UNIVERSIDAD LATINA

INCORPORADA A LA UNAM.

IMPLEMENTACION DE “BINSI“, PARA EL CONTROL DE ASISTENCIAS EN EL ÀREA DE ASUNTOS LEGALES SEGOB.

P R O Y E C T O

QUE PARA OBTENER EL GRADO DE:

LICENCIADO EN INFORMÁTICA

P R E S E N T A:

CARLOS ALBERTO VILLALOBOS REYES

ASESOR: MTRO. HUGO VELASQUEZ BRITO

MÉXICO, D.F. FEBRERO 2014.

AGRADECIMIENTOS

- *Gracias a Dios por ponerme en este camino, por ponerme a lado de gente que me impulsa a buscar nuevas metas y darme cuenta que todo esfuerzo tiene una recompensa.*

- *A mis padres no tengo más palabras para agradecerles todo lo que han hecho por mí, que no hay tiempo ni dinero con lo que yo les pueda pagar todo lo que me han dado, por enseñarme valores, que han formado la persona que ahora soy.*

- *A mi Tía July y a mi mamá Any les dedico esto y gracias por todo; siempre han sido un pilar en mi vida para lograr mis objetivos, me brindan consuelo, esperanza y amor.*

- *A mis Hermanos Jorge y Anne porque siempre están cuando los necesito, esto también es por ustedes.*

- *A mis niños Javi y Sofi por sus sonrisas por ser el motor que me impulsa a realizar muchas cosas y darles un gran ejemplo.*

- *A toda esa gente que conozco que me impulsa y que me retroalimenta de cosas que llenan mi corazón y alma.*

A todos y cada uno…..¡¡¡¡ Gracias!!!!!

ÍNDICE

Página

CAPÍTULO V
PROPUESTA

INTRODUCCION

Todas las huellas dactilares son únicas. La cuestión crítica es si podemos llegar a la información que es única y expresa de una manera que cumpla con el objetivo de la identificación positiva. Cómo llegar a expresar y la información única en la huella digital biométrica es nuestra misión y su motor de reconocimiento de huellas dactilares.

Cuando interactuamos con otras personas que estamos acostumbrados a identificar por su aspecto físico, su voz, u otros datos sensoriales. Cuando la prueba de necesidad identidad más allá de la apariencia física se obtiene una firma o nos fijamos en una foto de tarjeta de identificación. En el espacio cibernético, donde la necesidad de interactuar con un sistema digital o uno al otro a distancia, no tenemos esos medios de identificación disponibles. En casi todos los casos no podemos ver, oír, obtener una firma de la persona con la que estamos interactuando.

La biometría, es la medición de una característica física única, y es una solución ideal al problema de identificación digital. La biometría permite identificar a las personas mediantes estos sistemas, ya que atreves de estos sistemas de identificación de nosotros mismos en otros lados o hasta en el ciberespacio. Con los datos biométricos se pueden crear un personaje digital que haga e interactúe en el los espacios convenientes y de manera segura. De todos los datos biométricos, se incluida la cara, iris y escaneo de retina, la identificación de voz y otros, la huella dactilar es una de las más conveniente y fiable.

CAPÍTULO I.

METODOLOGIA

1.1 METODOLOGIA

Para la realización de registro de asistencia, se pretende la instalación del Sistema BINSI" PARA EL CONTROL DE ASISTENCIAS EN EL AREA DE ASUNTOS LEGALES SEGOB; se registra el número de empleado correspondiente a la huella digital de cada usuario. Este sistema cuenta con un software específico que facilita el proceso, ya que cuenta con un dispositivo que reconoce la huella y complementa con una base de datos.

El registro de la huella deberá registrarse 2 veces en este dispositivo para que no haya posibilidad de error ya que el usuario no coloca el dedo de igual manera cada vez que checa. El reloj hace reconocimiento de la huella no importando como coloca el dedo cada vez que se realiza la tarea.

- Se deberá registrar el número de empleado y huella digital de cada uno de los usuarios para incluirlos en la base de datos que el checador necesita para checar.

- Este proceso se puede hacer mediante un dispositivo conectado a la computadora en la que se tiene el programa del checador.

- El reloj checador cuenta con un programa que genera la base de datos. Al dar de alta la huella en el sistema, se genera un archivo único por empleado con todos sus datos.

- Diseño de sistema incluyendo el protocolo de comunicaciones necesario para su funcionamiento en la red de dispositivos controlados desde una PC.

- Ensayos de verificación del prototipo trabajando en un modo autónomo de red, pruebas de comunicación con la pc, depuración del sistema y del protocolo de comunicaciones.

