIVA 20786, VILCAHUAURA 2022"

PROBLEMA	OBJETIVOS	JUSTIFICACIÓN	HIPÓTESIS	VARIABLES	INSTRUMENTOS
Problema general ¿Qué relación existe entre el sistema de control de acceso biométrico y la seguridad física en la institución educativa 20786, Vilcahuaura 2022? **Problemas específicos** ¿Qué relación existe entre el sistema de identificación y la seguridad física en la institución educativa 20786, Vilcahuaura 2022? ¿Qué relación existe entre las características físicas y la seguridad física en la institución educativa 20786, Vilcahuaura 2022? ¿Qué relación existe entre el registro y autenticación y la seguridad física en la institución educativa 20786, Vilcahuaura 2022?	**Objetivo general** Establecer la relación entre el sistema de control de acceso biométrico y la seguridad física en la institución educativa 20786, Vilcahuaura 2022. **Objetivos específicos** Establecer la relación entre el sistema de identificación y la seguridad física en la institución educativa 20786, Vilcahuaura 2022. Establecer la relación entre las características físicas y la seguridad física en la institución educativa 20786, Vilcahuaura 2022. Establecer la relación entre el registro y autenticación, y la seguridad física en la institución educativa 20786, Vilcahuaura 2022.	**Justificación metodológica** Esta investigación aportara la experimentación, descripción, análisis e interpretación de los procesos que se podrían seguir para darles una alternativa de solución en cuanto a la restricción de acceso de personal al área de servidores electrónicos y equipos de red a cierto número de personal , todo mediante un control de acceso biométrico con el uso de huella dactilar, por lo que los principales beneficiados serían todos los integrantes de esta Institución Educativa, ya que evitara daños o perdidas de los recursos educativos importantes para la Institución, el cual podría ocasionar molestias a los docentes y alumnos que dependen de estos recursos para el normal desarrollo de sus clases. **Justificación social** Como sabemos el control de acceso es un aspecto muy importante al momento de tener protegida cierta área en donde se encuentran objetos, maquinas, instrumentos o información muy confidencial y valiosa, ya que de esta manera se garantiza la seguridad de estos mediante una estricta selección de personal capacitado para el ingreso y manipulación de los mismo sin tener que correr demasiados riesgos.	**Hipótesis general** El sistema de control de acceso biométrico se relaciona con la seguridad física en la institución educativa 20786, Vilcahuaura 2022 **Hipótesis específicas** El sistema de identificación se relaciona con la seguridad física en la institución educativa 20786, Vilcahuaura 2022 Las características físicas se relacionan con la seguridad física en la institución educativa 20786, Vilcahuaura 2022 El registro y autenticación se relaciona con la seguridad física en la institución educativa 20786, Vilcahuaura 2022	**Variable 1:** Sistema de control de acceso biométrico **Variable 2:** Seguridad física	Encuesta para medir la relación entre la variable independiente y dependiente

CAPÍTULO IV: RESULTADOS

4.1 Análisis de resultados

Este tipo de sistema está enfocado en la seguridad interna de la Institución Educativa 20756 - Vilcahuaura, ya que, nos permite controlar la cantidad de personas o usuarios que ingresan a un ambiente o algún área restringida, donde se almacenen los recursos indispensables para el normal desarrollo de las actividades de esta institución educativa, es decir, solo tendrán acceso aquellas personas que tengan autorización para el ingreso y se encuentren registradas en este sistema, haciendo uso de una característica física intrínseca de todo ser humano, como es el caso de la huella dactilar, de este modo, a diferencia de los métodos tradicionales de seguridad que se utilizan para la protección de dichos recursos, este sistema resulta más efectivo y seguro.

Dentro de los elementos principales utilizados, están el microcontrolador y el sensor de huella dactilar, cuyas especificaciones técnicas son parámetros importantes a tomar en cuenta dentro del diseño del sistema, debido a la cantidad de componentes electrónicos utilizados, la cantidad de información que se debe manejar, la cantidad de usuarios a registrar y el tiempo de respuesta del sistema para un funcionamiento efectivo.

Para la identificación de la huella dactilar, se utiliza un sensor óptico, el cual se encarga de capturar la imagen de la huella dactilar que se ubique en su lente y luego compara esta imagen con todas las muestras que tiene almacenado en su memoria interna para finalmente enviar la respuesta al microcontrolador mediante comunicación USART, el cual se encargara de enviar una señal para abrir la puerta en caso de que la lectura del sensor magnético colocado en la puerta indique que se

encuentra cerrada; adicionalmente, si la huella identificada es del encargado de añadir a nuevos usuarios (Director(a) de la Institución Educativa o docente encargado del aula), se le permitirá el acceso a un menú de opciones donde podrá ser capaz de registrar a nuevos usuarios, ver la cantidad de usuarios que ya han sido registrados, o eliminar usuarios ya registrados, las opciones podrán ser elegidas haciendo uso de unos pulsadores de control implementados.

4.1.1 Diseño del esquema electrónico

El diseño se realizó con ayuda del Software Proteus 8 Profesional, así que, teniendo en cuenta lo descrito anteriormente, el diseño de este sistema resultó de la siguiente manera:

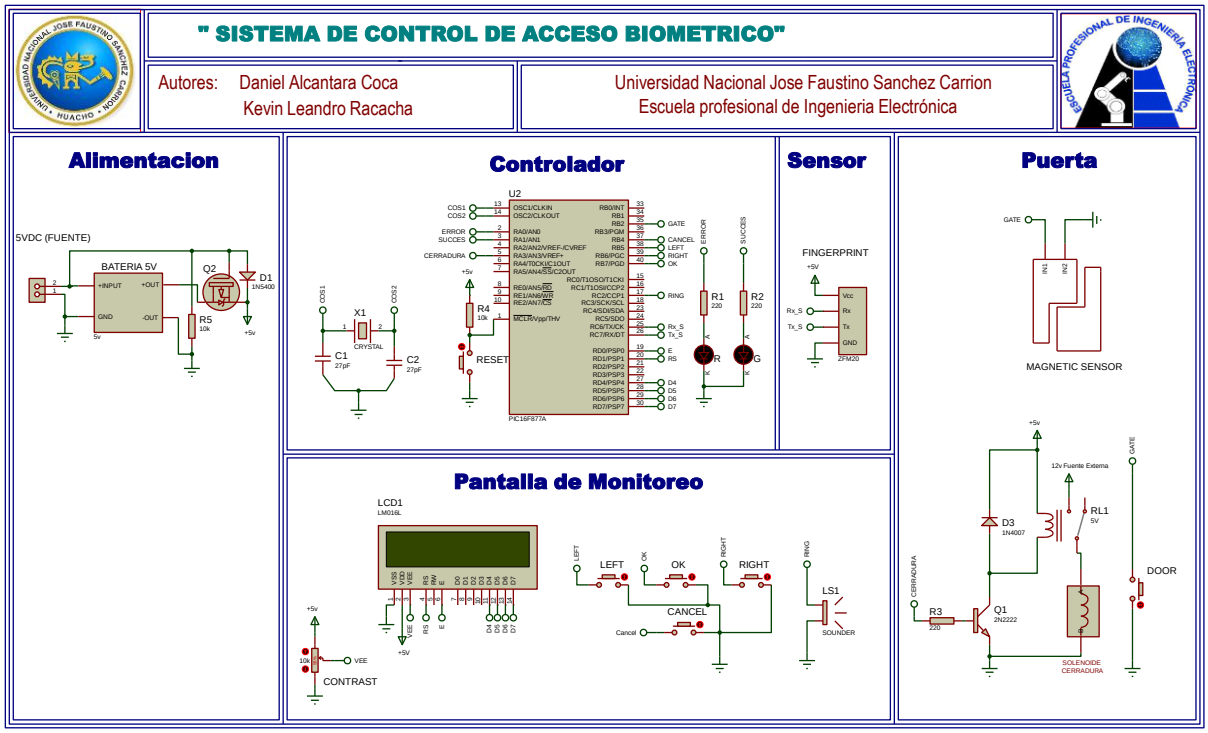


Figura 1. Esquema electrónico del sistema de control de acceso biométrico.

Fuente: Propia

4.1.2 Descripción del sistema

La elección de los componentes utilizados para el diseño del sistema, se hizo en base a su disponibilidad en el mercado, precio y calidad:

a) Microcontrolador. Se utilizó el microcontrolador 16F877A, el cual posee las características técnicas adecuadas para el correcto funcionamiento de todo el sistema, este componente es el encargado de controlar y procesar la información recibida por de los sensores y pulsadores, y devolver una respuesta en el menor tiempo posible.

b) Sensor de Huella Digital. El sensor de huella dactilar ZFM60 es que el cumplía con las características adecuadas para este proyecto y está disponible en el mercado nacional. Es un sensor óptico que captura y almacenas imágenes de las huellas dactilares que se ubiquen en la lente de este sensor, tiene capacidad para almacenar hasta 232 muestras distintas, alimentación de 5 voltios, trabaja con una memoria flash, nos proporciona la opción de poder eliminar alguna muestra almacenada, además, utiliza el protocolo de comunicación serial UART, el cual es compatible con el microcontrolador elegido.

Figura 2. Sensor óptico biométrico ZFM60

Fuente: https://avelectronics.cc/

c) Pantalla de Monitoreo. Para la visualización de los distintos estados del sistema, se optó por utilizar la pantalla LCD Hitachi HDD44780U 16X2, el cual nos ofrece un total de 32 caracteres, repartidos en 2 filas de 16 caracteres cada uno, utiliza una comunicación paralela (4 u 8 bits) para configurarlo y poder enviar caracteres o cadena de caracteres, las conexiones se realizó al puerto D del microcontrolador, es así que, este puerto se encarga del envío de los comandos para la configuración de la pantalla o mostrar caracteres. Así, la pantalla lcd 16x2, está encargada de monitorear el funcionamiento del sistema en tiempo real.

