TÍTULO DEL TRABAJO DE GRADO

Selección e implementación de un sistema de registro y control de personal por medio de huella dactilar para las Unidades Tecnológicas de Santander sede I.T.S.I.

PROYECTO DE INVESTIGACIÓN

AUTORES

JUAN GABRIEL GONZALEZJAIMES 1098686032
JAISON MARTINEZ SALAZAR 1096223918

Trabajo de Grado para optar al título de
Tecnólogo en electrónica industrial

DIRECTOR
Ing., M.Sc. LUIS OMAR SARMIENTO ALVAREZ

DIANOIA

UNIDADES TECNOLÓGICAS DE SANTANDER
FACULTAD CIENCIAS NATURALES E INGENIERÍAS
TECNOLOGIA EN ELECTRONICA INDUSTRIAL
BARRANCABERMEJA
FECHA DE PRESENTACIÓN: 31-07-2017

Nota de Aceptación

_____

_____

_____

_____

_____
Firma del jurado

_____
Firma del Jurado

DEDICATORIA

Este trabajo se lo queremos dedicar primero a Dios quien es el responsable de nuestros logros y gracias a él es el cumplimiento de los mismos, seguido a nuestros familiares quienes son el motor para superarnos como personas y capacitarnos en un arte, así mismo queremos agradecer a nuestro director el ingeniero Luis Omar Sarmiento Álvarez ya que con sus orientaciones, consejos y observaciones logramos el presente proyecto.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN EJECUTIVO

Por medio de un sistema biométrico que permita la identificación y verificación de cada individuo gracias a las características únicas de la huella dactilar y aplicando técnicas matemáticas y estadísticas encargadas de la autenticación del usuario, se realizará el reconocimiento de huellas dactilares al personal que labora en las Unidades Tecnológicas de Santander sede I.T.S.I. Con la implementación de la tecnología biométrica que permitirá controlar la entrada y salida de todo el personal, el sistema biométrico también recolectará la información almacenada correctamente de forma completa, exacta, actualizada, comprobable, y comprensible; Además se proyecta la transmisión automática de los datos recolectados hasta la sede de las UTS ubicada en el colegio Diego Hernández de Gallegos.

Este dispositivo hace parte del hardware o parte física del cual se compone el control de acceso, el cual se instalará al ingreso de l institución.

.

PALABRAS CLAVE. Almacenamiento, Huella Dactilar, Identificación, Registro, biométrico.

INTRODUCCIÓN

La recolección de datos ha sido al pasar del tiempo una tarea a mejorar en las organizaciones, ya que la misma es tediosa y debe ser veraz y comprobable, es por eso que la tecnología permite ser más eficientes y eficaces en la recolección de datos y en el control de los mismos según el tipo de necesidad de las organizaciones. Ideando herramientas informáticas que facilitan la identificación de los usuarios y trabajadores de las organizaciones, con el objetivo de evitar fraudes o llevando un control de ingreso y salida de los mismos. Uno de los sistemas más utilizados para el reconocimiento de las personas es el biométrico que es un "método automático de identificación y verificación de un individuo utilizando características físicas y de comportamiento precisas" (UNAM, Facultad de Ingeniería, 2017), tales como: patrones oculares, voz, escritura, huellas, entre otros.

Actualmente el más utilizado por su practicidad y precisión es el reconocimiento por huella dactilar, el cual consiste en un "proceso de lectura que comienza cuando se presiona el dedo sobre el lector. Este ya trae incorporado su propia fuente de iluminación, normalmente un juego de LED's para iluminar las vallas de la huella digital" (ISEC, 2017), posteriormente es tomada un impresión de la huella dactilar la cual es verificada con la base de datos según sus características como lo son los deltas y núcleos de la huella.

Dichas tecnología ha tenido gran acogida por su facilidad y practicidad, ya que facilita el seguimiento del personal en las organizaciones, en este caso en particular se escoge esta herramienta ya que las características permiten la adecuada utilización del mismo en la institución, al utiliza el reconocimiento de huellas por medio del terminal de tiempo y asistencia con funciones de control de acceso K30, por medio de una investigación bajo la modalidad de proyecto factible.

1. DESCRIPCIÓN DEL TRABAJO DE INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

Actualmente en las Unidades Tecnológicas de Santander sede I.T.S.I. el control de acceso del personal es realizado manualmente por un empleado que verifica por cada salón la hora de entrada y salida de cada docente, este control es llevado atreves de una planilla en donde se diligencia los horarios de cada docente, con el objetivo de llevar un seguimiento en el cumplimiento de los horarios y los pagos de cada docente según las horas de catedra dictadas.

Este proceso de verificación es lento, e inseguro ya que esa información que está almacenada en las planillas no representa ningún tipo de organización de datos, pues carece de información detallada de los horarios de los docentes, siendo poco confiable la hora de ingreso y salida plasmada en éstas sea real.

Esta problemática ha permitido buscar una solución que logre establecer un sistema de verificación confiable y segura para saber de forma exacta el horario de ingreso y salida del personal docentes de la institución I.T.S.I. y contribuyendo a la disminución de costos y mejoramiento de los servicios de la institución, por lo que se plantea como problema: ¿Cómo se implementa un sistema de reconocimiento de huella dactilar que permita conocer la hora de ingreso y salida del personal administrativo de la planta de docentes en el I.T.S.?

1.2. JUSTIFICACIÓN

Las organizaciones están sujetas a los diversos cambios que la tecnología al pasar del tiempo incorpora, esto motiva a las entidades a estar a la vanguardia de los avances tecnológicos - digitales. Por lo tanto es importante que las instituciones educativas y demás organizaciones implementen sistemas digitales en las diferentes áreas ya que la tecnología ofrece herramientas que mejora la calidad de servicio y la confiabilidad en la seguridad de la información.

Según lo anterior es impórtate tener en cuenta que la biometría es una tecnología-digital, que brinda seguridad ya que está basada en el reconocimiento y comprobación de una o varias características mediante algunos exámenes físicos de una persona, logrando obtener controles de sus salidas y entradas en lugares de forma remota.

Por consiguiente la implementación de un sistema biométrico de control de acceso en el I.T.S.I para los docentes de las Unidades Tecnológicas de Santander, será de gran apoyo dado a que por medio de huella dactilar permitirá tener un control más seguro y eficiente, mejorando la confiabilidad y seguridad en los ingresos y salidas de la planta de personal, mejorando el uso del tiempo de la jornada laboral en el plantel educativo.

La comunicación automática de los datos recolectados será realizada por medio de la aplicación TCP/IP que permitirá encontrar un camino que conecte la red del I.T.S.I con la del D.H.G esta función es realizada mediante routers que pueden enviar y recibir paquetes de datos por diferentes interfaces de red.

Todo esto contribuyendo en la puesta en práctica de los conocimientos adquiridos a lo largo de la carrera, al hacer una selección e instalación de un sistema biométrico de recolección de datos por medio de huella dactilar.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Implementar un sistema de registro y control biométrico para docentes que laboran en las UTS sede I.T.S.I con envío de datos mediante protocolo TCP/IP a las UTS sede Diego Hernández de Gallegos.

1.3.2. OBJETIVOS ESPECÍFICOS

- Realizar la selección e instalación de un sistema biométrico que permita obtener información sobre el registro de horas de ingreso y salida de la planta administrativa y docentes de la sede de I.T.S.I de la Unidades Tecnológicas de Santander.

- Instalar un sistema de comunicación IP que permita transmitir la información del sistema biométrico en tiempo real, adaptando los cambios que ofrece la tecnología al control de los docentes en su horario de ingreso y salida.

- Verificar el correcto funcionamiento del sistema biométrico en las Unidades Tecnológicas de Santander sede I.T.S.I, realizando ajustes al sistema de acuerdo a los procedimientos definidos en los manuales del equipo para recolectar la información sobre la verificación segura y confiable en el horario de ingreso y salida de todo el personal.

1.4. ESTADO DEL ARTE / ANTECEDENTES

“La evolución de la tecnología biométrica por medio de la autenticación basada en características físicas existe desde que existe el hombre” (Aguilera, 2012). Los sistemas de autentificación biométrica, basados en características físicas del usuario a identificar, el reconocimiento de formas, la inteligencia artificial y el aprendizaje son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos; la criptología se limita aquí a un uso secundario, como el cifrado de una base de datos de patrones retínales, o la transmisión de una huella dactilar entre un dispositivo analizador y una base de datos. “La autenticación basada en características físicas y sin darnos cuenta, es la que más utiliza cualquiera de nosotros en su vida cotidiana a diario identificamos a personas por los rasgos de su cara o por su voz” (Ricardo, 2007). Obviamente aquí el agente reconocedor lo tiene fácil porque es una persona, pero en el modelo aplicable a redes o sistemas Unix el agente ha de ser un dispositivo que, basándose en características del sujeto a identificar, le permita o deniegue acceso a un determinado recurso.