- Desarrollo e implementación de la aplicación pc para la gestión de la red de dispositivos controladores de acceso.

- Puesta en marcha de la red gestionada por la aplicación desde la pc, pruebas y ajustes finales del sistema completo.

1.2 JUSTIFICACIÒN

El presente proyecta se enmarca dentro de las actividades de la Unidad de Asuntos Legales y Derechos Humanos nace el proyecto para desarrollar un sistema de control de acceso basado en la tecnología biométrica de huella dactilar.

Gracias al auge y madurez que ha alcanzado la tecnología de reconocimiento de huella dactilar, actualmente en el mercado están empezado a aparecer dispositivos que aplican esta tecnología biométrica para autenticar usuarios en acceso de inmuebles. Estos sistemas presentan una mejora de seguridad y comodidad frente a clásicos sistemas de control de acceso. Respecto a otros sistemas, esta tecnología al utilizar la identificación de la huella dactilar del usuario no es imprescindible emplear alguna otra tarea. También incrementa la seguridad de acceso.

1.3 OBJETIVO

En este trabajo se muestra el desarrollo del sistema BINSI en el que se describe las ideas en las que se han inspirado el mismo. Se ponen diferencias y alternativas que existen a la hora de llevar a un lenguaje conceptual una solución al problema, resuelto de manera brillante por la naturaleza en el caso de la raza humana.

El objetivo de este proyecto es la implementación de un sistema biométrico de autenticación, orientado a una aplicación de control de acceso, utilizando como características biométrica la huella digital de la persona. La propuesta de investigación y desarrollo en este tema surge en marco de diversas problemáticas que surgen en nuestra área de trabajo.

Por otro lado, uno de los objetivos de este proyecto es la acumulación de experiencia y de conocimiento, es por esto que nos enfocamos en realizar un trabajo riguroso y metodológico que pueda ser objeto de futuras extensiones. Se plantea un objetivo práctico en el desarrollo.

1.4 HIPOTESIS

El concepto de biometría se deriva de las palabras griegas BIOS (de vida) metron (de medida), este concepto no se puso en práctica hasta finales del siglo XIX, se bien se sabe que al menos desde el siglo XIV los comerciantes chinos estampaban las impresiones y huellas de la palma de la mano en papel con tinta para distinguirles.

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

Durante los últimos tiempos los investigadores del campo de la ciencia cognitiva han perseguido crear sistemas dotados de las habilidades humanas. Un sistema biométrico es todo aquel que realiza labores de biometría de manera automática. En otras palabras, se trata de sistemas basados en medir y analizar las características físicas y del comportamiento humano con el propósito de autentificación.

En la actualidad, los métodos más aceptados de identificación se basan en la colección de rastros dactilares. La mayoría de los países del mundo utilizan las huellas digitales como sistema práctico y seguro de identificación. Con el avance tecnológico nuevos instrumentos de verificación de huella digitales.

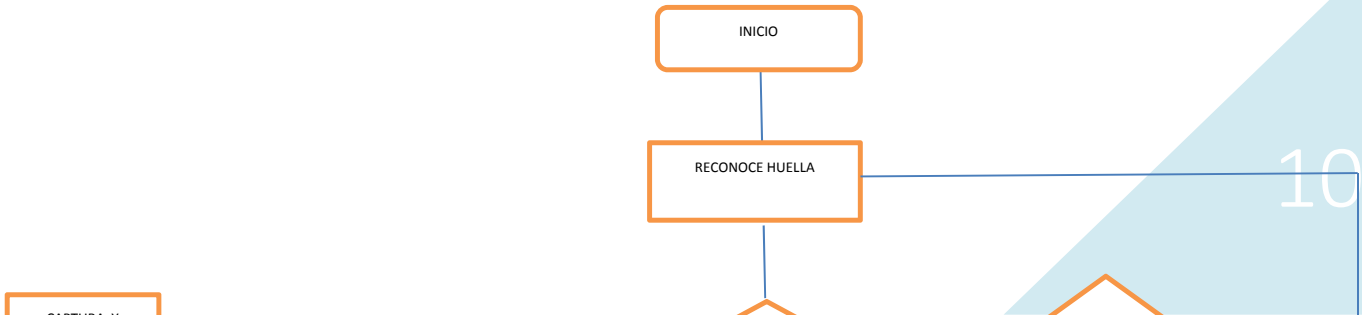
1.5 INSTRUMENTOS DE MEDICIÒN

Para desarrollar este proyecto y conseguir los objetivos mencionados anteriormente se han realizados las siguientes tarea.