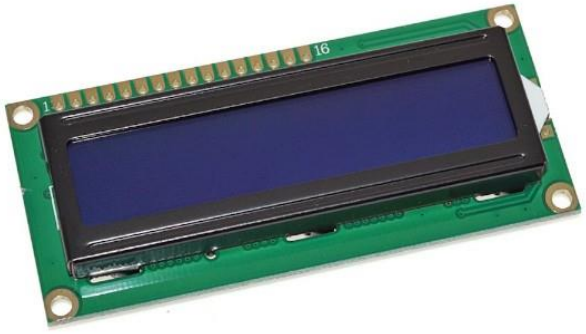


Figura 3. Pantalla LCD 16X2

Fuente: https://mastertronicventas.com/index.php/producto/pantalla-lcd-16x2-azul/

d) Pulsadores de Control. Para poder iniciar el proceso de identificación de la huella dactilar e ingresar al aula, así como, viajar entre las opciones del menú (agregar usuario, borrar usuario y ver cantidad de usuarios), se implementaron 4 pulsadores en configuración pull-up que van conectados al puerto A del microcontrolador, y estos se encargaran de enviar una señal digital para indicar

al microcontrolador si han sido presionados, y ejecute la acción correspondiente.

e) Sensor Magnético para puertas. Este tipo de sensor consta de 2 partes que van instalados en la esquina superior de la puerta, una de las partes posee 2 pines, los cuales mediante una configuración pull-up irán conectados al microcontrolador y a la línea común del circuito, la segunda pieza es un imán que activara la primera pieza, de modo que, si ambas se encuentran juntas o separadas se enviara un nivel alto o bajo de una señal digital, indicando que la puerta se encuentra cerrada o abierta.

Figura 4. Sensor magnético para puertas MC-38

Fuente: https://naylampmechatronics.com/

f) Cerradura Eléctrica. Esta cerradura tiene la misma funcionalidad que las cerraduras mecánicas convencionales, pero a diferencia de estas, la cerradura eléctrica se activara cuando se lo polarice con un voltaje de 12VDC, dicha activación estará controlada por el microcontrolador en base a la información que tenga del sistema, sin embargo, el voltaje que entrega es inferior a la

requerida, es por ello, que se adaptó un transistor tipo NPN como un Interruptor (Corte/Saturación), así, cuando se envíe la señal de activación por parte del microcontrolador, el transistor se activara polarizando el relé de 5v, y dejando pasar el voltaje de 12v para activar la cerradura eléctrica.

Figura 5. Cerradura Eléctrica 12v Chapa Puerta Solenoide

Fuente: https://www.promart.pe/cerradura-electrica-12v-doble-llave---boton/p?gclid=Cj0KCQiAxbefBhDfARIsAL4XLRp1HXl4vpKI9Iqmty7x-bGMoY5g26NRl4INfBMNEunwr5NLgpPm08IaAj2hEALw_wcB

La conexión de esta cerradura es de la siguiente manera:

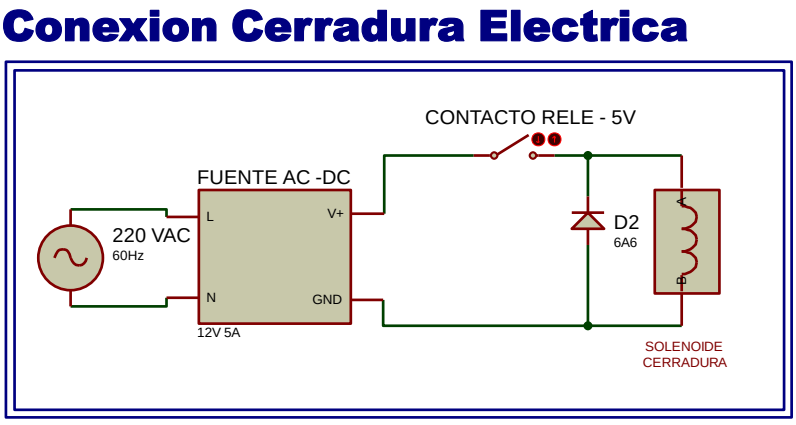


Figura 6. Circuito de la cerradura eléctrica.

Fuente: propia

Cabe resaltar que este tipo de cerraduras funcionan a 12 VAC y 1.2A; o 12VDC a 3 A, es por ello que se ha planteado una fuente de 12VDC a 5A y un diodo de 6A, para la descarga de la energía que se almacena en el solenoide de la cerradura.

g) Alimentación del circuito. Se utilizará una fuente de 5V DC, dado que es el voltaje máximo que necesita el circuito para funcionar correctamente. Asimismo, con el objetivo de evitar cualquier inconveniente debido a que el sistema se detenga, por alguna falla energética, que impida a los docentes de la Institución Educativa ingresar al aula en un momento importante, se agregó una alimentación alternativa automática, de modo que, cuando la fuente de alimentación falle, inmediatamente entre en funcionamiento esta alimentación de respaldo, el cual consta de una batería 1 baterías de litio 18650 de 1800mAh.

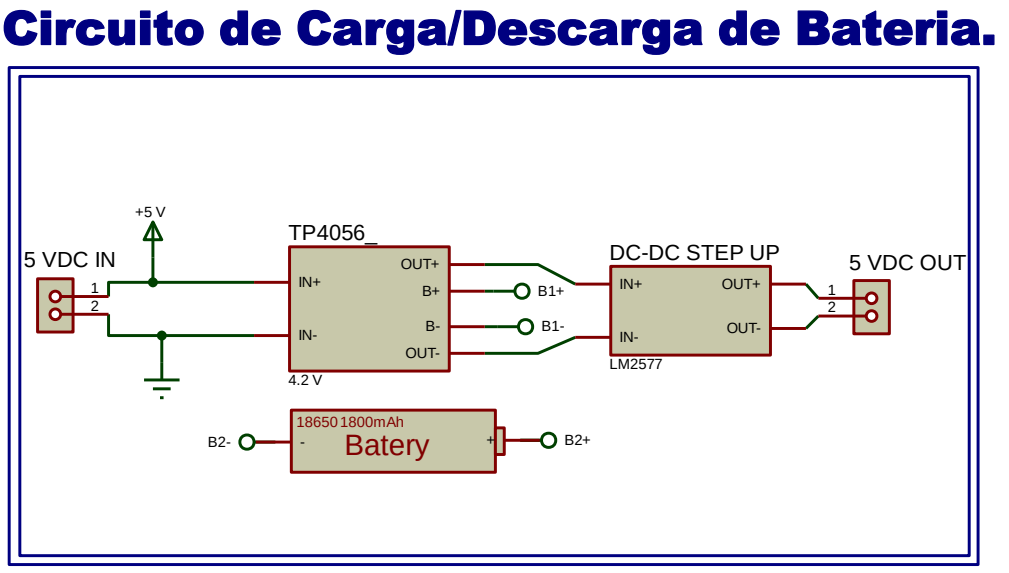


Figura 7. Circuito de respaldo de energía.

Fuente: propia

Como se aprecia en la Figura 6, este circuito se encuentra conectado a la alimentación principal de 5V DC conectados al TP4056 (400 mA consumo) encargado de mantener cargada la batería de litio 18650 (generando 4.2v); tiene una fuente elevadora de voltaje, que nos proporciona 5v de alimentación que va conectado al circuito de control. Finalmente, debemos recalcar que el módulo de carga de la batería permite hacer el cambio entre el uso de la fuente de 5v y el consumo de la carga de la batería, cuando la fuente sufra algún corte, además de que protege al circuito principal.

h) Fuente de Alimentación. La elección de la fuente de alimentación más adecuada, se realizó bajo el cálculo del consumo total que necesitara el circuito:

a. Para el circuito de carga: Ic = 0.4 A , Vc = 5v

$$Pc = 2W$$

b. Para el relé de activación: Ir = 0.07 A , Vr = 5v

$$Pr = 0.35\ W$$

c. Para el circuito de control o principal: Icp = 0.35 A , Vcp = 5v

$$Pcp = 1.75W$$

Con estos cálculos obtenemos un consumo máximo de

$$Pmax = Pc + Pr + Pcp = 4.1\ W.$$

Con el valor obtenido, podemos concluir que se necesita una fuente de alimentación de 5 VDC a 2 A, el cual nos otorga una potencia de 7W (reales), de la misma forma el circuito de alimentación de respaldo nos otorga una potencia de 5.17 Wh (reales), siendo suficiente para cubrir la demanda energética del sistema.

Para este circuito se ha elegido una fuente del tipo conmutada, que posee mejores características que una fuente lineal.

4.1.3 Software del sistema

Para el desarrollo del Software del sistema, se utilizó el programa MPLABX IDE V5.35, con el compilador XC8 V2.10; de esta manera, haciendo uso de la hoja de datos de cada uno de los componentes utilizados, se diseñó las librerías adecuadas para cada uno de estos, conteniendo las funciones utilizadas en el desarrollo del código del programa principal que se va a ejecutar.

4.1.4 Validación de los resultados

A continuación, se muestra el total de casos procesados, que representa los 25 docentes encuestados en la Institución Educativa 20786 – Vilcahuaura.

Tabla 1.

Casos procesados

Resumen de procesamiento de casos

		N	%
Casos	Válido	25	100,0
	Excluido[a]	0	,0
	Total	25	100,0

Mediante la aplicación del programa de análisis estadístico SPSS V26, se procede a hallar el nivel de confiabilidad mediante el valor del alfa de Cronbach, cuyo valor se muestra a continuación:

Tabla 2.

Valor de alfa de Cronbach

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
,916	15

Tabla 3

Sistema de Control de Acceso Biométrico

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	1	4,0	4,0	4,0
	Alto	24	96,0	96,0	100,0
	Total	25	100,0	100,0	

Se adjunta el siguiente grafico circular correspondiente a los datos obtenidos

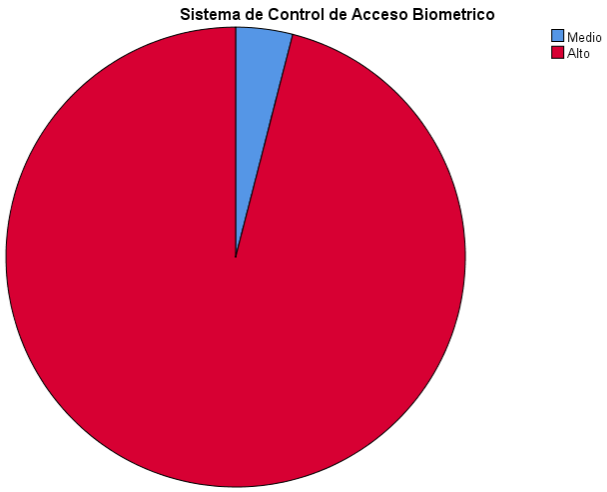


Figura 8. Gráfico dimensión sistema de control de acceso biométrico

Fuente: propia

De la tabla y gráfico, observamos que un 4% de docentes encuestados expresan un nivel medio en la variable Sistema de Control de Acceso Biométrico, y un 96% un nivel alto, en la institución educativa 20786 de Vilcahuaura.