El estudio del arte “Modelo, diseño e implementación de una plataforma biométrica existen muchas aplicaciones prácticas de la biometría, pero es importante centrarse en que los sistemas biométricos aportan una solución muy efectiva al problema de la identificación, ya que se basan en las características físicas o de comportamiento del individuo, lo que supone una alternativa mucho más cómoda, fiable y segura que el uso de contraseñas, tarjetas o señas de identificación, ya que se identifica a la persona por “quien es” no por “que posee” o “que recuerda”. “El hecho de que los sistemas biométricos sean tan fiables ha contribuido para que esta área haya evolucionado considerablemente en los últimos años y cada vez sean más utilizados los sistemas biométricos” (Escorihuela, 2011). Dentro de la amplia gama de posibilidades que nos ofrece la biometría, la que ha cobrado más importancia ha sido la relacionada con la de identificación de los individuos.

Es importante conocer los orígenes de biometría es por eso que basados en “la identificación basada en la huella dactilar se viene utilizando en los Estados Unidos y Europa Occidental desde hace más de cien (100) años” (Jairo Alonso Gómez Cano, 2017).

Los grandes avances comerciales en los dispositivos biométricos se dieron en los años setenta con un sistema llamado Identimat, que medía la forma de la mano y la longitud de los dedos, la mayoría de los países del mundo utiliza las huellas digitales como sistema práctico y seguro de identificación. Con el avance tecnológico nuevos instrumentos aparecen para la obtención y verificación de huellas digitales. También se comienzan a utilizar otros rasgos morfológicos como variantes de identificación, por ejemplo, el iris del ojo, el calor facial o la voz. Actualmente la biometría se presenta en un sin número de aplicaciones, demostrando ser el mejor método de identificación humana (Jairo Alonso Gómez Cano, 2017).

Las Unidades Tecnológicas de Santander realizo un trabajo investigativo donde los estudiantes propusieron como tema central de su proyecto la “implementación de un sistema de registro y control, por medio de tecnología biométrica, para controlar la asistencia del personal que labora en las unidades tecnológicas de Santander sede D.H.G.” (Leal, A., Bermudez Padilla., & Gonzalez, 2016). Este trabajo ha sido de gran importancia pues las Unidades Tecnológicas de Santander, ya que no realizaba un proceso de control de acceso a docente o personal administrativo de la institución. Esta situación se presta para que se presenten ausencias, salidas antes del horario o retrasos. Los principales afectados por esta situación son los estudiantes ya que en algunos casos ven reducido el tiempo de cada clase, con el consecuente detrimento académico; es por eso que se realizó la implementación de este trabajo en la sede (D.H.G.) para luego implementarla en otras sedes de las Unidades Tecnológicas de Santander (I.T.S.I.).

2. MARCOS REFERENCIALES

2.1. MARCO TEORICO

2.1.1. Biometría

“Los orígenes de la biometría se remontan a los años setenta cuando la empresa NEC comienza a trabajar junto al FBI en la aplicación de técnicas matemáticas y estadísticas de un individuo basado en rangos conductuales o intrínsecos” (Bulla Camacho, Rodriguez Gonzalez, & Gutierrez Ricardo, 2006).

De esta manera se comienzan a desarrollar una serie de algoritmos que permitieran medir y analizar las características y del comportamiento de humanos con propósitos de autenticación, estos sistemas incluyen un dispositivo de captación que en segundos obtiene una muestra biométrica de la persona y la compara con una base de datos, donde se analiza si corresponde o no a la identidad de la persona en cuestión, las huellas dactilares, la retina, el iris, los patrones faciales, las venas de la mano, o la geometría de la palma de la mano representan las características físicas del ser humano.

Con el pasar de los años la biométrica ha crecido de manera exponencial ya que la inserción de todas estas tecnologías y métodos totalmente automáticos genera cambios en la manera de vivir de las personas, esto ayudara que las personas que han olvidado sus contraseñas, las tarjetas o identificaciones como la licencia de conducir o el pasaporte al ser olvidados, robados o perdidos. Sean remplazados por los sistemas biométricos que se han vuelvo tan populares, los más destacados son el reconocimiento facial o de huella digital, sin embargo existen algunos como escáner de retina, comparación del habla, geometría de la mano entre otros. Tecnologías biométricas comúnmente utilizadas.

Los sistemas biométricos funcionan con arreglo a un modelo general que consiste en el registro de la persona en el sistema. “Durante el proceso de registro, el sistema captura el rasgo característico de la persona, como por ejemplo la huella digital, y lo procesa para crear una representación electrónica llamada modelo de referencia” (Giz Bueno & Tolosa Borja, 2017). De acuerdo con la teoría tradicional

en biometría, el siguiente paso del sistema biométrico consiste en verificar la identidad de la persona o identificar a la persona. En el caso de verificación, la persona le informa al sistema cuál es su identidad, ya sea presentando una tarjeta de identificación o introduciendo alguna clave especial. Se captura el rasgo biométrico y se compara con el modelo de referencia de la persona. Si ambos modelos coinciden, la verificación se realizó con éxito, si no es fallida.

Figura 1: Biometría de huella

Fuente: http://www.integri-sys.com/es/soluciones_biometria

Tabla 1: Clases de biometría y sus características

	Iris	Retina	Huella Dactilar	Geometría de mano	Escritura y firma	Voz	Rostro
Fiabilidad	Muy Alta	Muy Alta	Alta	Alta	Alta	Alta	Alta
Usabilidad	Media	Baja	Alta	Alta	Alta	Alta	Alta
Seguridad	Muy Alta	Muy Alta	Alta	Alta	Media	Media	Media
Aceptación	Media	Media	Media	Alta	Muy Alta	Alta	Muy Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media	Media

Fuente: www.cc3m.com/biometria

2.1.2. Almacenamiento de datos

“Las empresas buscan soluciones tecnológicas que faciliten la realización de operaciones eficientes con sus proveedores, clientes y usuarios internos; y alta disponibilidad que garantice “estar en línea” cuando alguno de ellos requiera algún servicio, y que cumplan los estándares de seguridad” (Alto nivel, 2017).

Por ende se debe también aclara que existen dos clases de almacenamiento, como lo son el interno y el externo los cuales se diferencian en que los internis no hacen parte de la memoria interna del ordenador como (RAM y ROM).

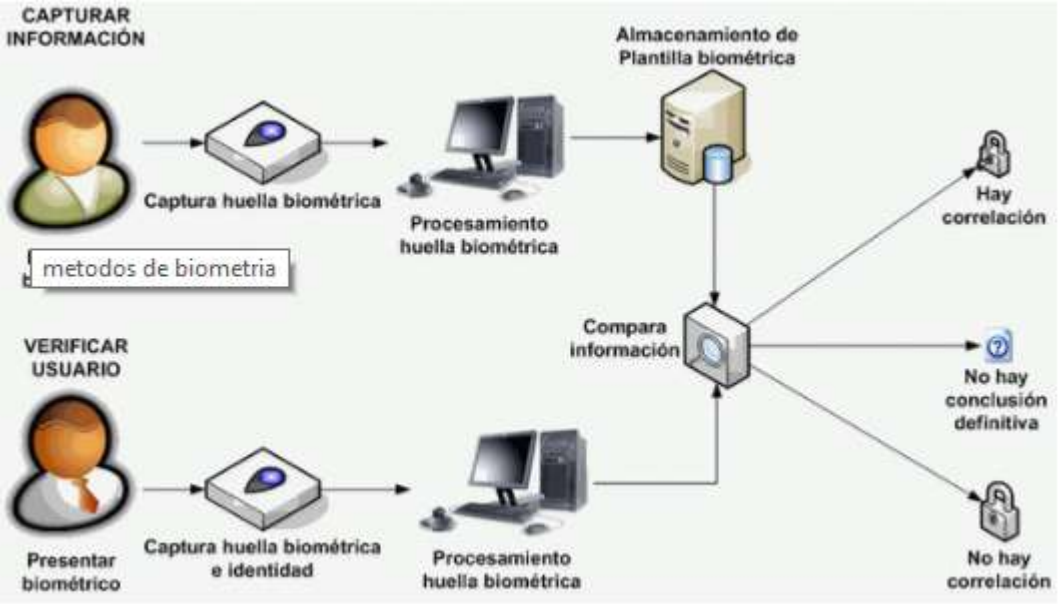
Los dispositivos de almacenamiento también se pueden clasificar según el modo de acceder a los datos que contienen:

El acceso secuencial: en este tipo, para acceder a la información se debe leer registro por registro desde el inicio, hasta llegar al registro particular que contiene los datos a los que deseamos acceder. Estas memorias se clasifican en registros de desplazamiento, dispositivos por acoplamiento por carga y memorias de burbuja.