- Estudio, valoración y elección de componentes principales del dispositivo controlador (lector de huella) que permita la gestión del sistema, así como la implementación del reconocimiento de huella dactilar.

- Inicio y desarrollo de los modelos preliminares para la estructura del dispositivo controlador, y pruebas de estos para su evaluación.

- Diseño hardware de la arquitectura de la placa madre del dispositivo controlador.



CAPÍTULO II

INTRODUCCIÓN A LOS SISTEMAS BIOMETRICOS

2.1 CONCEPTO
2.2. INTRODUCCION

En este capítulo se explicara la razón para la elección de los componentes o elementos principales y necesarios para la implementación de nuestro sistema de control de acceso. En este se emplea la tecnología de autenticación biométrica de huella dactilar, elemento fundamental de nuestro dispositivo de control de acceso.

Aquí se detallaran también las características y parámetros técnicos de esta tecnología, así como las necesidades del sistema, lo que será la columna vertebral de nuestro sistema de control de acceso.

Autenticación Biométrica de huella dactilar.

Dentro de este campo de reconocimiento de formas destacan las aplicaciones biométricas que consisten en la media, el procesamiento y análisis estadísticos de datos identificativos bilógicos de los seres humanos. Un sistema biométrico es esencialmente un sistema de reconocimiento de formas que reconocen a una persona mediante la autenticidad de características fisiológicas y comportamiento que posee. Un tema importante en el diseño de sistemas biométricos es determinar cómo va a ser reconocida cada persona. Dependiendo de cada contexto de la aplicación o de las circunstancias de empleo, un sistema biométrico puede tener dos modos de operación como sistema de verificación o de identificación.

Un sistema de identificación reconoce a una persona a través de la búsqueda en la base de datos de patrones de una coincidencia con el patrón capturado. Esta realiza comparaciones uno a muchos para establecer la identidad del sujeto (o el resultado de la búsqueda es negativo si el sujeto no está registrado en la base de datos).

El termino Autenticación es frecuentemente usado en el campo de estudio de sistema biométrico, a menudo como sinónimo de verificación, en realidad el lenguaje de las tecnologías de la información, autenticar a un usuario significa deja al sistema averiguar la identidad del usuario independientemente del modo.

Todo lo dicho se aplica a cualquier sistema de autenticación biométrica por lo que es válido, también para un sistema biométrico basado en la autenticación por huella dactilar, el cual es un caso particular de estos sistemas en el que las características y patrones biométricos se extraen de la huella dactilar de las personas, en lugar de otras características biométricas como son el rostro humano, en reconocimiento facial, el iris o retina, en reconocimiento ocular, o la forma de escribir en un teclado, como ejemplo de reconocimiento de la dinámica de un determinado comportamiento humano.

2.3 VENTAJAS DE LA BIOMETRIA

- Todo y cada uno de nosotros cuentan con diez huellas dactilares y cada una es única, diferente de otra persona, incluso los gemelos idénticos tiene huellas digitales únicas.

- A diferencia de las contraseñas, códigos, pin y las tarjetas inteligentes que se utilizan actualmente, nuestras huellas digitales son imposibles de olvidar o perder y pueden que nunca se las roben.

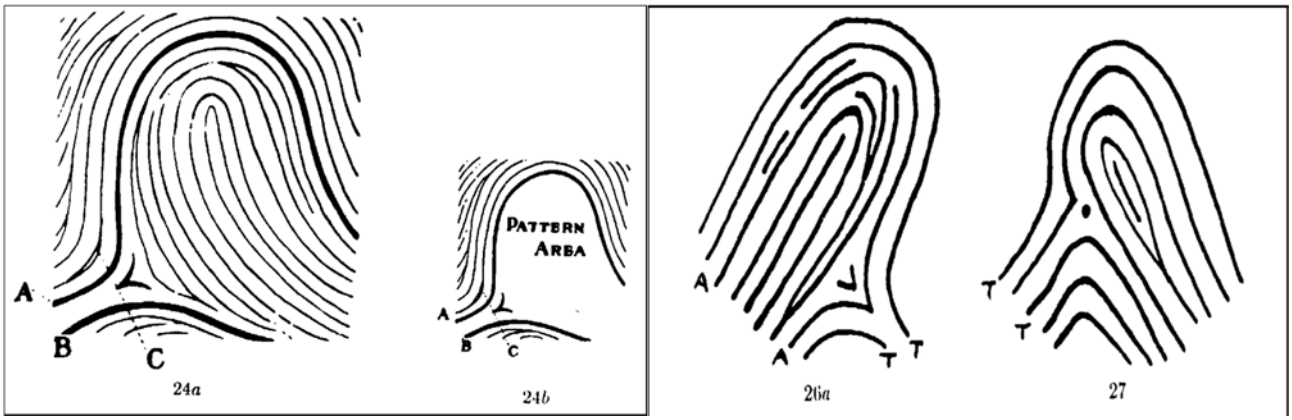
- Tenemos 10 huellas dactilares en contraposición a una sola voz, una cara o dos ojos.