Tabla 4

Sistema de Identificación

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	2	8,0	8,0	8,0
	Alto	23	92,0	92,0	100,0
	Total	25	100,0	100,0	

Se adjunta el siguiente grafico circular correspondiente a los datos obtenidos

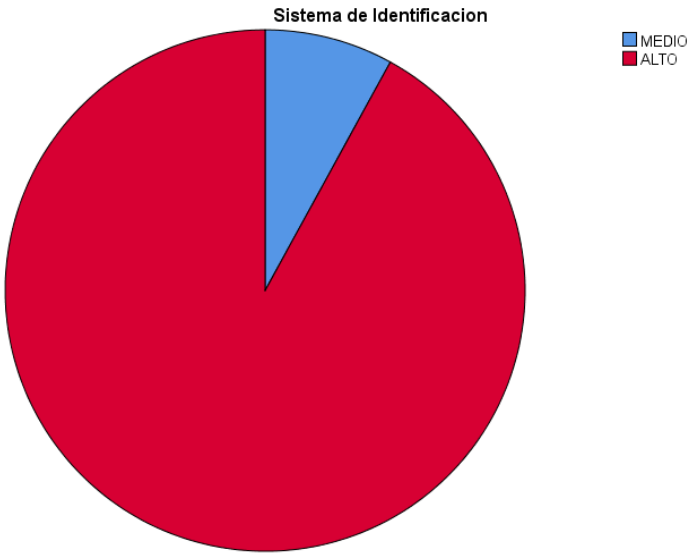


Figura 9. Gráfico dimensión sistema de identificación

Fuente: propia

De la tabla y gráfico, observamos que un 8% de docentes encuestados expresan un nivel medio en la dimensión Riesgos, y un 92% un nivel alto, en la institución educativa 20786 de Vilcahuaura.

Tabla 5

Característica Física

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Alto	25	100,0	100,0	100,0

Se adjunta el siguiente grafico circular correspondiente a los datos obtenidos

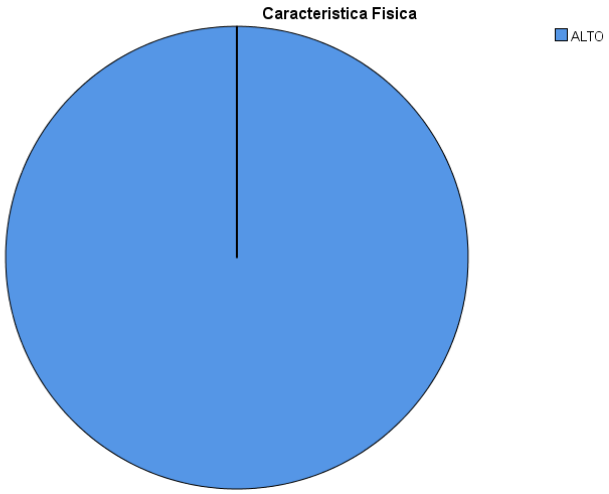


Figura 10. Gráfico dimensión característica física

Fuente: propia

De la tabla y gráfico, observamos que el 100% de docentes encuestados expresan un nivel alto en la dimensión Característica Física, en la institución educativa 20786 de Vilcahuaura.

Tabla 6

Registro y Autorización

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	4	16,0	16,0	16,0
	Alto	21	84,0	84,0	100,0
	Total	25	100,0	100,0	

Se adjunta el siguiente grafico circular correspondiente a los datos obtenidos

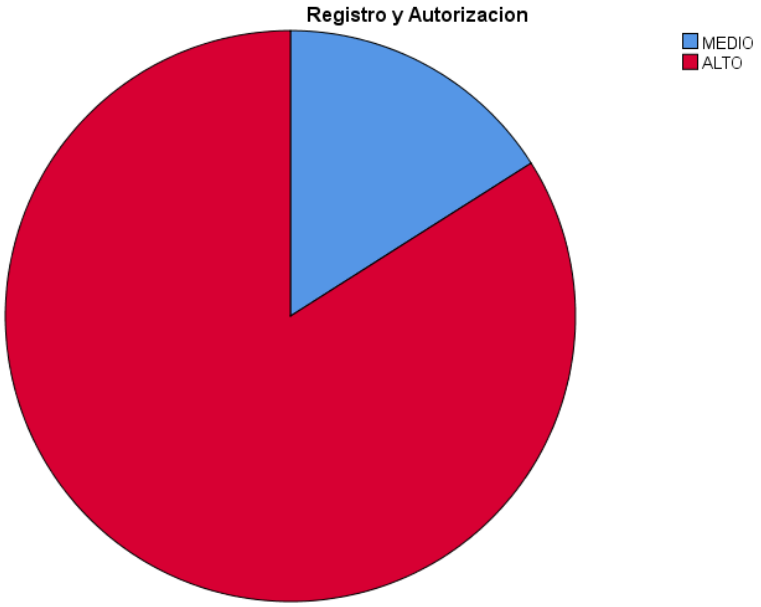


Figura 11. Gráfico dimensión registro y autorización

Fuente: propia

De la tabla y gráfico, observamos que un 16% de docentes encuestados expresan un nivel medio en la dimensión Registro y Autorización, y un 84% un nivel alto, en la institución educativa 20786 de Vilcahuaura.

Tabla 7

Seguridad Física

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	4	16,0	16,0	16,0
	Alto	21	84,0	84,0	100,0
	Total	25	100,0	100,0	

Se adjunta el siguiente grafico circular correspondiente a los datos obtenidos

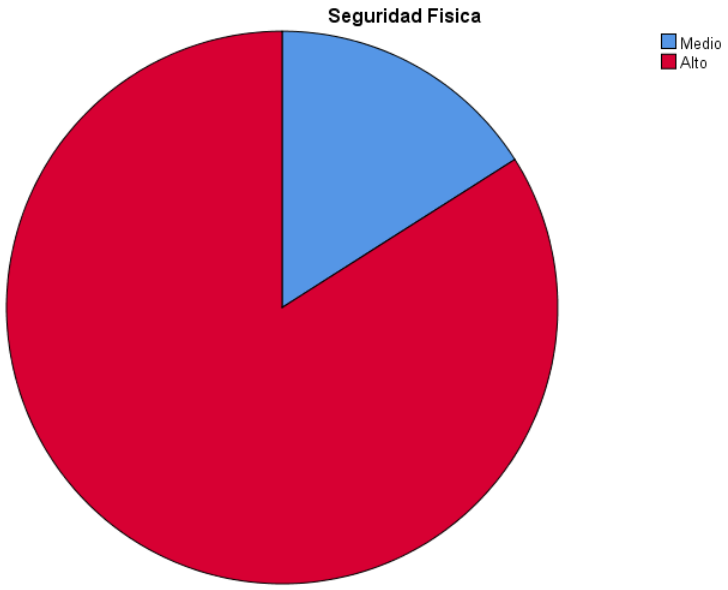


Figura 12. Gráfico dimensión seguridad física

Fuente: propia

De la tabla y gráfico, observamos que un 16% de docentes encuestados expresan un nivel medio en la variable Seguridad Física, y un 84% un nivel alto, en la institución educativa 20786 de Vilcahuaura.

Tabla 8

Mecanismo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	4	16,0	16,0	16,0
	Alto	21	84,0	84,0	100,0
	Total	25	100,0	100,0	

Se adjunta el siguiente grafico circular correspondiente a los datos obtenidos

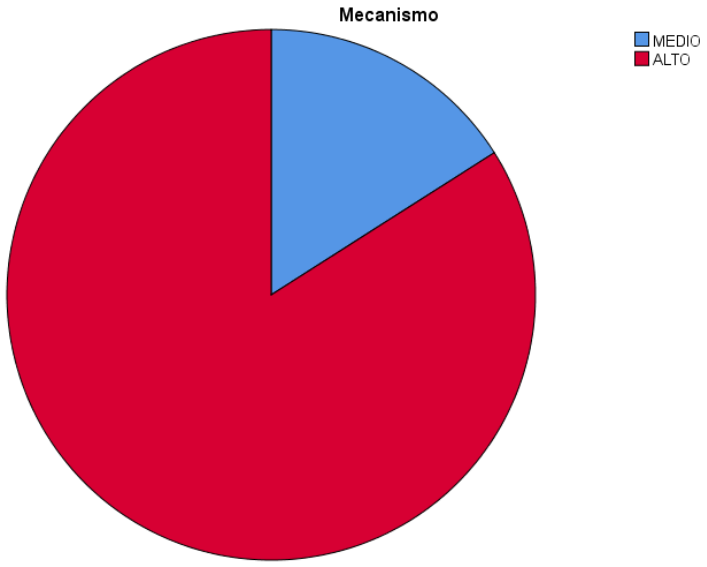


Figura 13. Gráfico dimensión mecanismo

Fuente: propia

De la tabla y gráfico, observamos que un 16% de docentes encuestados expresan un nivel medio en la dimensión Mecanismo, y un 84% un nivel alto, en la institución educativa 20786 de Vilcahuaura.