El acceso aleatorio: el elemento de lectura accede directamente a la dirección donde encontramos la información físicamente a la que se pretende acceder, sin tener que pasar previamente por la almacenada entre el principio de la grabación y el lugar donde se guarda la información buscada. O según la volatilidad de la información:

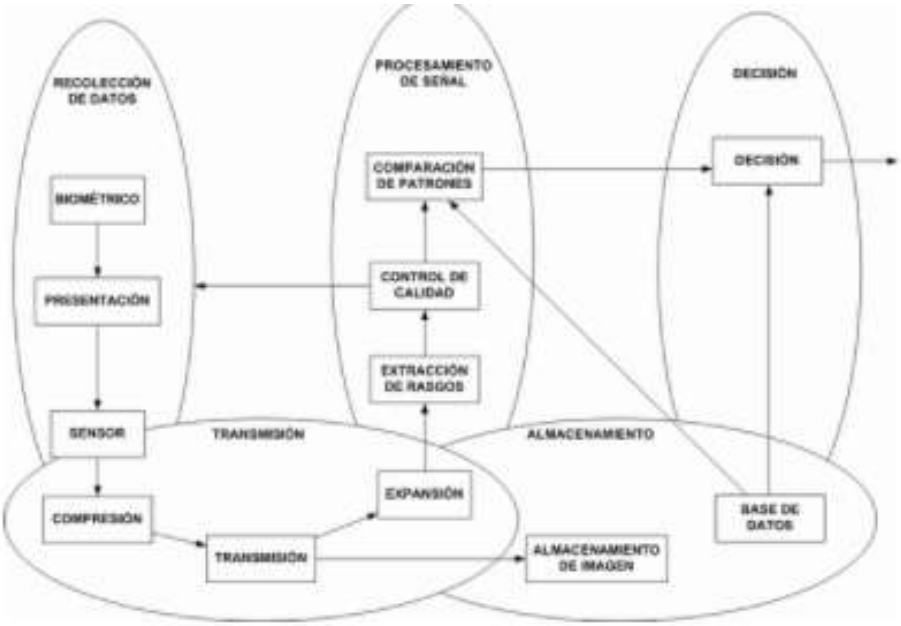
La memoria volátil requiere energía constante para seguir manteniendo la información almacenada y sólo suele utilizarse en las memorias primarias, como por ejemplo la memoria RAM. Por otra parte, la memoria no volátil retiene la información almacenada incluso cuando no se recibe electricidad constantemente. Se utiliza para almacenar a largo plazo y por tanto, en memorias secundarias. (UIB, 2017).

Figura 2: Almacenamiento de datos biométricos



Fuente: FRAX expertos en Biometría

Figura 3: Relacionamiento de datos biométricos



Fuente: FRAX expertos en Biometría

2.1.3. Huella Dactilar

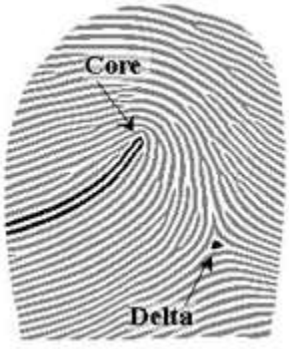
La huella dactilar es una característica física única que distingue a todos los seres humanos y la ciencia que se encarga de su estudio se conoce como Dactiloscopia, que viene de los vocablos griegos daktilos (dedos) y skopein (examen o estudio). Este nombre fue inventado por el doctor Francisco Latzina en sustitución al dado en 1892 por Sir Francis Galtón (Icnofalangometría). (Ecured, 2017). Todos los sistemas dactiloscópicos se basan en tres principios fundamentales:

Perennidad: Gracias al fisiólogo checo Juan Evangelista Purkinje se sabe que las huellas dactilares se manifiestan a partir del sexto mes del desarrollo del embrión y que están presentes a lo largo de toda la vida de los seres humanos y hasta la descomposición del cadáver (Purkynĕ, 1823) .

Inmutabilidad: Las huellas dactilares no se ven afectadas en sus características por el desarrollo físico de los individuos ni por enfermedades de ningún tipo y en caso de que llegase a presentarse un desgaste involuntario (por ejemplo una herida o quemadura), el tejido epidérmico que la conforma es capaz de regenerase tomando su forma original en un periodo de 15 días.

Diversidad Infinita: Las huellas dactilares son únicas e irrepetibles, cada ser humano posee huellas dactilares con características individuales. Es un error común pensar que los gemelos idénticos no cumplen con este principio, sin embargo las huellas dactilares no se desarrollan debido a un proceso genético sino a un proceso aleatorio por lo que no existe ningún tipo de correlación entre gemelos idénticos o individuos de una misma familia (UNAM, Facultad de Ingeniería, 2017).

Figura 4: Puntos singulares de huella dactilar



Fuente: UNAM - Facultad de Ingeniería

2.1.4. Identificación

La información de identificación personal (PII) es cualquier dato que podría identificar potencialmente a un individuo específico.

Cualquier información que puede ser utilizada para distinguir una persona de otra, y que puede ser usada para quitarle el anonimato a los datos anónimos puede ser considerada PII. PII puede ser sensible o no sensible. (techtarget, 2017).

2.1.5. Registro

“Acción que se refiere a almacenar algo o a dejar constancia de ello en algún tipo de documento. Un dato, por su parte, es una información que posibilita el acceso a un conocimiento”. La noción de registro de datos, por lo tanto, está vinculada a consignar determinadas informaciones en un soporte. El registro de datos puede desarrollarse tanto en un papel como en formato digital”. (Pérez Porto , Julián; Merino, María, 2017).

Tabla 2: Ejemplo de registro de datos

Fuente: Imágenes Google

2.2. MARCO HISTORICO

Según “Marcelo Malpighi, identificó que las características de los dedos no cambiaban y eran diferentes unas de otras” (Maya Vargas, 2013), esta información permitió a Jan Evangelist Purkinje (Purkyně, 1823), establecer que las huellas eran únicas y las figuras que se formaban en ellas no cambiaban con el paso del tiempo, Henry Faulds Fue el primero que inicio con la utilización de la ficha decadactilar y comprobó que al coger objetos se dejaban huellas sin la necesidad de estar manchados. “Francisco.G Presenta la propuesta de la creación de un sistema de identificación afianzado en la perennidad, individualidad de las huellas dactilares, asegura que la posibilidad que dedos distintos dejen la misma huella dactilar son menos de una en 64 billones” (Maya Vargas, 2013). Gracias al avance de la tecnología en 1905 y 1908 se pudo implementar el sistema de huella dactilar a la Fuerza Aérea, Ejército y Armada de Estado Unidos.

Existe una gran variedad de tecnologías biométricas, tantas como características biométricas. Muchas de ellas se están aplicando en la vida real y otras están en proceso de estudio. Algunas características biométricas que se utilizan actualmente son: voz, huellas dactilares, cara, iris, retina, venas de la mano, forma de la mano, forma de la oreja, forma de andar, forma de escribir en un teclado, firma, ADN y olor. (Velasquez Valencia, Jorge Eduardo; Linares Jaramillo, Alvaro Andres, 2013).

A continuación, se explican algunas de estas características:

2.2.1. Iris

La tecnología que permite el reconocimiento del iris tiene en cuenta las características únicas de este; en si los sistemas biométricos poseen entre 13 y 60 propiedades distintas, mientras que el iris posee 266 puntos únicos. Se cree que Cada ojo es único y permanece estable con el tiempo y en los ambientes (Anonimo, 2013)

2.2.2. Retina

La retina Es un elemento característico de cada individuo que ha permitido que los sistemas de autenticación por medio de la tecnología biométrica puedan capturar y analizar los patrones de la red vascular alrededor del nervio óptico. El escáner de retina ilumina, a través de la pupila, una región de la retina con luz infrarroja y almacena la información del contraste de los patrones vasculares reflejados para

compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

2.2.3. Huella Dactilar

"Esta técnica es el método más viejo en autenticación de identidad y ha sido usada desde 1896 y ha sido ampliamente usada en la identificación de criminales" (Velasquez Valencia, Jorge Eduardo; Linares Jaramillo, Alvaro Andres, 2013). Cada sujeto o individuo posee un patrón único de huellas y para el reconocimiento usualmente se analiza la información geométrica que se produce entre los patrones de la huella.