- Las huellas dactilares se han utilizado durante siglos para la identificación y tenemos un importante base de datos, sobre el cual basar nuestra reivindicación de la singularidad de cada huella dactilar.

- Sabemos que la probabilidad de 2 huellas dactilares iguales es casi imposible.

2. 4 ASPECTOS BASICOS DE IDENTIFICACIÓN DE HUELLA DACTILAR

- La piel en las superficies interiores de nuestras manos, dedos, pies y de los de los dedos en los pies es “RIDGED” cubierto con las pautas plantadas concéntricos, a estas cordilleras se le llaman crestas de fricción y que sirven de hacer más fácil de entender o mantener los objetos y superficies sin deslizamiento.
- Se trata de numerosas y diferentes formas de crestas de fricción.
- Algunas de estas formas rotas y bifurcadas.
- Las huellas dactilares son extremadamente complejas.
- Se pueden clasificar determinadas características.



2.5 TERMINOLOGIA DE IDENTIFICACIÓN

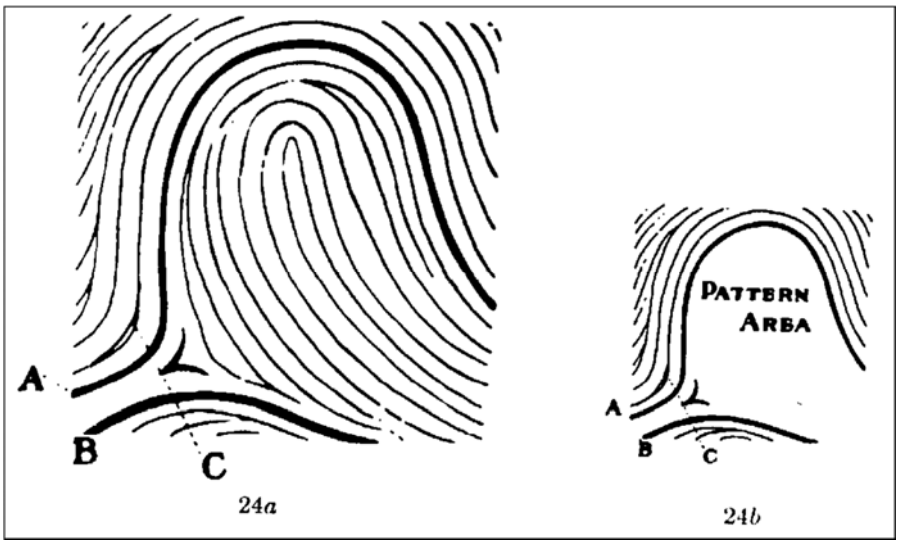
La terminología de identificación de huella digital es extremadamente compleja, esta tiene el fin de leer y clasificar determinadas características, en las cuales se han establecido una gran base de datos de impresión. Aunque algunas empresas de biometría no guardan imágenes de las huellas dactilares y no utilizan el mismo proceso para analizarla. Muchas de las metodologías que han sido establecidas a lo largo de años en la aplicación para algoritmos para la utilización de biometría digital.

Con este sistema se hace el uso de características de huellas digitales para el uso de identificación de individuos con las siguientes características y funciones estas características incluyen:

- Patrones básicos Ridge
- Tipos de Líneas
- Contar Ridge
- Plan Espacio
- Delta
- Tipo de Lineas

Las características locales son también conocidas como puntos de minutia, se trata de la pequeña características singulares de las cordilleras de huellas digitales que se utilizan para una identificación positiva. Es posible que dos o más personas tenga idénticas características mundiales pero todavía tiene diferentes huellas dactilares y cada una pose características locales minutia puntos que son diferentes de los demás.

El plan espacio es la parte de la huella digital que contiene todas las características



Algunas características son:

- Las huellas dactilares pueden ser leidas y clasificadas sobre la información base.
- Algunos puntos minutia pueden ser utilizados para el final de identificación
- Para identificar alguna diferencia significativa

Lo que se propone con el Sistema BINSI es utilizar un algoritmo que haga el reconocimiento de huella y no utilizar lo que las demás empresas en el mercado utilizan la las líneas de huella dactilar para así obtener la información. BINSI obtiene la mayor cantidad de información en el proceso de leer la huella dactilar.