Tabla 9

Riesgos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	4	16,0	16,0	16,0
	Alto	21	84,0	84,0	100,0
	Total	25	100,0	100,0	

Se adjunta el siguiente grafico circular correspondiente a los datos obtenidos

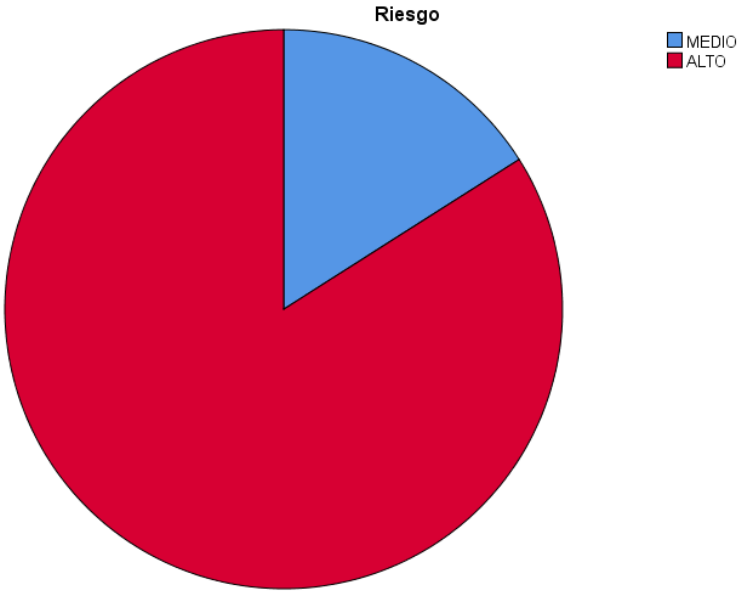


Figura 14. Gráfico dimensión riesgo

Fuente: propia

De la tabla y gráfico, observamos que un 16% de docentes encuestados expresan un nivel medio en la dimensión Riesgos, y un 84% un nivel alto, en la institución educativa 20786 de Vilcahuaura.

Tabla 10

Protección

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	4	16,0	16,0	16,0
	Alto	21	84,0	84,0	100,0
	Total	25	100,0	100,0	

Se adjunta el siguiente grafico circular correspondiente a los datos obtenidos

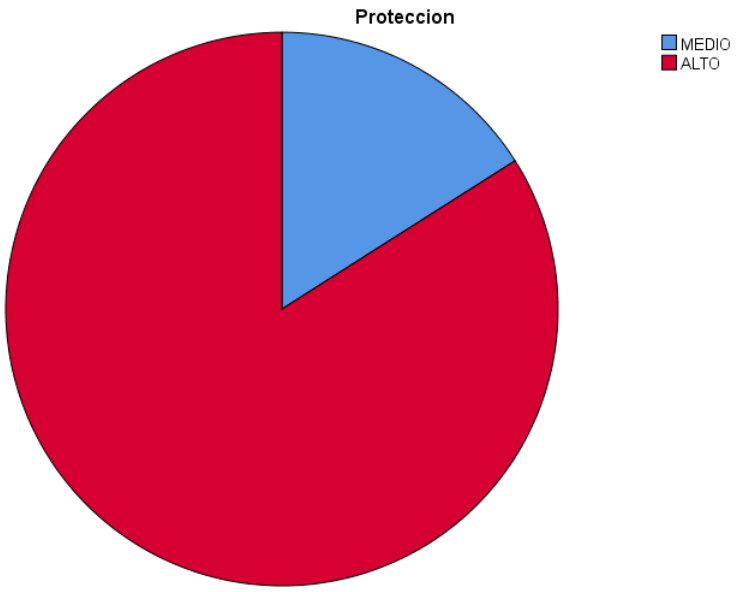


Figura 15. Gráfico dimensión protección

Fuente: propia

De la tabla y gráfico, observamos que un 16% de docentes encuestados expresan un nivel medio en la dimensión Protección, y un 84% un nivel alto, en la institución educativa 20786 de Vilcahuaura.

4.2 Contrastación de hipótesis

Aplicamos una prueba de normalidad a los datos para saber que saber que prueba de hipótesis emplearemos:

Tabla 11

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Sistema de control de acceso biométrico	,135	25	,200*	,932	25	,095
Seguridad física	,161	25	,096	,933	25	,102

Nota: como la población con la que trabajaremos es menor a 50 utilizaremos la prueba de Shapiro-Wilk. Observamos que la significancia es mayor a 0,05; por lo que tenemos datos normales y trabajaremos con la prueba de correlación de R de Pearson.

Hipótesis general

Hipótesis nula: El sistema de control de acceso biométrico no se relaciona con la seguridad física en la institución educativa 20786, Vilcahuaura 2022

Hipótesis Alternativa: El sistema de control de acceso biométrico se relaciona con la seguridad física en la institución educativa 20786, Vilcahuaura 2022

Tabla 12

Sistema de Control de Acceso Biométrico y la Seguridad Física.

		Sistema de Control de Acceso Biométrico	Seguridad Física
Sistema de Control de Acceso Biométrico	Correlación de Pearson	1	,754**
	Sig. (bilateral)		,000
	N	25	25
Seguridad Física	Correlación de Pearson	,754**	1
	Sig. (bilateral)	,000	
	N	25	25

**. La correlación es significativa en el nivel 0,01 (bilateral).

El valor del estadístico r de Pearson es de 0.754, a demás esta correlación es significativa. Por lo que se puede afirmar con un 99% de confianza, que en el ámbito de estudio hay una correlación positiva alta entre la

variable **sistemas de control de acceso biométrico** y la variable **seguridad física** porque el valor de Sig. (bilateral) es de 0.000, que se encuentra por debajo del 0.01 requerido. Por lo que se acepta la hipótesis alterna.

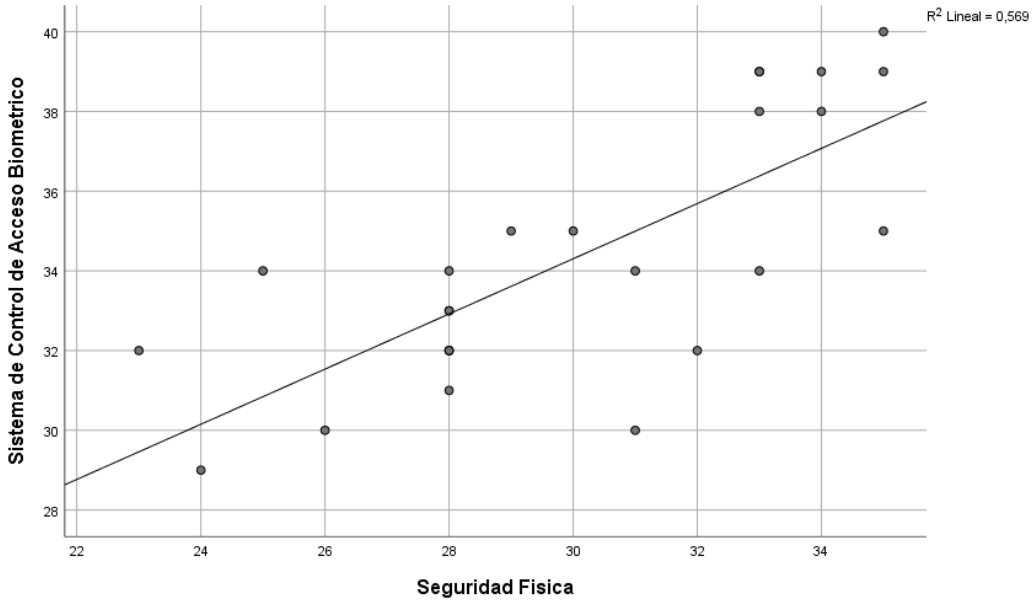


Figura 16*. El sistema de control de acceso biométrico y la seguridad física.*

Hipótesis específica 1:

Hipótesis Nula: El sistema de identificación no se relaciona con la seguridad física en la institución educativa 20786, Vilcahuaura 2022.

Hipótesis Alternativa: El sistema de identificación se relaciona con la seguridad física en la institución educativa 20786, Vilcahuaura 2022.

Tabla 13

Sistema de Identificación y la Seguridad Física.

		Sistema de Identificación	Seguridad Física
Sistema de Identificación	Correlación de Pearson	1	,623**
	Sig. (bilateral)		,001
	N	25	25
Seguridad Física	Correlación de Pearson	,623**	1
	Sig. (bilateral)	,001	
	N	25	25

**. La correlación es significativa en el nivel 0,01 (bilateral).

El valor del estadístico r de Pearson es de 0.623, además esta correlación es significativa. Por lo que se puede afirmar con un 99% de confianza, que en el ámbito de estudio hay una correlación positiva moderada entre la dimensión **sistemas de identificación** y la variable **seguridad física** porque el valor de Sig. (bilateral) es de 0.001, que se encuentra por debajo del 0.01 requerido. Por lo que se acepta la hipótesis alterna.

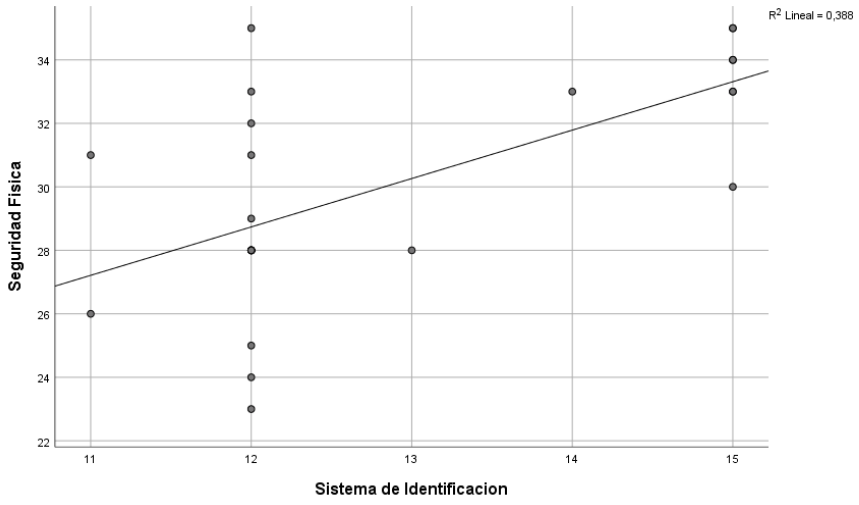


Figura 17. *El sistema de identificación y la seguridad física.*

Hipótesis especifica 2:

Ho: Las características físicas no se relacionan con la seguridad física en la institución educativa 20786, Vilcahuaura 2022

Ha: Las características físicas se relacionan con la seguridad física en la institución educativa 20786, Vilcahuaura 2022

Tabla 14

La Característica Física y la Seguridad Física.