La huella dactilar en su estructura como método de identificación, está formada por crestas papilares y surcos interpapilares los cuales están localizados en la piel formando los dibujos en la falange distal de los dedos de las manos, lo que hace que se formen puntos característicos, un núcleo y uno o varios deltas, con el fin de llevar a cabo la verificación de identidad, están constituidas por sudor, aceites corporales, grasas y sustancias químicas externas a la piel sustancias expulsadas por las glándulas sebáceas, glándulas sudoríparas y poros que hacen que al coger un objeto cualquiera que sea quede plasmada la huella dactilar sobre la superficie manipulada.

2.2.4. Reseña de la empresa ZKTeco

En 1985, ZKTeco (anteriormente 'ZKSoftware') inició el desarrollo de un algoritmo biométrico revolucionario, dando como resultado la creación de nuestros algoritmos de reconocimiento de huella digital y de rostro líderes en la industria.

En el 2009, ZKTeco construyó una zona industrial de 50,000m2 con certificación ISO9000. La instalación permite controlar la calidad, investigación, diseño, fabricación, ensamblaje y envió de productos, todo bajo un mismo techo.

En el 2015, con el objetivo de proporcionar una solución total de seguridad, se libera el software ZKBioSecurity el cual permitirá la gestión de control de acceso, asistencia, patrullaje, estacionamiento, control de elevadores, módulo de visitantes, videovigilancia y cerraduras inteligentes en una misma plataforma basada en web.

Hoy en día, el servicio y la red de ventas de ZK dependen sus socios y oficinas en todo el mundo. Más de 220 millones de personas utilizan productos ZKTeco en aproximadamente 200 países. ZKTeco se ha convertido en una marca reconocida y respetada en la industria de la seguridad y tecnología biométrica.

2.3. MARCO LEGAL

Actualmente y producto de la suplantación de identidades por parte de los delincuentes cibernéticos, el gobierno idea mecanismos de control con las bases de datos , logrando mantener un control de las mismas y posibilitado que los usuarios de las distintas organizaciones no los saturen de información, la cual es entregada a las organizaciones además de la venta de bases de datos para fraudes y robos, ya que al conocer los datos específicos de las personas como: correos electrónicos, teléfonos, dirección y otros datos personales , los cuales son fundamentales para saber la ubicación de los usuarios.

Dentro de los requisitos para el tratamiento de datos se encuentra:

2.3.1. Política de tratamiento de datos

Las personas que gestionan bases de datos personales en Colombia deben adoptar un manual interno de políticas y procedimientos con el fin de proteger los derechos de los titulares y atender sus consultas y reclamos.

La política de tratamiento de datos debe ponerse a disposición de los titulares y debe estar escrita en un lenguaje claro y sencillo. La política de tratamiento de datos debe: identificar a quien opera la base de datos personales y proveer sus datos de contacto, definir expresamente el tipo de tratamiento de los datos personales y la finalidad del mismo, establecer los derechos de los titulares, detallar el procedimiento de solicitud de información, actualización, rectificación y supresión de datos personales, así como el procedimiento de revocación de autorización de tratamiento de datos personales, y la vigencia de política de datos.

2.3.2. Aviso de privacidad

El Decreto No. 1377 de 2013 permite que se utilice un aviso de privacidad al momento de la recolección de datos personales, cuando no les sea posible comunicar a los titulares toda la política de tratamiento de datos.

2.3.3. Autorización

Quienes operan y gestionan bases de datos personales deben obtener el consentimiento previo, expreso e informado de los titulares para realizar el

tratamiento de los datos personales. La autorización deberá ser obtenida al momento de la recolección de los datos y almacenada en cualquier medio que permita su consulta posterior.

2.3.4. Medidas de seguridad

En virtud del principio de seguridad de la información, las personas que operen y gestionen bases de datos personales deben implementar medidas necesarias en el tratamiento de datos personales. Esto con el fin de evitar la adulteración, pérdida, acceso o uso no autorizado de estos datos.

2.3.5. Inscripción ante el Registro Nacional de Bases de Datos (RNBD).

El Registro Nacional de Bases de Datos (RNBD) es el directorio de las bases de datos gestionadas en Colombia, el cual es administrado por la Superintendencia de Industria y Comercio (SIC) y está disponible para su libre consulta. En virtud del Decreto No. 886 de 2014, el Decreto 1074 de 2015 y la Circular Externa No. 2 de 2015, el gobierno reglamentó la inscripción de base de datos personales en el RNBD (Narváez, 2017).

3. DESARROLLO DEL TRABAJO DE GRADO

3.1. Recopilación, análisis y sistematización del sistema biométrico. En la identificación y registro de docentes

Con el objetivo de facilitar la obtención de la información por medio de una herramienta biométrica atreves de la que se recolecte la información del personal docente, se realizó una investigación preliminar de los equipos que se ajustaran a las necesidades del planten de la institución y se llegó a la determinación del equipo K30 de la empresa ZKTeco, el cual cuenta con las características necesarias y la rapidez en la solución de inconvenientes con respecto adecuado funcionamiento del software.

3.1.1. Características del Terminal de Tiempo

El K30 es una elegante terminal de tiempo y asistencia con funciones básicas de control de acceso, con pantalla TFT de 2.8 pulgadas. Permite comunicación con cerraduras eléctricas y con botones de salida. La comunicación TCP/IP y el puerto USB permiten la gestión de los datos de forma extremadamente sencilla. Además, incorpora una batería de respaldo con lo que se elimina el problema de fallos de electricidad (ZKTeco, 2015).

Tabla 3: Características equipo K30

Comunicación	TCP/IP y USB Host.
Batería	De respaldo incorporada
Control de acceso	Simple
Alarma	Externa.
Diseño	Elegante.
Idiomas	Multiples
Reporte	SSR en formato Excel.

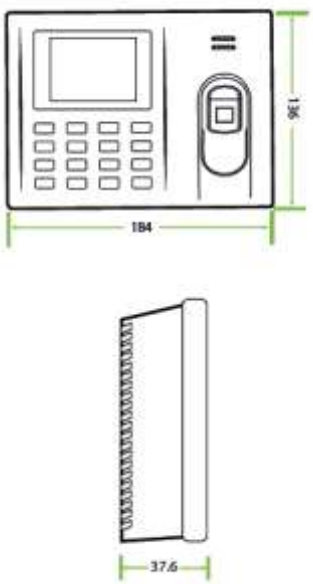
Fuente: Autor

Tabla 4: Especificaciones equipo K30

Capacidad de Huellas	1.000 (2.000 sin SSR)
Capacidad de Tarjetas ID	1.000 (Opcional)
Capacidad de Registros	80.000
Pantalla	Pantalla TFT 2.8 pulgadas
Comunicación	TCP/IP, USB-Host
Funciones Estándar	Codigo de Trabajo, SMS, Horario de Verano, Búsquda Self-Service, Cambio Automático de Estado, Timbre Programado, Entrada T9, ID de Usuario de 9 Dígitos, Batería Incorporada, Timbre Externo.
Funciones Opcionales	Tarjetas ID / MIFARE
Software	ZKTime 5.0
Fuente de Alimentación	DC 12V 1.5A
Velocidad de Verificación	0.5 Seg
Temperatura de Operación	0°c - 45°c
Humedad de Operación	20% - 80%
Dimensiones	184 x 136 x 37.6 mm