- **El core point** se encuentra en el centro aproximadamente del dedo, este punto se utiliza como punto de referencia para la lectura y clasificación de la impresión.

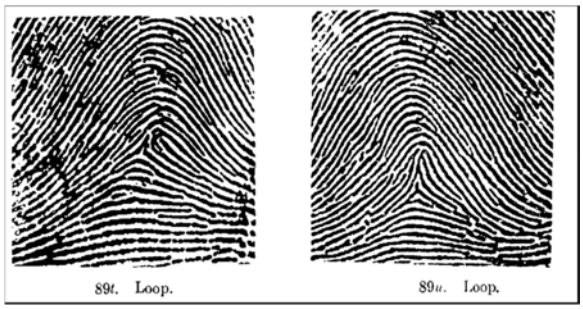
Tipo de líneas: son las dos cordilleras más lejanas que empiezan en forma paralela y divergen y rodean a la zona de patrón.

- **Delta**: es punto de la primera bifurcación que termina de forma abrupta, o la reunión de dos cordilleras más cercanas al centro de la divergencia de dos tipos de línea que se encuentran en el mismo nivel o directamente en punto delante de la divergencia. Se trata de un punto fijo de terminado para facilitar este proceso.
- **Ridge patrones Básicos:** a través de los años los que trabajan con huella dactilares han definidos las agrupaciones de impresiones sobre la base de patrones de la huella digital en las cordilleras. Esta clasificación hace más fácil de buscar en las grandes bases de datos de huellas dactilares. La cresta de patrones básicos no son suficientes para la identificación sino también ayuda a reducir la búsqueda. Ciertos productos son a base de óptica correlación de cresta mundial considera la identificación positiva debe basarse en verificación de minuta de puntos además de las características mundiales.

El nuevo paradigma digital para la identificación de huellas digitales utiliza muchos elementos del proceso de categorización que han estado vigentes durante años, así como algunos nuevos conceptos para la comprensión y la categorización de características mundiales. Además de la definición de pautas de cresta, BINSI ha determinado que hay ciertas formas de cresta para fluir alrededor de una huella dactilar, y que hay limitaciones de flujo de comportamiento puede ser explotado para su identificación. El reconocimiento de BINSI usa como como motor las características de patrones mundiales de cresta y el flujo de características para identificar a las personas. Hay una serie de pautas básicas tres de las más comunes son el lazo, arco y verticilo.

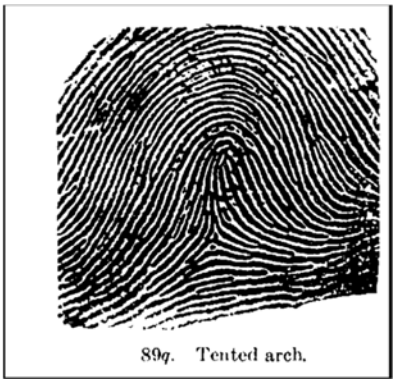
LOOP: Se caracteriza por que las crestas que forman su núcleo nacen en el costado izquierdo del dibujo y hacen un recorrido a la derecha, para dar vuelta sobre si misma y regresar al mismo punto. de partida .

89s. Loop.

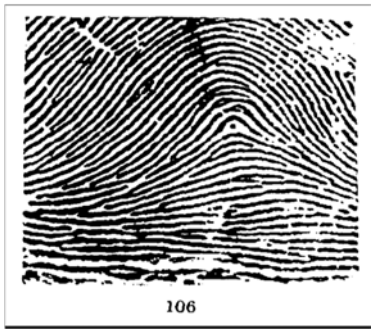


89t. Loop. 89u. Loop.

ARCH: Este dactilograma es uno de los tipos fundamentales, carece de puntos delta y de núcleo se caracteriza porque el comienzo las crestas son casi rectas y paulatinamente se van arqueando para dar la forma aproximada de un medio circulo.



89q. Tented arch.



106

VERTICILIO: Se denomina verticilo debido a que sus dibujos en muchos casos son similares a las flores; su características más importante es que cuenta con dos puntos Delta, uno del lado derecho y otro de lado izquierdo, sus núcleo puede adoptar formas circulares, elípticas y espirales. Se pueden encontrar verticilos con tres deltas llamados también trideltos, aunque esto sucede en poca frecuencia.

Este ocupa el 30% de todas las huellas dactilares y se define por los menos en una cordillera que hace un círculo completo.

PRESILLAS EXTERNAS: Al igual que las presillas Internas, cuenta con un punto Delta, pero está ubicada del lado izquierdo. Las crestas papilares que forman el núcleo nacen a la derecha y su recorrido es la izquierda para dar vueltas sobre si mismas y regresar al mismo punto de partida.