		Característica Física	Seguridad Física
Característica Física	Correlación de Pearson	1	,661**
	Sig. (bilateral)		,000
	N	25	25
Seguridad Física	Correlación de Pearson	,661**	1
	Sig. (bilateral)	,000	
	N	25	25

**. La correlación es significativa en el nivel 0,01 (bilateral).

El valor del estadístico r de Pearson es de 0.661, además esta correlación es significativa. Por lo que se puede afirmar con un 99% de confianza, que en el ámbito de estudio hay una correlación positiva moderada entre la dimensión **características físicas** y la variable **seguridad física** porque el valor de Sig. (bilateral) es de 0.000, que se encuentra por debajo del 0.01 requerido. Por lo que se acepta la hipótesis alterna.

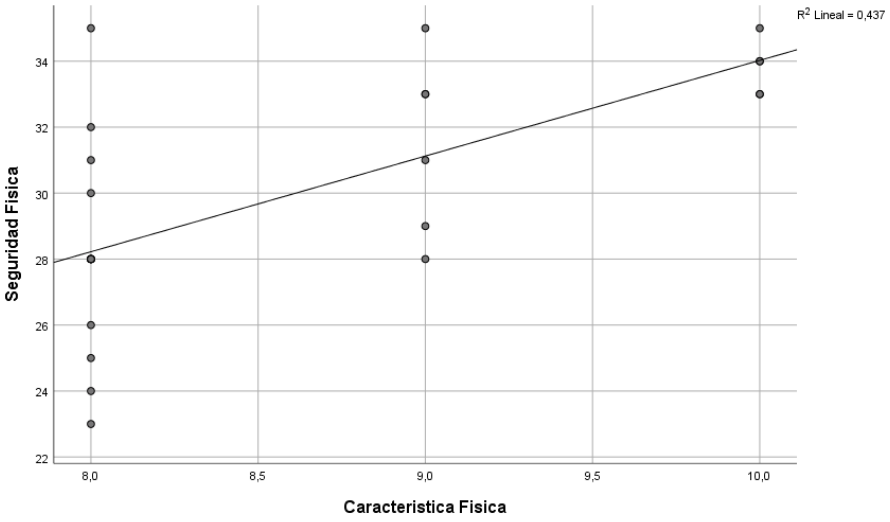


Figura 18. *La característica física y la seguridad física.*

Hipótesis Especifica 3:

Hipótesis Nula: El registro y autorización no se relaciona con la seguridad física en la institución educativa 20786, Vilcahuaura 2022

Hipótesis Alternativa: El registró y autorización se relaciona con la seguridad física en la institución educativa 20786, Vilcahuaura 2022

Tabla 15

El registro y Autorización y la Seguridad Física.

		Registro y Autorización	Seguridad Física
Registro y Autorización	Correlación de Pearson	1	,650**
	Sig. (bilateral)		,000
	N	25	25
Seguridad Física	Correlación de Pearson	,650**	1
	Sig. (bilateral)	,000	
	N	25	25

**. La correlación es significativa en el nivel 0,01 (bilateral).

El valor del estadístico r de Pearson es de 0.650, a demás esta correlación es significativa. Por lo que se puede afirmar con un 99% de confianza, que en el ámbito de estudio hay una correlación positiva moderada entre la dimensión **registro de autenticación** y la variable **seguridad física** porque el valor de Sig. (bilateral) es de 0.000, que se encuentra por debajo del 0.01 requerido. Por lo que se acepta la hipótesis alterna.

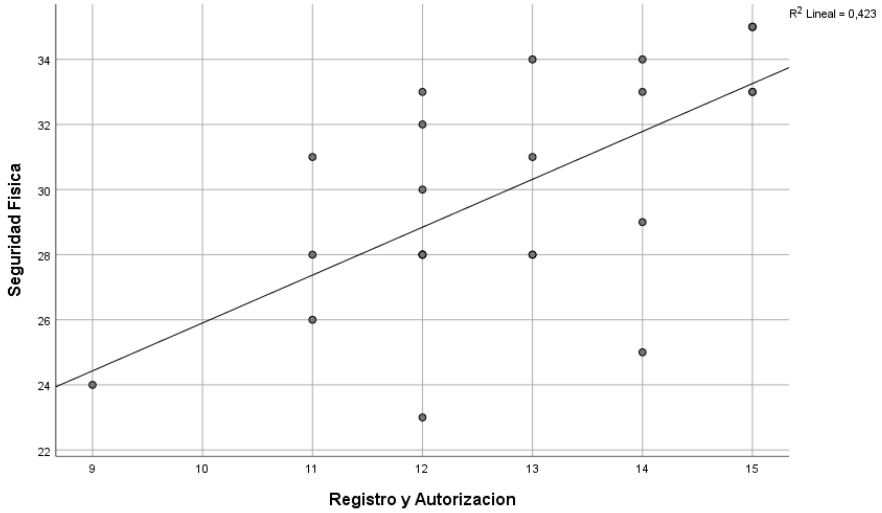


Figura 19. *El registro y autorización y la seguridad física.*

CAPÍTULO V: DISCUSIÓN

5.1 Discusión de los resultados

Según los resultados estadísticos que se obtuvieron se puede sustentar que existe una relación entre el sistema de acceso biométrico y la seguridad fisca de la institución educativa 20786 Vilcahuaura, basado en la correlación de Pearson que nos da un valor de 0,754, afirmándonos una buena correlación entre las variables.

También se analizaron las dimensiones de la variable uno contrastándolas con la variable dos, de esta manera mediante análisis estadísticos logramos corroborar la relación existente. Teniendo como primera dimensión sometida a prueba la de sistema de identificación y la seguridad física en la institución educativa 20786 de Vilcahuaura. Logrando obtener un resultado positivo ya que la prueba de correlación de Pearson arrojo que con un 0,623 existe relación entre la dimensión y la variable.

Según el resultado de nuestra segunda dimensión nos dice que existe una relación entre las características físicas y la seguridad física en la institución educativa 20786 de Vilcahuaura, ya que obtuvimos un valor de 0,661 con la prueba de correlación de Pearson, aceptando así nuestra hipótesis alterna.

Para nuestra tercera dimensión pudimos demostrar que existe relación entre registro y autenticación y la seguridad física en la institución educativa 20786 de Vilcahuaura, ya que la prueba de correlación de Pearson nos dio un resultado de 0,650 representando una buena correlación.

Con los resultados obtenidos podemos coincidir con la investigación de Guerra, J. (2021), titulada "*Aplicación de reconocimiento biométrico por huella dactilar y su influencia en la seguridad lógica en SEDAPAL"* el cual tuvo como objetivo determinar de qué manera influye la aplicación de reconocimiento biométrico por huella dactilar

en el control de acceso en SEDAPAL (p.25) y concluyo que: “La aplicación de reconocimiento biométrico por huella dactilar si influye en la seguridad lógica en SEDAPAL (…)” (p.139). En el aspecto que, existe una relación significativa entre el sistema de reconocimiento biométrico dactilar y el campo de la seguridad.

Así mismo coincidimos con la investigación de San Martin Guillen (2019), titulada “*Diseño e implementación de un sistema de control de acceso por biometría”* el cual tuvo como objetivo el diseñar e implementar un sistema de control de acceso por medio de características biométricas (p.3) y tienen como conclusión:

> “se logró cumplir el objetivo ya que se diseñó e implemento un sistema de control de acceso que, a través del análisis de las características biométricas de los usuarios, mejora la seguridad del taller, aceptando el ingreso únicamente del personal inscrito en la base de datos” (P.47).

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Del estudio realizado podemos concluir:

1°. Conclusión: Existe una relación entre el sistema de control de acceso biométrico y la seguridad física en la institución educativa 20786, Vilcahuaura, basándonos en los resultados obtenidos mediante la prueba de correlación de Pearson que arrojo un valor de 0.754.

2°. Conclusión: Existe una relación entre el sistema de identificación y la seguridad física en la institución educativa 20786, Vilcahuaura, basándonos en los resultados obtenidos mediante la prueba de correlación de Pearson que arrojo un valor de 0.623.

3°. Conclusión: Existe una relación entre la característica física y la seguridad física en la institución educativa 20786, Vilcahuaura, basándonos en los resultados obtenidos mediante la prueba de correlación de Pearson que arrojo un valor de 0.661.

4°. Conclusión: Existe una relación entre el registro y autorización, y la seguridad física en la institución educativa 20786, Vilcahuaura, basándonos en los resultados obtenidos mediante la prueba de correlación de Pearson que arrojo un valor de 0.650.

6.2 Recomendaciones

- Dar mantenimiento preventivo al sistema periódicamente, para detectar a tiempo cualquier tipo de falla que pueda ocurrir y darle solución.
- El dispositivo debe ubicarse en un lugar adecuado, de fácil acceso, y sin estar expuesto a temperaturas ambientales altas.
- Al tratarse de un sensor óptico, se recomienda cubrir totalmente la lente del sensor al momento de registrar la huella, ya sea para agregar un usuario nuevo o intentar ingresar al ambiente.
- Es recomendable tener un sistema de respaldo energético para asegurar completamente el funcionamiento del sistema de acceso, evitando el acceso a usuarios no autorizados.
- Brindar capacitación adecuada a los usuarios, sobre el uso de esta herramienta, tanto para el registro correcto de los usuarios, las configuraciones y las precauciones a tener en cuenta, para el correcto funcionamiento del dispositivo.
- Para reforzar la seguridad de acceso al ambiente, se puede optar por usar chapas eléctricas más sofisticadas, que sean mucho más resistentes, así como, usar puertas de un material más resistente.
- Ampliar la investigación, enfocado en mejorar este sistema de control de acceso, ya sea aumentando las funcionalidades que pueda ofrecer, así como, agregar un sistema de protección de respaldo, en caso de un mal funcionamiento por fallas electrónicas o alguna vulneración forzada del dispositivo.

REFERENCIAS

7.1 Referencias bibliográficas

Arteaga, J. (2018). Implementación de un control de acceso utilizando sistema biométrico para el laboratorio de electrónica y robótica de la Universidad Estatal del Sur de Manabí.

Ccamerccoa, V. (2020). Implementación de un sistema automatizado para gestionar la seguridad de accesos en viviendas juliaqueñas mediante aplicativo móvil e internet de las cosas.