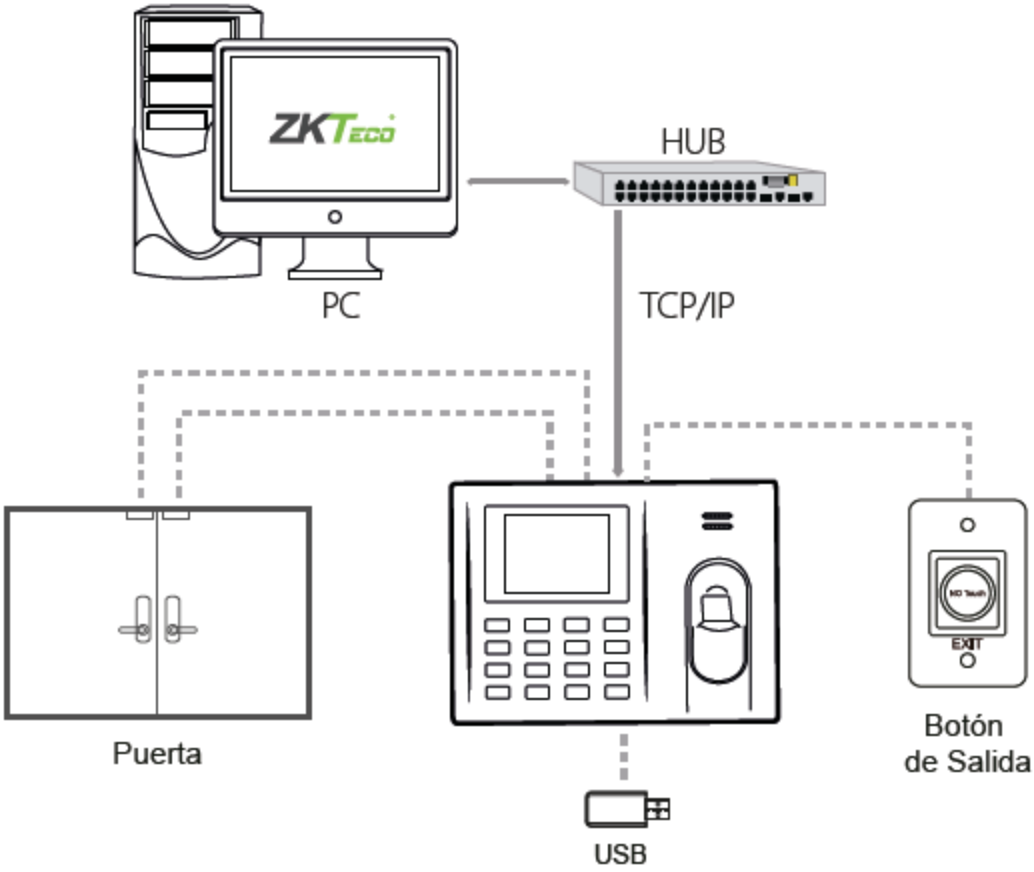
Fuente: Hoja de especificaciones ZKTeco.

Figura 5: Dimensiones del equipo en (mm)



Fuente: Hoja de especificaciones ZKTeco

Figura 6: Diagrama de Aplicación



Fuente: Hoja de especificaciones ZKTeco

3.2. Verificación del sistema del equipo K30

Posterior del análisis en la selección del sistema, se determina según el manual del equipo el paso a paso de la instalación, documentando como se debe realizar la interface del sistema logrando que de forma remota se comunique el lector con el equipo (pc) principal.

3.3. Pasos de instalación

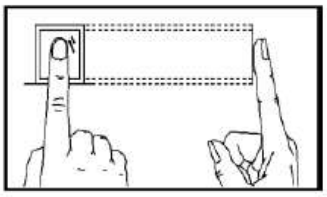
- Instalar la máquina y conectar a la fuente de alimentación.

- Insertar una USB o una tarjeta SD en la máquina de asistencia. Establecer los turnos deseados
  Nota: Para registrar un nuevo usuario deberá tener los privilegios de administrador.
- Insertar la USB o la SD en la máquina de asistencia.
- Desde la interfaz principal escoger Administración de usuarios. Para registrar Huellas de empleados y password.
- Verificar que la Huellas y los password a registrar estén disponibles y no registrados.
- Asegurarse de que el tiempo en la máquina o dispositivo es correcto antes de empezar la grabación de la asistencia.
- Al final de cada mes, escoger el reporte para descargar el reporte a la USB o tarjeta SD. (ZKTeco (Alvaro Obregón), 2016)

3.4. Recomendaciones para colocación del dedo

Dedos recomendados: El índice, el medio o el anular; el dedo gordo y el pequeño no son recomendados (debido a que son muy torpes y es difícil su lectura).

Figura 7: Forma correcta de colocar la huella



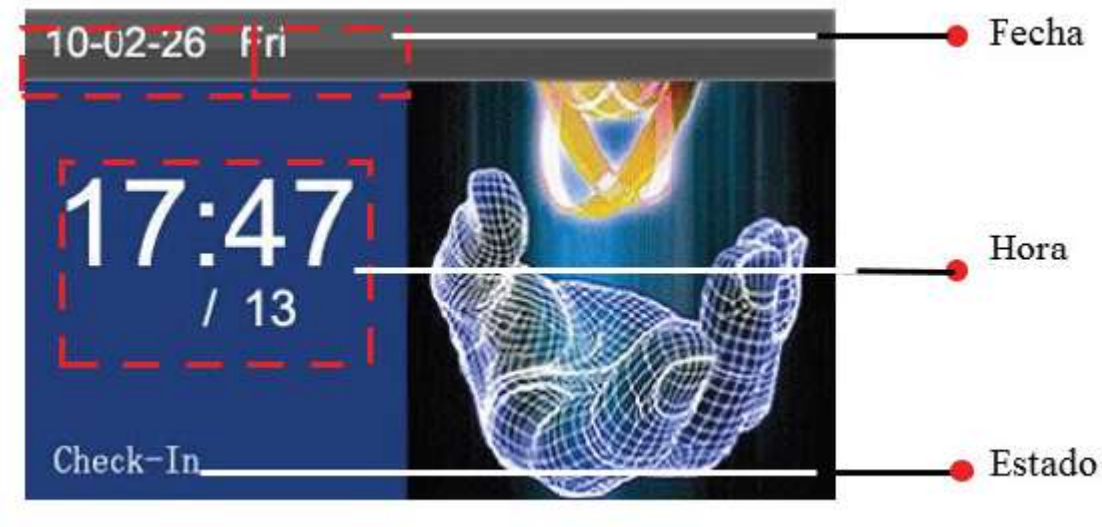
El dedo debe colocarse en una forma totalmente plana y centrado en el sensor

Fuente: Manual de usuario ZKTeco

3.5. Interfaz principal

Se debe tener precaución e identificar cada una de las características de la interfaz con el objetivo de que los datos sean cargados de forma correcta.

Figura 8: Pantallazo interfaz principal



Fuente: Manual de usuario ZKTeco

3.6. Verificación de asistencia

Con el objetivo de que el usuario este seguro que sus datos fueron tomados de forma correcta se generan unos reportes y alertas en tiempo real, en donde se detecta si fue o no tomada la huella de no ser así, se debe digitar el password que es una opción que tiene el sistema con el objetivo de facilitar el acceso, solo si la huella no es escaneada.

Figura 9: Pantallazo cuando la huella es tomada de forma correcta

Fuente: Manual de usuario ZKTeco

Una vez el docente marque la entrada, el dispositivo le indicara si la toma de esta ha sido correcta promedio de un flecha de color verde de lo contrrio devera repetir el procesimiento.

Figura 10: Pantallazo cuando el password es digitado de forma correcta

Fuente: Manual de usuario ZKTeco

Si en lugar de la huella se le ha sido signada una contraseña esta al ingresarse de manera correcta arroja un pantallazo según la figura 10, de lo contrario se debera ingresar nuevamente.

3.7. Menú principal del sistema

Al oprimir M/OK se desplegara la siguiente ventana:

Figura 11: Pantallazo menú principal

Fuente: Manual de usuario ZKTeco

En la figura 11, se observa el menú principal del dispositivo, el cual le da acceso al administrador a las diferentes características del biométrico K30.

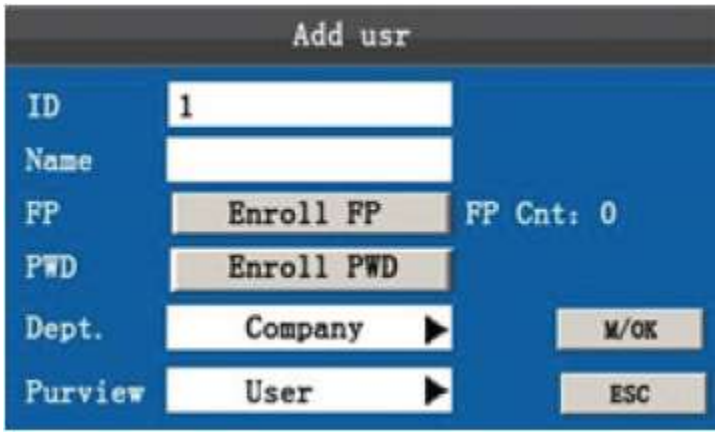
3.7.1. Usuario (User):

En esta opción se crean los usuarios es decir se alimenta la base de datos con la información de los docentes incluyendo ID, nombre, huella, password y privilegios.
Con el objetivo de tener claridad en la alimentación de la base de datos de los usuarios se detalla un ejemplo con el cual se explica la inscripción de un usuario.

1. La base de datos se debe construir basándose en los perfiles de los docentes, según la información personal requerida como nombre, cedula, horarios, tiempos de contratación.

2. Teniendo en cuenta los anteriores criterios se procede a seleccionar el docente para la alimentación de la base de datos en la opción agregar usuario, en donde se despliega la siguiente ventana.