CAPÍTULO III

BINSI (SISTEMA INTEGRAL BEOMETRICO)

3.1 DEFINICIÓN DE CONTROL

Empecemos de donde viene la palabra control proviene del termino francés controle y significa comprobación, inspección, fiscalización o intervención. También puede hacer referencia al dominio, mando y preponderancia a la regulación sobre un sistema.

el control ha sido definido bajo dos grandes perspectivas, una perspectiva limitada y una perspectiva amplia. Desde la perspectiva limitada, el control se concibe como la verificación a posteriori de los resultados conseguidos en el seguimiento de los objetivos planteados y el control de gastos invertidos en el proceso realizado por los niveles directivos donde la estandarización en términos cuantitativos, forma parte central de la acción de control.

Bajo la perspectiva amplia, el control es concebido como la actividad no solo a nivel directivo, sino en todos los niveles y miembros de la entidad, orientando la organización hacia el cumplimiento de los objetivos propuestos bajo mecanismos de la medición cualitativos y cuantitativos. Este enfoque hace énfasis en los factores sociales y culturales presentes en contexto institucional ya que parte del principio es que el propio comportamiento individual quien define la última instancia la eficacia de los métodos de control elegidos en la dinámica de gestión.

Todo esto lleva a pensar que el control es un mecanismo que permite corregir desviaciones a través de indicadores cualitativos y cuantitativos dentro de un contexto social amplio, a fin

de logar el cumplimiento delos objetivos claves para el éxito organizacional, es decir el control se entiende no como el proceso netamente técnico de seguimiento, sino también como proceso informal donde se evalúan factores culturales, organizativos, humanos y grupales.

El control es una etapa primordial en la administración, pues aunque la empresa cuente con magníficos planes, una estructura organizacional adecuada y una dirección eficiente, el ejecutivo no podrá verificar cual es la situación real de la organización y no existe un mecanismo que cerciore e informe si los hechos van de acuerdo con los objetivos.

El concepto de control es muy general y puede ser utilizado en el contexto organizacional para evaluar el desempeño general frente un plan estratégico. A fin de incentivar que cada uno establezca una definición propia del concepto se revisara algunos planteamientos de varios estudiosos del tema:

- Henry farol: el control consiste en verificar si todo ocurre de conformidad con lo adoptado, con las instrucciones emitidas y con los principios establecidos. Tiene como fin señalar las debilidades y errores a fin de rectificarlos e impedir que se produzcan nuevamente.
- Robert B Buchele: el proceso de medir los actuales resultados en relación con los planes, diagnosticando la razón de las desviaciones y tomando las medidas correctivas necesarias.

La palabra control tiene muchas connotaciones y su significado depende de la función o de la tarea en que se aplique; puede ser atendida:

- Como la función administrativa que hace parte del proceso administrativo junto con la planeación, organización y dirección, y lo que la precede.
- Como los medios de regulación utilizados por un individuo, o empresa como determinadas tareas reguladoras que un controlador aplica en una empresa para acompañar y avalar su desempeño y orientar sus decisiones.
- También hay casos que la palabra control sirve para diseñar un sistema automático que mantenga un grado constante de flujo o de funcionamiento de sistema total; es el caso de procesamiento continuo y automático.

3.2 PROCESAMIENTO DE LA HUELLA DACTILAR

Los pasos para el procesamiento de la huella dactilar por un sistema automatizado de identificación de impresiones dactilares son:

1.- mejorar de la imagen: este proceso consiste en eliminar las zonas confusas de la imagen origina dejando solo zonas con información de máxima fiabilidad.

2.-Binarización: el objetivo de esta etapa es pasar la imagen original en tonos de gris, blanco y negro, reconstruyendo posibles cortes y mejorando la calidad global de la imagen.

3.-Adelgazamiento: con este proceso todas las crestas de las líneas dactilares tiene el mismo grosor haciendo que los puntos característicos de la huella dactilar se puede identificar con más facilidad.

4.-Extracción de puntos Característicos: a partir de la imagen adelgazada y el sistema es capaz de detectar y extraer la posición exacta de los puntos característicos. Dentro de esta etapa cabe destacar:

a) Construcción de un índice o vector: este es el proceso final que mediante algoritmos matemáticos completa la creación de un índice matemático, el cual constituye la esencia de la huella dactilar analizada, según las características consideradas, almacenando en forma de fichero.

b) Identificación y Verificación: Una vez que se tiene o vector de muchas huellas, el sistema es capaz de realizar búsquedas para verificar la identidad de una persona.