Córdova, I. (2017). El proyecto de investigación cuantitativa. San Marcos.

Menéndez, V., y Cabrera, J. (2019). Propuesta para el diseño de un sistema de validación y autentificación.

Ñaupas, H., Elías, M., Novoa, E., y Alberto, V. (2014). Metodología de la Investigación. Cuantitativa. Ediciones de la U.

Pampa, J., y Lozano, Á. (2020). La tecnología de seguridad física y el sistema de seguridad en la escuela militar de Chorrillos "Coronel Francisco Bolognesi", 2020.

Pérez, H. (2018). Sistema de control de acceso por reconocimiento de iris para el ingreso de personal a la Empresa Electroservicios Querubín de la ciudad de Puyo.

7.2 Referencias electrónicas

Cadillo, J. (2018). Modelo de sistema biométrico de interfaz híbrida para cerraduras de Seguridad Electrónicas. Obtenido de http://repositorio.unsa.edu.pe/handle/UNSA/6635

Fernández, G. (2017). Sistema de control de acceso basado en la tecnología de autenticación. Obtenido de https://repositorio.umsa.bo/handle/123456789/13398

Guerra, G., y Jiménez, R. (2021). Aplicación de reconocimiento biométrico por huella dactilar y su Influencia en la Seguridad Lógica de SEDAPAL, 2020. Obtenido de https://repositorio.ucv.edu.pe/handle/20.500.12692/66536.

Montaña, D. (2017). Sistema de identificación mediante huella digital para el control de accesos a La Universidad Libre sede Bosque Popular simulado en entorno web. Obtenido de https://repository.unilibre.edu.co/handle/10901/10557

San Martin, E. (2019). Diseño e implementación de un sistema de un sistema de control de acceso por biometría. Obtenido de https://repositorio.utp.edu.pe/handle/20.500.12867/2648

Sotelo, A. (2020). Diseño de un prototipo de control de acceso basado en tecnología biométrica de huella dactilar, lector de barras y RFID. Obtenido de https://repositorio.utp.edu.pe/handle/20.500.12867/3796

Vallejo, P., y Carrera, A. (2017). Implementación de un sistema biométrico de huellas dactilares para el control de asistencia estudiantil en la Escuela de Ingeniería Industrial de la Facultad de Mecánica. Obtenido de http://dspace.espoch.edu.ec/handle/123456789/6834

ANEXOS

VALIDACIÓN DEL CUESTIONARIO

Estimado ingeniero se le presenta a continuación los indicadores para la evaluación de cada Ítem del cuestionario que se le hizo entrega en formato PDF. Antes de iniciar con la evaluación por favor llenar sus datos personales. A continuación, marque con una (x) su respuesta en los recuadros valorados del 1 al 5.

Nombres y apellidos: Ing. Oscar Miguel De La Cruz
Profesión: Ingeniero Electrónico
Código CIP: 85598

CONTENIDO		EVALUACIÓN				
Ítem	**Criterio**	**1**	**2**	**3**	**4**	**5**
1	Coherencia				**X**	
	Claridad				**X**	
	Escala				**X**	
	Relevancia				**X**	
2	Coherencia					**X**
	Claridad				**X**	
	Escala			**X**		
	Relevancia				**X**	
3	Coherencia					
	Claridad				**X**	**X**
	Escala				**X**	
	Relevancia			**X**		
4	Coherencia				**X**	
	Claridad			**X**		
	Escala			**X**		
	Relevancia				**X**	
5	Coherencia			**X**		
	Claridad				**X**	
	Escala			**X**		
	Relevancia				**X**	
6	Coherencia			**X**		
	Claridad				**X**	
	Escala					**X**
	Relevancia				**X**	
7	Coherencia				**X**	
	Claridad				**X**	
	Escala					**X**
	Relevancia			**X**		
8	Coherencia				**X**	
	Claridad				**X**	
	Escala				**X**	
	Relevancia				**X**	
9	Coherencia				**X**	
	Claridad			**X**		
	Escala					**X**
	Relevancia				**X**	
10	Coherencia				**X**	
	Claridad				**X**	

	Escala				X	
	Relevancia				X	
11	Coherencia				X	
	Claridad				X	
	Escala				X	
	Relevancia				X	
12	Coherencia			X		
	Claridad			X		
	Escala				X	
	Relevancia				X	
13	Coherencia				X	
	Claridad				X	
	Escala					X
	Relevancia			X		
14	Coherencia				X	
	Claridad				X	
	Escala				X	
	Relevancia				X	
15	Coherencia				X	
	Claridad				X	
	Escala			X		
	Relevancia					X

OBSERVACIONES:

VALIDACIÓN DEL CUESTIONARIO

Estimado ingeniero se le presenta a continuación los indicadores para la evaluación de cada Ítem del cuestionario que se le hizo entrega en formato PDF. Antes de iniciar con la evaluación por favor llenar sus datos personales. A continuación, marque con una (x) su respuesta en los recuadros valorados del 1 al 5.

Nombres y apellidos: Ing. Franco Jhordy Mirando Portella
Profesión: Ingeniero Electrónico
Código CIP: 234743

CONTENIDO		EVALUACIÓN				
Ítem	**Criterio**	**1**	**2**	**3**	**4**	**5**
1	Coherencia					**X**
	Claridad					**X**
	Escala					**X**
	Relevancia					**X**
2	Coherencia					**X**
	Claridad					**X**
	Escala					**X**
	Relevancia				**X**	
3	Coherencia					**X**
	Claridad					**X**
	Escala					**X**
	Relevancia					**X**
4	Coherencia					**X**
	Claridad					**X**
	Escala					**X**
	Relevancia					**X**
5	Coherencia					**X**
	Claridad					**X**
	Escala					**X**
	Relevancia					**X**
6	Coherencia					**X**
	Claridad				**X**	
	Escala					**X**
	Relevancia					**X**
7	Coherencia					**X**
	Claridad					**X**
	Escala					**X**
	Relevancia					**X**
8	Coherencia					**X**
	Claridad					**X**
	Escala					**X**
	Relevancia					**X**
9	Coherencia					**X**
	Claridad					**X**
	Escala					**X**
	Relevancia					**X**
10	Coherencia					**X**
	Claridad					**X**

	Escala					**X**
	Relevancia					**X**
11	Coherencia					**X**
	Claridad					**X**
	Escala					**X**
	Relevancia				**X**	
12	Coherencia					**X**
	Claridad					**X**
	Escala					**X**
	Relevancia					**X**
13	Coherencia					**X**
	Claridad					**X**
	Escala					**X**
	Relevancia					**X**
14	Coherencia					**X**
	Claridad					**X**
	Escala					**X**
	Relevancia					**X**
15	Coherencia					**X**
	Claridad				**X**	
	Escala					**X**
	Relevancia					**X**

OBSERVACIONES:

VALIDACIÓN DEL CUESTIONARIO

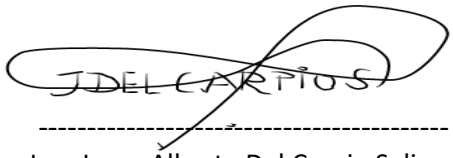
Estimado ingeniero se le presenta a continuación los indicadores para la evaluación de cada Ítem del cuestionario que se le hizo entrega en formato PDF. Antes de iniciar con la evaluación por favor llenar sus datos personales. A continuación, marque con una (x) su respuesta en los recuadros valorados del 1 al 5.

Nombres y apellidos: Ing. Del Carpio Salinas Jorge Alberto
Profesión: Ingeniero Electrónico
Código CIP: 25498

CONTENIDO		EVALUACIÓN				
Ítem	**Criterio**	**1**	**2**	**3**	**4**	**5**
1	Coherencia					**X**
	Claridad					**X**
	Escala				**X**	
	Relevancia				**X**	
2	Coherencia					**X**
	Claridad				**X**	
	Escala				**X**	
	Relevancia				**X**	
3	Coherencia				**X**	
	Claridad					**X**
	Escala				**X**	
	Relevancia				**X**	
4	Coherencia				**X**	
	Claridad					**X**
	Escala					**X**
	Relevancia				**X**	
5	Coherencia				**X**	
	Claridad				**X**	
	Escala					**X**
	Relevancia					**X**
6	Coherencia					**X**
	Claridad				**X**	
	Escala					**X**
	Relevancia				**X**	
7	Coherencia				**X**	
	Claridad				**X**	
	Escala					**X**
	Relevancia					**X**
8	Coherencia				**X**	
	Claridad				**X**	
	Escala				**X**	
	Relevancia				**X**	
9	Coherencia				**X**	
	Claridad					**X**
	Escala					**X**
	Relevancia				**X**	
10	Coherencia					**X**
	Claridad					**X**

	Escala					**X**
	Relevancia				**X**	
11	Coherencia				**X**	
	Claridad				**X**	
	Escala					**X**
	Relevancia					**X**
12	Coherencia				**X**	
	Claridad					**X**
	Escala					**X**
	Relevancia				**X**	
13	Coherencia				**X**	
	Claridad					**X**
	Escala					**X**
	Relevancia			**X**		
14	Coherencia					**X**
	Claridad					**X**
	Escala				**X**	
	Relevancia				**X**	
15	Coherencia					**X**
	Claridad					**X**
	Escala				**X**	
	Relevancia					**X**

OBSERVACIONES:



Ing. Jorge Alberto Del Carpio Salinas

VALIDACIÓN DEL CUESTIONARIO

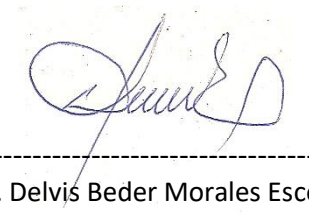
Estimado ingeniero se le presenta a continuación los indicadores para la evaluación de cada Ítem del cuestionario que se le hizo entrega en formato PDF. Antes de iniciar con la evaluación por favor llenar sus datos personales. A continuación, marque con una (x) su respuesta en los recuadros valorados del 1 al 5.