Figura 12: inscripción de docentes



Fuente: Manual de usuario ZKTeco

3. Se diligencia los datos del docente como se muestra en la figura 12; **ID, Nombre, FP** (huella del usurio, pueden ser hasta 10), **PWD** (password del usurio, este utiliza cuendo no es tomada la huella), **Dept** (Sección o departamento al que pertenece el docente) y **Purview** (configuración de privilegios). En este último se determina si el docente es administrador o usuario ordinario.

Nota: El usuario administrado, esquíen puede eliminar y descargar los registros ya que tiene acceso al menú principal, mientras que los usuarios ordinarios solo podrán visualizar la verificación en el ingreso o salida marcada en el sistema.

Administrar Usuarios: Facilita la búsqueda de información de los usuarios antes creados en la opción de agregar usuarios, en esta aplicación se puede editar o borrar la información de los usuarios y las actividades realizadas por los mismos.

Sistema: Se encuentran los parámetros del sistema, incluyendo parámetros básicos de voz, parámetros de Huellas y Huellas de asistencia.

Reporte: Los repostes se pueden descargar por medio de una USB, cuando la información no es descargada de forma remota, esta aplicación sirve de contingencia cuando existen fallas con el internet de la institución al facilita la descarga de datos los cuales pueden ser visualizados desde un pc.

Administrar Datos: Permite restablecer el equipo a valores de fábrica y actualizar la versión del software. (ZKTeco (Alvaro Obregón), 2016)

Almacenamiento de Datos: Sirve para descargar desde una USB los datos almacenados hasta la fecha como usuarios, huellas, etc. Los cuales se encuentren en el sistema.

Registros: Este Menú permite realizar una fácil consulta de los registros de asistencia salvados en el equipo.

Información del Sistema: Podrá verificar aquí el estado de almacenamiento así como la versión e información del equipo. (ZKTeco (Alvaro Obregón), 2016).

3.8. Reportes del sistema

Los reportes del sistema en donde se encuentra la base de datos de los horarios de entrada, descansos y salidas del personal son enviados de forma remota atreves del sistema o según daño o falla que se presente, este puede ser descargado por medio de USB en donde se recolecta la información y posteriormente es descargada para su revisión y comprobación.

Tabla 5: Reportes del sistema por horario

Attendance Setting Report

Shift						
Number	First time zone		Second time zone		Overtime	
	On-duty	Off-duty	On-duty	Off-duty	Check-In	Check-Out
1	09:00	18:00				
2	09:00	12:00	13:30	18:00		
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						

Fuente: Manual de usuario ZKTeco

Tabla 6: Reportes del sistema por turno

Schedule Setting Report

Special shifts 25-Ask for leave, 26-Out, Null-Holiday

Schedule date				2013-1-1																											
ID	Name	Department	Card number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
				TUE	WED	THU	FRI	SAT	SUN	MON	TUE	WED	THU	FRI	SAT	SUN	MON	TUE	WED	THU	FRI	SAT	SUN	MON	TUE	WED	THU	FRI	SAT	SUN	MON	TUE	WED	THU
1	Joe	company																																
2	David	company																																
3	Mark	company																																
4	Jack	company																																

Fuente: Manual de usuario ZKTeco

La tabla 6 muestra el planning en este caso mensual de los docentes registrados en el dispositivo, se asigna el turno que deberá cumplir el docente en el transcurso del mes, estos turnos son creados de acuerdo a la base datos suministrada por las UTS en la tabla 5, para lograr una recolección de datos lo más veraz posible.

3.9. Reunión con un docente que labora en las Unidades Tecnológicas de Santander y explicación de las características, objetivos y alcances del trabajo.

Se realiza inducción en donde se explica al docente Luis Omar Sarmiento los procedimiento para el adecuado almacenamiento de datos y la alimentación de la base de datos con la información necesaria para identificar al docente, dentro de la inducción se explica el menú principal del sistema y las funciones a realizar encada uno, esto con el objetivo que el docente posteriormente realice una retroalimentación de la información a la persona encargada del biométrico.

En la misma reunión se verifico y socializo el cumplimiento de los objetivos, junto con las recomendaciones que se encuentran incluidas dentro del presente documento, como también los resultados del proyecto.

3.10. Visita e instalación del biométrico, según previa selección del lugar.

Para la realización del montaje se determinó como mejor opción la instalación del biométrico, dentro de la garita del celador ya que la sede es compartida con el colegio ITSI, lo que posibilita una mala utilización por de los alumnos al ubicase en un lugar visible de los mismo y sin supervisión de un delegado del a UTS, así

mismo se tuvo en cuenta que el biométrico según recomendación del proveedor del equipo, debe ser instalado bajo techo ya que al encontrarse en la intemperie puede presentar daños en su adecuado funcionamiento, perdiendo la garantía del equipo.

- El biométrico es ubicado entrando a la garita a mano izquierda a 1,50 metros de altura del piso, de tal forma que sea visible para el docente y él mismo pueda realizar su registro sin interferir con las funciones del celador de la institución.

- El switch de red está ubicado en la oficina de secretaria general a 30 metros del biométrico, para lo que se hace necesario utilizar aproximadamente 40 metros de cable de red.

Nota: Consulte los Anexos A al final del documento para una observación grafica del proceso de instalación.

3.11. Problemas

Antes del montaje del biométrico se solicitó permiso a la institución para la verificación en la conexión del cable de red, dicho permiso fue negado ya que se encontraban en corte académico, solo hasta el día de la instalación del biométrico la institución dio el permiso para la manipulación del rack donde se presentaron los siguientes inconvenientes:

- Para configurar el equipo a la red interna del lugar se necesita que el administrador de la red, asigne una IP fija, por medio de la cual se re direcciona el equipo. Es de aclarar que la institución cuenta con una IP fija pero ya está configurada y usada para las necesidades internas de la institución.

- No hay puerto libre y habilitado en el swicth para conectar el cable de red que enlaza el biométrico.

3.12. Posibles soluciones

- Realizar las diligencias con el proveedor de internet de la institución, para realizar la compra de una IP fija, la cual se le asignaría al equipo para obtención de datos de forma remota (en este caso desde el colegio DHG).

- Compra de un swicth para la habilitación del puerto necesario para el cable de red del dispositivo.

- Configuración de la red por parte del contratista del colegio ITSI, ya que es una red compleja que tiene su propio usuario administrador y sus puertos bloqueados.

- Asignación de un servidor con un punto de red configurado (También es necesario que el administrador de la red lo habilite) para descargar el software del biométrico e instalarlo y realizar pruebas.

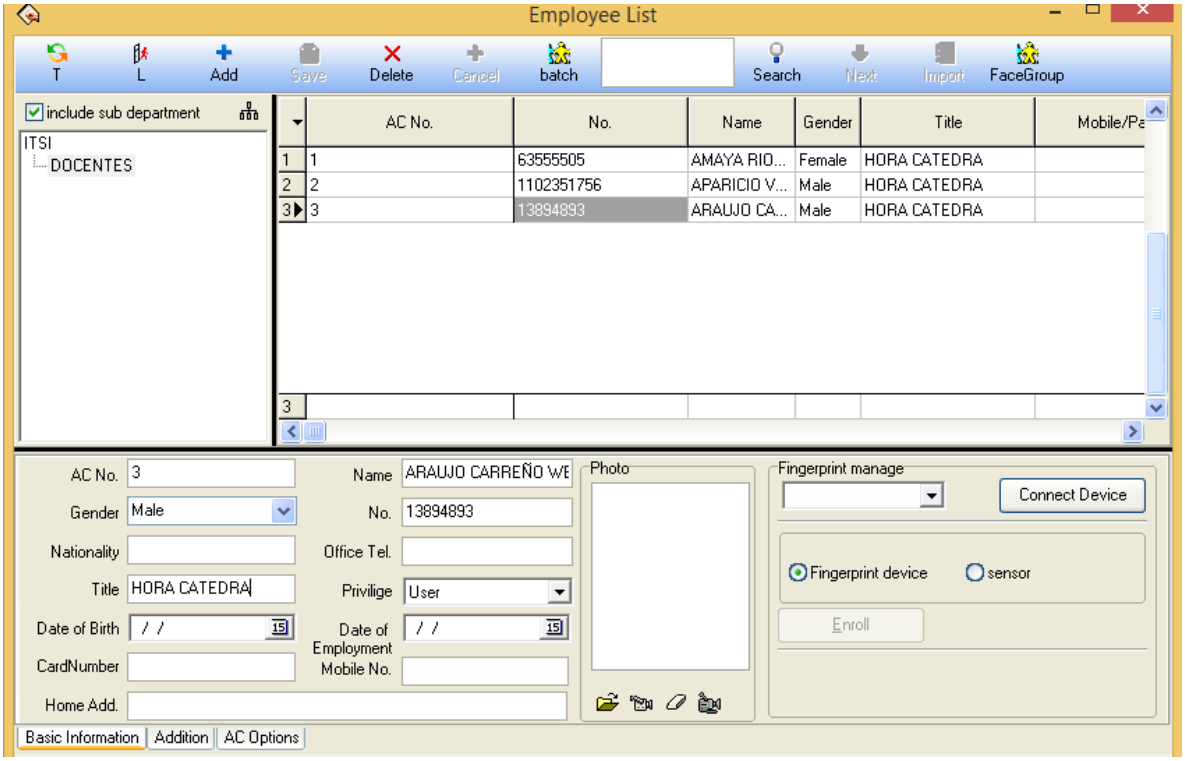
4. RESULTADOS

4.1. Registro de base de datos

Con el objetivo de alimentar la base de datos y realizar la entrega del biométrico, se solicitó a la universidad la lista de docentes que dictaran sus asignaturas en el ITSI, dicha información fue entregada para ser ajustada junto con sus respectivos horarios de ingreso y salida del plantel.