La extracción de puntos característicos es por lo tanto el proceso final que completa la obtención de la plantilla de la huella o patrón biométrico dactilar. La cantidad mínima de puntos característicos necesarios para proceder a comparaciones eficaces entre imágenes dactilares. La extracción de puntos característicos es un área en la que la investigación es continua y al día de hoy se puede llevar a cabo con diversas técnicas.

- Extracción de puntos característicos desde la imagen de la huella. En esta técnica se apuesta por hacer un pre procesado de la huella antes de detectar las características de la misma. Una vez hecho esto busca patrones a identificar sobre la huella pre procesada.

- En la cual la anchura de las crestas es de un pixel. El pre procesamiento de la huella hace que el sistema de extracción pueda trabajar con huellas con un amplio rango de cualidades. Esta es la técnica más clásica y típica dentro de la extracción de puntos característicos de huella dactilar.

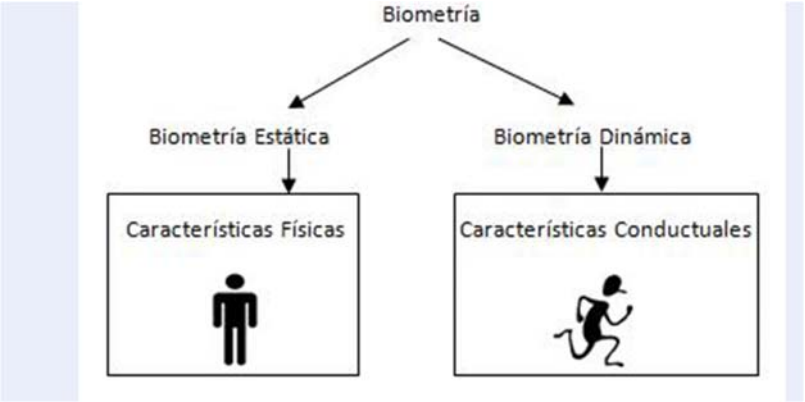
- Extracción de los puntos característicos mediante un banco de filtros. Esta es una técnica bastante novedosa y utiliza extracción de puntos característicos de huellas dactilares basada en filtro de banco. Esta técnica es usada para capturar información útil en las bandas de canales de imagen y descomponer la información en componentes ortogonales en términos de frecuencia espaciales. La técnica presenta buenas características de precisión, en cuanto a la velocidad de extracción presenta resultados pobres, siempre peores que las técnicas de extracción más clásica.

- Extracción de los puntos característicos sobre la propia imagen de la huella en escala de grises. En esta técnica se caracteriza por la realizar la extracción sobre la propia huella y no sobre la imagen adelgazada o mejorada de la misma. Esto presenta muchos inconvenientes y hace que la extracción se más lenta, inexacta y dependiente de la calidad de huella. Además trabajando directamente sobre la huella en escala de grises se detectaran un gran número de puntos característicos falsos y habrá otros muchos auténticos que no se detecten. Debido a estos inconvenientes la técnica no es muy utilizada.

3.3 CLASIFICACIÓN DE LOS SISTEMAS BIOMETRICOS

Como se han mencionado en varias ocasiones, la biometría es el estudio de métodos automáticos para el reconocimiento único de individuos basados en rasgos conductuales o físicos intrínsecos y dependiendo del tipo de características que utilicen para llevar a cabo

dicha identificación es que la biometría se divide en dos grandes tipos: Biometría estática y Biometría Dinámica.



La medición de las características físicas de individuo corresponde a la Biometría Estática. Los principales estudios y aplicaciones de esta rama de la biometría están basados en los sistemas biométricos de huellas dactilares, geometría de la mano.

3.4 PAPEL DE LOS ESTANDARES BIOMETRICOS

Actualmente, la mayoría del hardware y software relacionado con los distintos sistemas biométricos están basados en tecnología propietaria de las empresas que lo fabrican. Son varios aspectos en los que los dispositivos varían, por ejemplo la forma en que los sensores biométricos y los sistemas con aplicaciones se comunican, el método utilizado para extraer las características con información discriminante de las muestras biométricas (huellas digitales) que se toman y procesan en caso, las técnicas o métodos de comparación de los patrones, la longitud y el contenido de los patrones, incluidos el método de almacenamiento y recuperación de los datos biométricos.