Nombres y apellidos: Ing. Delvis Beder Morales Escobar
Profesión: Ingeniero Electrónico
Código CIP: 107525

CONTENIDO		EVALUACIÓN				
Ítem	**Criterio**	**1**	**2**	**3**	**4**	**5**
1	Coherencia			X		
	Claridad					X
	Escala					X
	Relevancia				X	
2	Coherencia					X
	Claridad					X
	Escala				X	
	Relevancia					X
3	Coherencia				X	
	Claridad					X
	Escala				X	
	Relevancia				X	
4	Coherencia				X	
	Claridad					X
	Escala					X
	Relevancia				X	
5	Coherencia				X	
	Claridad				X	
	Escala				X	
	Relevancia					X
6	Coherencia				X	
	Claridad				X	
	Escala					X
	Relevancia				X	
7	Coherencia					X
	Claridad				X	
	Escala					X
	Relevancia					X
8	Coherencia					X
	Claridad					X
	Escala				X	
	Relevancia				X	
9	Coherencia				X	
	Claridad				X	
	Escala			X		
	Relevancia				X	
10	Coherencia				X	
	Claridad				X	

	Escala				X	
	Relevancia				X	
11	Coherencia					X
	Claridad				X	
	Escala					X
	Relevancia				X	
12	Coherencia				X	
	Claridad					X
	Escala				X	
	Relevancia			X		
13	Coherencia				X	
	Claridad					X
	Escala					X
	Relevancia					X
14	Coherencia					X
	Claridad					X
	Escala					X
	Relevancia				X	
15	Coherencia					X
	Claridad				X	
	Escala				X	
	Relevancia					X
	Relevancia					X

OBSERVACIONES:



Ing. Delvis Beder Morales Escobar

VALIDACIÓN DEL CUESTIONARIO

Estimado ingeniero se le presenta a continuación los indicadores para la evaluación de cada Ítem del cuestionario que se le hizo entrega en formato PDF. Antes de iniciar con la evaluación por favor llenar sus datos personales. A continuación, marque con una (x) su respuesta en los recuadros valorados del 1 al 5.

Nombres y apellidos: Ing. Ernesto Díaz Ronceros
Profesión: Ingeniero Electrónico
Código CIP: 197965

CONTENIDO		EVALUACIÓN				
Ítem	**Criterio**	**1**	**2**	**3**	**4**	**5**
1	Coherencia					X
	Claridad					X
	Escala					X
	Relevancia				X	
2	Coherencia					X
	Claridad					X
	Escala					X
	Relevancia					X
3	Coherencia				X	
	Claridad				X	
	Escala			X		
	Relevancia				X	
4	Coherencia					X
	Claridad					X
	Escala				X	
	Relevancia				X	
5	Coherencia				X	
	Claridad					X
	Escala				X	
	Relevancia					X
6	Coherencia					X
	Claridad					X
	Escala				X	
	Relevancia					X
7	Coherencia					X
	Claridad				X	
	Escala					X
	Relevancia					X
8	Coherencia					X
	Claridad					X
	Escala					X
	Relevancia					X
9	Coherencia					X
	Claridad					X
	Escala					X
	Relevancia					X
10	Coherencia					X
	Claridad					X

	Escala					X
	Relevancia					X
11	Coherencia					X
	Claridad				X	
	Escala					X
	Relevancia					X
12	Coherencia					X
	Claridad					X
	Escala					X
	Relevancia				X	
13	Coherencia					X
	Claridad					X
	Escala					X
	Relevancia					X
14	Coherencia					X
	Claridad					X
	Escala					X
	Relevancia					X
15	Coherencia					X
	Claridad					X
	Escala					X
	Relevancia				X	

OBSERVACIONES:

Tabla16.

Resultados del proceso de validación de jueces

Ítem	Jueces					Sx1	Mx	CVCi	Pei	CVCtc
	1	2	3	4	5					
Ítem 1	16	19	20	18	17	90	4.5	0.9	0.00032	0.89968
Ítem 2	16	20	19	17	19	91	4.55	0.91	0.00032	0.90968
Ítem 3	16	15	20	17	17	85	4.25	0.85	0.00032	0.84968
Ítem 4	14	18	20	18	18	88	4.4	0.88	0.00032	0.87968
Ítem 5	14	18	20	18	17	87	4.35	0.87	0.00032	0.86968
Ítem 6	16	19	19	18	17	89	4.45	0.89	0.00032	0.88968
Ítem 7	16	19	20	18	19	92	4.6	0.92	0.00032	0.91968
Ítem 8	16	20	20	16	18	90	4.5	0.9	0.00032	0.89968
Ítem 9	16	20	20	18	15	89	4.45	0.89	0.00032	0.88968
Ítem 10	16	20	20	19	16	91	4.55	0.91	0.00032	0.90968
Ítem 11	16	19	19	18	18	90	4.5	0.9	0.00032	0.89968
Ítem 12	14	19	20	18	16	87	4.35	0.87	0.00032	0.86968
Ítem 13	16	20	20	17	19	92	4.6	0.92	0.00032	0.91968
Ítem 14	16	20	20	18	19	93	4.65	0.93	0.00032	0.92968
Ítem 15	16	19	19	19	18	91	4.55	0.91	0.00032	0.90968
Promedio CVCtc										0.90013

Autoría propia

El promedio de los coeficientes de validez de contenido es 0.90013 lo que significa una validez y concordancia excelentes.

ANEXO 2: Confiabilidad del Instrumento

CONFIABILIDAD

FORMULACIÓN:

El alfa de Cronbach es siempre la relación promedio entre las variables (o elementos) que pertenecen al tamaño. Se pueden calcular de dos maneras: contraste o asociación con factores. Cabe señalar que las dos fórmulas son versiones de esto y el otro se puede deducir.

A partir de las varianzas, el alfa de Cronbach se calcula así:

$$\alpha = \left[\frac{K}{K-1}\right]\left[1 - \frac{\sum_{i=0}^{K} {S_i}^2}{{S_i}^2}\right]$$

Donde:

- ✓ ${S_i}^2$, es la varianza del ítem i,
- ✓ ${S_i}^2$, es la varianza de la suma de todos los ítems y
- ✓ K es el número de preguntas o ítems.

Es así que, a partir de las correlaciones entre los ítems, el alfa de Cronbach se calcula así:

$$\alpha = \frac{np}{1 + p(n-1)}$$

Donde:

- ✓ n, es el número de ítems y
- ✓ p, es el promedio de las correlaciones lineales entre cada uno de los ítems.

Entonces, aplicando a los ítems de la encuesta realizada:

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,916	15

ANEXO N°3

ENCUESTA PARA MEDIR LAS VARIABLES SISTEMA DE ACCESO BIOMÉTRICO Y LA SEGURIDAD FISICA

UNIVERSIDAD NACIONAL JOSE FAUSTINO SANCHEZ CARRION

Cuestionario para conocer el *Diseño De Un Sistema De Control De Acceso Biométrico y La Seguridad Física De La Institución Educativa 20786, Vilcahuaura 2022*

Saludos estimado docente, esperamos su cordial colaboración en el desarrollo del presente cuestionario, se agradece su honestidad, responsabilidad y no dejar alguna pregunta sin contestar.

Instrucciones: Lea cuidadosamente cada enunciado y marque con un aspa (x) el recuadro con la escala que considere adecuada, solo se admite una respuesta por enunciado.

Escala valorativa

Totalmente de acuerdo	De acuerdo	Neutral	En desacuerdo	Totalmente en desacuerdo
5	4	3	2	1

Cada enunciado responde a la pregunta **¿Está de acuerdo con…?**

Sistema de Control de Acceso Biométrico (X)						
Nº	**ITEMS**	**T.D.A**	**D.A**	**N.**	**E.D**	**T.E.D**
01	El sistema de identificación de usuario, tipo biométrico para la seguridad de los recursos de la institución.					
02	El nivel de confiabilidad en seguridad que ofrece el control de acceso del tipo biométrico.					
03	El costo que implica instalar un sistema de control de acceso biométrico.					
04	El sistema reconozca solo un rasgo único de la persona, como la huella dactilar.					
05	La facilidad de detección de la huella dactilar.					

06	Restringir la cantidad de usuarios permitidos para tener acceso al espacio de los equipos electrónicos					
07	Tiempo medio de respuesta del sistema de acceso biométrico					
08	El sistema debe ser automatizado.					
Seguridad Física (Y)						
09	Con el tipo de mecanismo de acceso planteado para la protección de los equipos electrónicos.					
10	El mecanismo de acceso planteado es fiable.					
11	El mecanismo de acceso planteado resulta sencillo de utilizar.					
12	El sistema planteado disminuirá el nivel de riesgo de hurtos a los que se encuentran expuestos los recursos importantes de la institución.					
13	El sistema planteado disminuirá el nivel de vulnerabilidad de los recursos importantes de la institución.					
14	El sistema planteado aumentaría el nivel de seguridad hacia los ambientes de la institución.					
15	La técnica planteada para resguardar efectivamente los recursos de la institución.					

10.0 ADDRESSABLE UNIVERSAL SYNCHRONOUS ASYNCHRONOUS RECEIVER TRANSMITTER (USART)

The Universal Synchronous Asynchronous Receiver Transmitter (USART) module is one of the two serial I/O modules. (USART is also known as a Serial Communications Interface or SCI.) The USART can be configured as a full-duplex asynchronous system that can communicate with peripheral devices, such as CRT terminals and personal computers, or it can be configured as a half-duplex synchronous system that can communicate with peripheral devices, such as A/D or D/A integrated circuits, serial EEPROMs, etc.

The USART can be configured in the following modes:

- Asynchronous (full-duplex)
- Synchronous – Master (half-duplex)
- Synchronous – Slave (half-duplex)

Bit SPEN (RCSTA<7>) and bits TRISC<7:6> have to be set in order to configure pins RC6/TX/CK and RC7/RX/DT as the Universal Synchronous Asynchronous Receiver Transmitter.

The USART module also has a multi-processor communication capability using 9-bit address detection.