La siguiente es una ilustración de cómo se generan los perfiles de usuario e ingresos de los respectivos horarios. La base de datos está conformada con la siguiente información, como lo es: nombre, cedula, genero, fecha de contratación y privilegios (administrador o usuario).

Figura 13: Diligenciamiento base de datos docentes

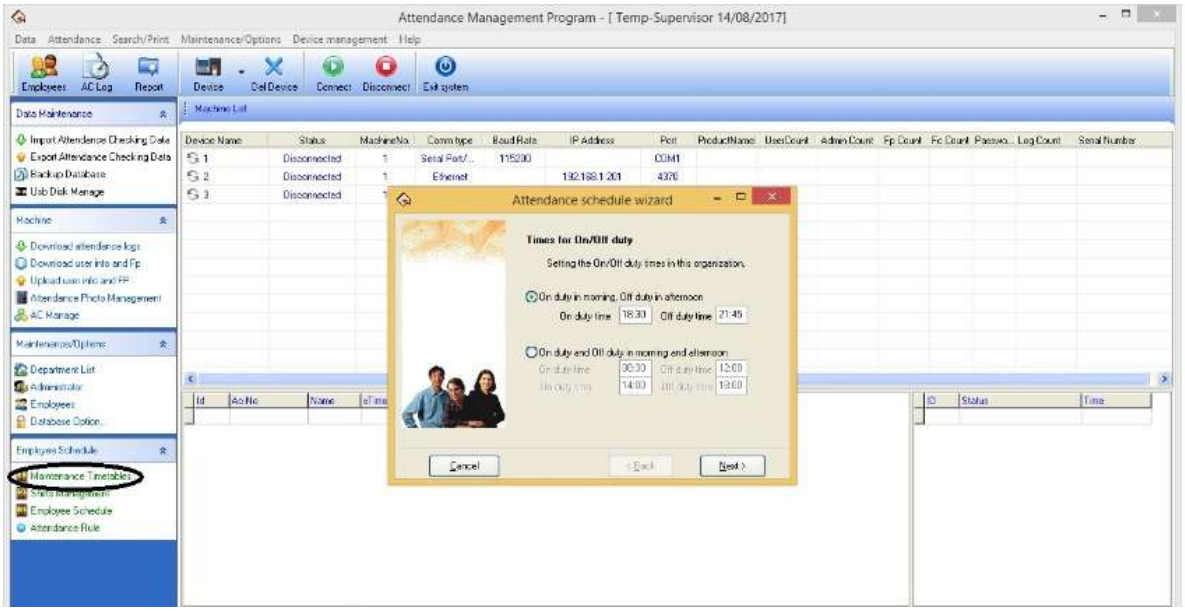


Fuente: Autor

Posteriormente se hace necesario la creación del horario en el cual se deberán registrar los docentes para lo cual seguimos los siguientes pasos:

4.2. Asignación de turno

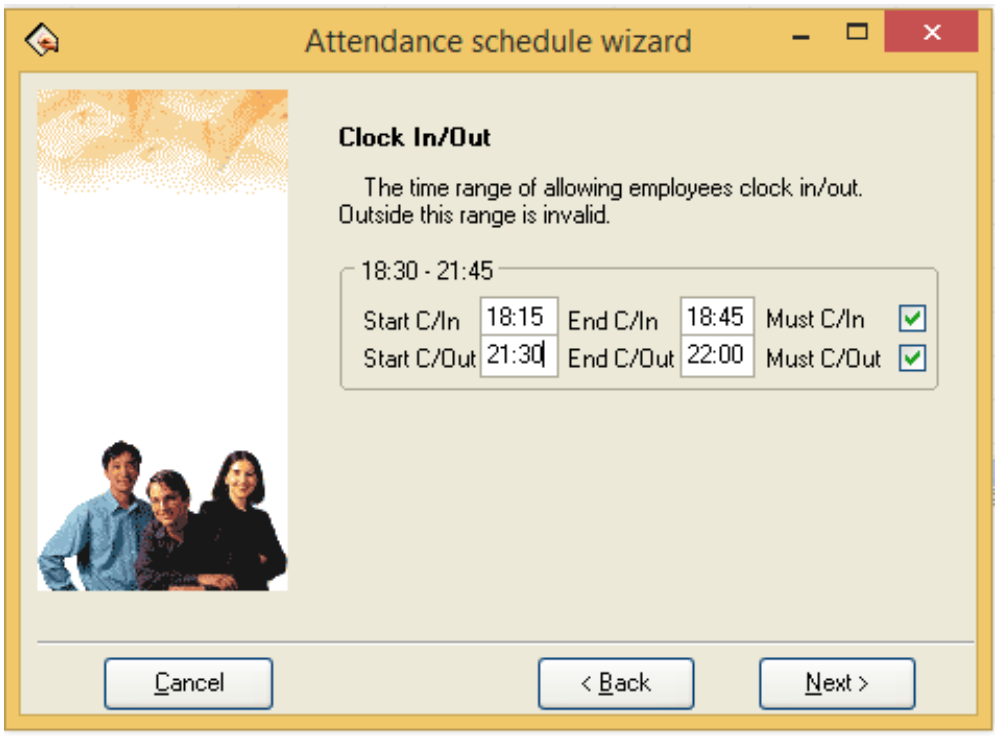
Figura 14: Turnos docentes



Fuente: Autor

Para realizar la asignación de los turnos se hace click en el área señalada en la figura 14 maintenance timetables, seguido se desplegara una ventana en la cual se escoge si son turnos con jornada en la mañana y en la tarde, como lo es en este caso de una sola jornada, seguido se ingresa la hora de inicio de la jornada y hora de salida.

Figura 15: Horarios docentes



Fuente: Autor

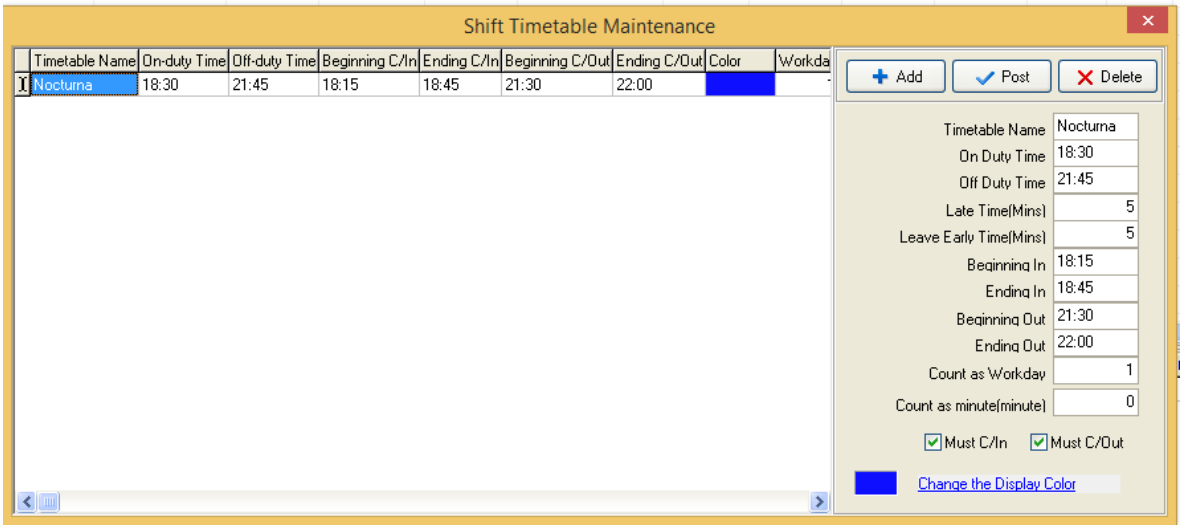
Posteriormente, se establece los tiempos en los cuales será válido el ingreso de los docentes, se asigna una ventana de tiempo de 30 minutos dentro de los cuales será válido el registro de ingreso, pasada esta ventana el dispositivo no tomara las huellas, es de resaltar que las ventanas de tiempo son modificables por parte de un usuario con privilegios de administrador, esto se evidencia en l figura 15.

Figura 16: Rangos de marcaje

Fuente: Autor

La figura 16 muestra el tiempo en el que se considera que el docente ha llegado temprano o tarde respectivamente. En este caso se da un rango de 5 minutos.

Figura 17: Ejemplo de horario para los docentes



Fuente: Autor

Los horarios que manejan los docentes de la institución están divididos en bloques de dos horas, un ejemplo de una jornada normal sería el mostrado en la figura 17.

5. CONCLUSIONES

Con la puesta en marcha del biométrico se logró disminuir los tiempos en la recolección de datos en la asistencia o insistencia de docentes, contribuyendo en una mejor organización y control en los tiempos de las jornadas. Este adelanto tecnológico incorporado en el plantel permite conocer la hora de entrada y salida de los docentes en horarios específicos ya que la información puede ser descargada en cualquier momento.

Es importante argumentar que con el objetivo que la información sea manejada desde un solo servidor, y que la misma esté a disposición en tiempo real, es necesario instalar un sistema que permita realizar la transmisión de los datos al DHG, por medio de una IP fija, En la investigación se planteó realizar dicho enlace pero debido a que la UTS sede I.T.S.I. no cuenta con los recursos para su instalación, la presente investigación no incorpora este proceso, pero si se deja la salvedad de la importancia del mismo. Así mismo es de aclarar que la sede I.T.S.I. cuenta con un punto de red pero el mismo es utilizado para configuraciones internas del plantel, imposibilitando la conexión de un cable de red que enlace el biométrico, por lo que se hace necesario considerar habilitar un nuevo punto y el pago mensual para el funcionamiento de los datos, logrando así la articulación entre sedes.

6. RECOMENDACIONES

- Realizar un mantenimiento preventivo del equipo de forma periódica, y que el mismo sea incorporado en los manuales o sistemas de la institución con el fin de que cuente con un seguimiento del equipo evitando el deterioro del mismo.

- Delegar el personal idóneo que tenga la función de administrador del biométrico, evitando malas manipulaciones y alteraciones o pérdida de los datos.

- Realizar seguimiento en la alimentación de la base de datos del biométrico, teniendo en cuenta fechas de contrato de los docentes y la depuración de la información que no se necesite en los siguientes periodos o semestres.

- Instalación de un nuevo punto de red en la sede I.T.S.I. logrando la transmisión de datos al DHG atreves de una IP fija.

- Articular atreves de la red todas las sedes de las unidades tecnológicas de Santander de la ciudad de Barrancabermeja, para manejar la base de datos en un solo PC, logrando un control y seguimiento en tiempo real de la misma.

7. REFERENCIAS BIBLIOGRÁFICAS

Leal, A., R., Bermudez Padilla., C., & Gonzalez. (2016). SELECCIÓN E IMPLEMENTACION DE UN SISTEMA DE REGISTRO Y CONTROL DE PERSONAL POR MEDIO DE HUELLA DACTILAR. 4. Barrancabermeja, Santander, Colombia: UNIDADES TECNOLOGICAS DE SANTANDER SEDE D.H.G.

Aguilera, M. M. (2012). *RECONOCIMIENTO BIOMÉTRICO BASADO EN IMÁGENES DE HUELLAS PALMARES.* Madrid: Universidad Autónoma de Madrid.

Alto nivel. (20 de 07 de 2017). *Claves de almacenamiento de datos para tu negocio.* Obtenido de http://www.altonivel.com.mx/33792-claves-de-almacenamiento-de-datos-para-tu-negocio/

Anonimo. (2013). *"RECONOCIMIENTO DE IDENTIDAD USANDO BIOMETRIA DE HUELLA Y ROSTRO PARA APLICACIONES DE SEGURIDAD.* INSTITUTO POLITÉCNICO NACIONAL . Culhuacan: instituto politecnico nacional. Obtenido de http://sappi.ipn.mx/cgpi/archivos_anexo/20070894_4392.pdf

Bulla Camacho, M. H., Rodriguez Gonzalez, H., & Gutierrez Ricardo, J. (2006). PROTOTIPO DE ACCESO A LA U.S.B. MEDIANTE IDENTIFICACIÓN BIOMÉTRICA. 34. Bogotá, Cundinamarca, Colombia: Universidad de San Buenaventura.

Ecured. (19 de 07 de 2017). *Reconocimiento de huella dactilar*. Obtenido de Ecured conocimiento para todos: https://www.ecured.cu/index.php/EcuRed:T%C3%A9rminos_y_Condiciones

Escorihuela, D. O. (2011). *MODELADO, DISEÑO E IMPLEMENTACION DE UNA PLATAFORMA BIOMETRICA.* Madrid: Universidad Carlos III de Madrid.

Giz Bueno , A., & Tolosa Borja, C. (15 de 03 de 2017). *SISTEMAS BIOMÉTRICOS.* Obtenido de www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

ISEC. (08 de 07 de 2017). *Soluciones que unen y comunucan al hombre*. Obtenido de http://www.isec.com.co/biometricos-lector-de-huella-digital/

Jairo Alonso Gómez Cano. (29 de 07 de 2017). *Sistema de huella digital para blibliotecas*. Obtenido de https://inbiosys.wordpress.com/nuestros-productos/sistemas-de-huella-digital/

Maya Vargas, A. (2013). *CONTROLES DE SEGURIDAD.* Bogota: Universidad Militar Nueva Granada. Obtenido de http://repository.unimilitar.edu.co/bitstream/10654/11168/1/MayaVargasAdriana2013.pdf

Narváez, C. (20 de 07 de 2017). *Protección de datos personales: listado de requisitos legales*. Obtenido de colombiadigital.net/opinion/columnistas/derecho-digital/item/8870-proteccion-de-datos-personales-listado-de-requisitos-legales.html

Pérez Porto , Julián; Merino, María. (20 de 07 de 2017). *Definiciones*. Obtenido de Registro de datos: http://definicion.de/registro-de-datos/

Purkyně, J. E. (1823). *Grupos de configuraciones principales de huellas dactilares.*

Ricardo, J. E. (2007). *ESTUDIO DE FACTIBILIDAD PARA EL CONTROL DE ACCESO BIOMÉTRICO,.* Bogota: Universidad de la Salle.

techtarget. (20 de 07 de 2017). *Información de identificación personal (PII)*. Obtenido de http://searchdatacenter.techtarget.com/es/definicion/Informacion-de-identificacion-personal-PII

UIB. (20 de 07 de 2017). *informatica: compenentes de un ordenador*. Obtenido de sites.google.com/site/partesdeunordenador/indicepartes/almacenamiento

UNAM, Facultad de Ingeniería. (08 de 07 de 2017). *redyseguridad*. Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/biometria/basesteoricas/caracteristicassistema.html

Velasquez Valencia, Jorge Eduardo; Linares Jaramillo, Alvaro Andres. (2013). *SOLUCIONES INTELIGENTES PARA EL CONTROL DE ACCESO FÍSICO.* UNIVERSIDAD TECNOLÓGICA DE PEREIRA , pereira. Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4090/0053682V434.pdf;jsessionid=E1B541804920831297AA673BB29CC702?sequence=1

Velasquez Valencia, Jorge Eduardo; Linares Jaramillo, Alvaro Andres. (2013). *SOLUCIONES INTELIGENTES PARA EL CONTROL DE ACCESO FÍSICO MEDIANTE EL USO DE TECNOLOGÍA BIOMÉTRICA.* Pereira: Universidad Tecnologica de Pereira.

ZKTeco (Alvaro Obregón). (2016). Manual de usurio. México D.F.

ZKTeco. (2015). *Hoja de espeficaciones Equipos K30.* México D.F.: ZKTeco.

8. ANEXOS

8.1. Instalación del biométrico

Figura 18 Biométrico instalado

Fuente: Autor

Figura 19: instalación de canaleta

Fuente: Autor

Figura 20: instalación cable de red

Fuente: Autor

Previa escogencia del lugar y a la altura establecida, se instala la canaleta por la cual pasara el cable de red del dispositivo, como se muestra en la figura 19. Una vez terminado este paso se instala el cable de red, que conectara el switch ubicado en coordinacion academica con el biometrico.

La figura 20 es la instalacion terminada del dispositivo, de tal forma de no entorpecer las labores de los celadores del ITSI.