REGISTER 10-1: TXSTA: TRANSMIT STATUS AND CONTROL REGISTER (ADDRESS 98h)

R/W-0	R/W-0	R/W-0	R/W-0	U-0	R/W-0	R-1	R/W-0
CSRC	TX9	TXEN	SYNC	—	BRGH	TRMT	TX9D
bit 7							bit 0

bit 7 **CSRC:** Clock Source Select bit
Asynchronous mode:
Don't care.
Synchronous mode:
1 = Master mode (clock generated internally from BRG)
0 = Slave mode (clock from external source)

bit 6 **TX9**: 9-bit Transmit Enable bit
1 = Selects 9-bit transmission
0 = Selects 8-bit transmission

bit 5 **TXEN**: Transmit Enable bit
1 = Transmit enabled
0 = Transmit disabled
Note: SREN/CREN overrides TXEN in Sync mode.

bit 4 **SYNC**: USART Mode Select bit
1 = Synchronous mode
0 = Asynchronous mode

bit 3 **Unimplemented:** Read as '0'

bit 2 **BRGH**: High Baud Rate Select bit
Asynchronous mode:
1 = High speed
0 = Low speed
Synchronous mode:
Unused in this mode.

bit 1 **TRMT**: Transmit Shift Register Status bit
1 = TSR empty
0 = TSR full

bit 0 **TX9D:** 9th bit of Transmit Data, can be Parity bit

Legend:			
R = Readable bit	W = Writable bit	U = Unimplemented bit, read as '0'	
- n = Value at POR	'1' = Bit is set	'0' = Bit is cleared	x = Bit is unknown

ANEXO 5: Pantalla LCD 16X2

HD44780U (LCD-II)

(Dot Matrix Liquid Crystal Display Controller/Driver)

HITACHI

Description

The HD44780U dot-matrix liquid crystal display controller and driver LSI displays alphanumerics, Japanese kana characters, and symbols. It can be configured to drive a dot-matrix liquid crystal display under the control of a 4- or 8-bit microprocessor. Since all the functions such as display RAM, character generator, and liquid crystal driver, required for driving a dot-matrix liquid crystal display are internally provided on one chip, a minimal system can be interfaced with this controller/driver.

A single HD44780U can display up to one 8-character line or two 8-character lines.

The HD44780U has pin function compatibility with the HD44780S which allows the user to easily replace an LCD-II with an HD44780U. The HD44780U character generator ROM is extended to generate 208 5 × 8 dot character fonts and 32 5 × 10 dot character fonts for a total of 240 different character fonts.

The low power supply (2.7V to 5.5V) of the HD44780U is suitable for any portable battery-driven product requiring low power dissipation.

Features

- 5 × 8 and 5 × 10 dot matrix possible
- Low power operation support:
  — 2.7 to 5.5V
- Wide range of liquid crystal display driver power
  — 3.0 to 11V
- Liquid crystal drive waveform
  — A (One line frequency AC waveform)
- Correspond to high speed MPU bus interface
  — 2 MHz (when V_{CC} = 5V)
- 4-bit or 8-bit MPU interface enabled
- 80 × 8-bit display RAM (80 characters max.)
- 9,920-bit character generator ROM for a total of 240 character fonts
  — 208 character fonts (5 × 8 dot)
  — 32 character fonts (5 × 10 dot)

Header	Module address	Package identifier	Package length	Confirmation code	Checksum
2 bytes	4 byte	1 byte	2 bytes	1 byte	2 bytes
0xEF01	xxxx	07H	0003H	xxH	Sum

Note: Confirmation code=00H: password setting complete;

Confirmation code=01H: error when receiving package;

6.2.3 Set Module address

Description: Set Module address. (Refer to 4.7 for adderss information)

Input Parameter: None;

Return Parameter: Confirmation code (1 byte)

Instruction code: 15H

Command (or instruction) package format:

Header	Original Module address	Package identifier	Package length	Instruction code	New Module address	Checksum
2 bytes	4bytes	1 byte	2 bytes	1 byte	4 bytes	2 bytes
0xEF01	xxxx	01H	0007H	15H	xxxx	sum

Acknowledge package format:

Header	New Module address	Package identifier	Package length	Confirmation code	Checksum
2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
0xEF01	xxxx	07H	0003H	xxH	Sum

Note: Confirmation code=00H: address setting complete;

Confirmation code=01H: error when receiving package;

6.2.4 Set system parameter

Description: Operation parameter settings. (Refer to 4.4 for more information)

Input Parameter: Parameter number;

Return Parameter: Confirmation code (1 byte)

Instruction code: 0eH

Command (or instruction) package format:

Header	Module address	Package identifier	Package length	Instruction code	Parameter number	Contents	Checksum
2 bytes	4bytes	1 byte	2 bytes	1 byte	1byte	1byte	2 bytes
0xEF01	Xxxx	01H	0005H	0eH	4/5/6	xx	sum

Acknowledge package format:

ANEXO 7: Base de datos.

	Sistema de control de acceso Biométrico															
N°	Sistema de Identificación					Características físicas				Registro y autorización					ST1	X
	1	2	3	S1	D1	4	5	S2	D2	6	7	8	S3	D3		
1	5	5	5	15	Alto	4	5	9	Alto	5	5	5	15	Alto	**39**	Alto
2	5	5	5	15	Alto	5	5	10	Alto	5	5	5	15	Alto	**40**	Alto
3	5	5	5	15	Alto	5	4	9	Alto	5	5	5	15	Alto	**39**	Alto
4	5	5	5	15	Alto	5	5	10	Alto	4	4	5	13	Alto	**38**	Alto
5	5	5	5	15	Alto	5	5	10	Alto	5	5	4	14	Alto	**39**	Alto
6	4	4	4	12	Alto	4	4	8	Alto	5	5	5	15	Alto	**35**	Alto
7	5	5	5	15	Alto	5	5	10	Alto	5	4	5	14	Alto	**39**	Alto
8	4	4	4	12	Alto	5	5	10	Alto	4	4	4	12	Alto	**34**	Alto
9	5	5	4	14	Alto	5	4	9	Alto	5	5	5	15	Alto	**38**	Alto
10	4	4	4	12	Alto	4	5	9	Alto	4	5	4	13	Alto	**34**	Alto
11	5	5	5	15	Alto	4	4	8	Alto	4	4	4	12	Alto	**35**	Alto
12	4	4	4	12	Alto	4	5	9	Alto	4	5	5	14	Alto	**35**	Alto
13	4	4	4	12	Alto	4	4	8	Alto	4	4	4	12	Alto	**32**	Alto
14	4	4	4	12	Alto	4	4	8	Alto	4	3	4	11	Medio	**31**	Alto
15	5	4	4	13	Alto	4	4	8	Alto	4	5	4	13	Alto	**34**	Alto
16	4	4	4	12	Alto	5	4	9	Alto	4	4	4	12	Alto	**33**	Alto
17	4	4	4	12	Alto	4	4	8	Alto	4	5	5	14	Alto	**34**	Alto
18	4	4	4	12	Alto	4	4	8	Alto	4	5	4	13	Alto	**33**	Alto
19	4	4	3	11	Medio	4	4	8	Alto	3	4	4	11	Medio	**30**	Alto
20	4	4	4	12	Alto	4	4	8	Alto	4	4	4	12	Alto	**32**	Alto
21	4	4	4	12	Alto	4	4	8	Alto	4	4	4	12	Alto	**32**	Alto
22	4	4	4	12	Alto	4	4	8	Alto	4	4	4	12	Alto	**32**	Alto
23	4	4	3	11	Medio	4	4	8	Alto	4	3	4	11	Medio	**30**	Alto
24	4	4	4	12	Alto	4	4	8	Alto	4	4	4	12	Alto	**32**	Alto
25	4	4	4	12	Alto	4	4	8	Alto	2	3	4	9	Medio	**29**	Medio

	Seguridad Física														
N°	Mecanismos					Riesgos				Protección				ST2	Y
	9	10	11	S4	D4	12	13	S5	D5	14	15	S6	D6		
1	5	5	5	15	Alto	5	5	10	Alto	5	5	10	Alto	**35**	Alto
2	5	5	5	15	Alto	5	5	10	Alto	5	5	10	Alto	**35**	Alto
3	5	5	5	15	Alto	5	4	9	Alto	4	5	9	Alto	**33**	Alto
4	5	5	5	15	Alto	5	5	10	Alto	4	5	9	Alto	**34**	Alto
5	5	5	5	15	Alto	5	4	9	Alto	5	4	9	Alto	**33**	Alto
6	5	5	5	15	Alto	5	5	10	Alto	5	5	10	Alto	**35**	Alto
7	5	5	5	15	Alto	4	5	9	Alto	5	5	10	Alto	**34**	Alto
8	4	5	5	14	Alto	4	5	9	Alto	5	5	10	Alto	**33**	Alto
9	4	5	5	14	Alto	5	4	9	Alto	5	5	10	Alto	**33**	Alto
10	4	4	4	12	Alto	5	5	10	Alto	4	5	9	Alto	**31**	Alto
11	4	4	5	13	Alto	5	4	9	Alto	4	4	8	Alto	**30**	Alto
12	4	4	4	12	Alto	5	4	9	Alto	3	5	8	Alto	**29**	Alto
13	5	5	5	15	Alto	5	5	10	Alto	2	5	7	Medio	**32**	Alto
14	4	4	4	12	Alto	4	4	8	Alto	4	4	8	Alto	**28**	Alto
15	4	4	4	12	Alto	4	4	8	Alto	4	4	8	Alto	**28**	Alto
16	4	4	4	12	Alto	4	4	8	Alto	4	4	8	Alto	**28**	Alto
17	4	3	4	11	Medio	3	3	6	Medio	4	4	8	Alto	**25**	Medio
18	4	4	4	12	Alto	5	5	10	Alto	2	4	6	Medio	**28**	Alto
19	4	4	4	12	Alto	5	5	10	Alto	5	4	9	Alto	**31**	Alto
20	4	4	4	12	Alto	5	5	10	Alto	2	4	6	Medio	**28**	Alto
21	4	4	4	12	Alto	4	4	8	Alto	4	4	8	Alto	**28**	Alto
22	4	4	4	12	Alto	4	4	8	Alto	4	4	8	Alto	**28**	Alto
23	4	4	3	11	Medio	4	3	7	Medio	5	3	8	Alto	**26**	Medio
24	4	3	3	10	Medio	3	3	6	Medio	3	4	7	Medio	**23**	Medio
25	3	3	4	10	Medio	3	3	6	Medio	4	4	8	Alto	**24**	Medio