Como consecuencia de esto, cuando una compañía decide por una determinada tecnología biométrica para integrar en algún producto o para o para producirla ella misma, queda atada a misma en el que el futuro pues si algún momento, decidiese incorporar nueva tecnología de esta naturaleza tendría que volver a implementar su sistema o al menos gran parte del mismo. Debido a la naturaleza emergente de esta tecnología y a la poca madurez de muchos productos de biometría, los desarrolladores de aplicaciones que hacen uso de la tecnología biométrica temen que las empresas fabricantes de dicha tecnología cambien de rumbo o modifiquen sus productos obligándose a tirar gran parte del trabajo que hayan realizado así como su dinero.

Sin embargo, se debe aclarar que el desarrollo de estándares biométricos y su adopción general no aseguran una total compatibilidad entre dispositivos y tecnologías y que, en muchos casos, seguirá siendo necesaria una adaptación de los antiguos sistemas o aplicaciones para que funcionen con los nuevos dispositivos o tecnología que se decida utilizar. Esto es debido a que los algoritmos y los procesos diseñados e implementados por los fabricantes de tecnología biométrica para la extracción de datos o muestras, el proceso de extracción de las características de las mismas, e incluso el proceso de autenticación biométrica del usuario difícilmente llegara a estándares biométricos permita a los desarrolladores de aplicaciones con tecnología biométrica puedan optar por un amplio rango de dispositivos y tecnologías intercambiables de una forma directa, es decir sin necesidad de las ya mencionadas adaptaciones, de ese modo los riesgos que se mencionaron se verán reducidos de forma significativa.

3.5 ESTANDARES BIOMETRICOS

BioAPI.

El consorcio BioAPI nace en Abril de 1998 durante la conferencia CardTech/SecureTech con el apoyo de algunas de las compañías informáticas más importantes a nivel internacional como IBM y Hewlett-Packard. La primera especificación apareció en Septiembre de 2000 y la especificación final en Marzo de 2001. La idea era desarrollar una alternativa a otras iniciativas de estandarización. BioAPI ha llegado a ser uno de los esfuerzos más relevantes en la generación de estándares biométricos con varios objetivos como: desarrollar una Interfaz de Programación de Aplicaciones (API por sus siglas en inglés) independiente del parámetro biométrico y del hardware de los distintos fabricantes, crear un estándar independiente del sistema operativo, trabajar de forma coordinada con desarrolladores e integradores de aplicaciones con elementos biométricos para generar una API de fácil uso y de fácil convivencia con otros estándares ya existentes, entre otros.

Desde un punto de vista general, BioAPI intenta estandarizar el modo en el que las aplicaciones se comunican con los dispositivos biométricos y la forma en la que los datos son almacenados y utilizados, ofreciendo a los desarrolladores un conjunto común de llamadas a funciones para interactuar modularmente con los distintos dispositivos biométricos, algoritmos, etc. Sin embargo, no pretende estandarizar el modo en el que los datos son generados por los dispositivos biométricos, ni entrometerse en los rasgos distintivos que define la tecnología biométrica de cada fabricante. El resultado de ello es que, en algunos casos, obliga a los usuarios a 're-entrenarse' en el uso de estos dispositivos.

Las funciones de BioAPI cubren aspectos como el entrenamiento, la verificación e identificación de usuarios, la captura de datos, el proceso de los mismos, la comparación de patrones y el almacenamiento de la información biométrica. Establece un alto nivel de abstracción que permite a los desarrolladores olvidarse de los detalles particulares de fabricación de los distintos productos y de las tecnologías empleadas por los diferentes fabricantes. Actualmente muy pocas soluciones en esta área son compatibles con BioAPI aunque es muy importante resaltar que es un estándar ampliamente aceptado por la industria biométrica, incluso es apoyado por agencias estatales como es el caso de Estados Unidos. Esta participación y apoyo por parte de tantos interlocutores ha prolongado el tiempo de desarrollo de este estándar, que tardó varios años en producir su versión 1.0. Esto puede convertirse en un problema a medio plazo ya que otros estándares están apareciendo con un mayor dinamismo y con un gran empuje, apoyados por otros grandes fabricantes de tecnología como es el caso de BAPI y Microsoft.

BAPI

BAPI es un nuevo estándar biométrico desarrollado y planeado por un vendedor de soluciones biométricas llamado I/O Software en lugar de un consorcio de compañías e instituciones como fue el caso de BioAPI. En Mayo de 2000, Microsoft licenció BAPI, aunque había sido uno de los primeros en apostar por BioAPI, con la intención de incluirlo en las futuras versiones de sus sistemas operativos (Windows). BAPI se fusionó con su predecesor BioAPI llegando casi a reemplazarlo. La idea de que la tecnología biométrica forme parte de un sistema operativo ha hecho madurar esta área tecnológica, dejando de ser considerada como una tecnología del futuro y formado parte de un panorama actual de posibilidades a tener en cuenta a la hora de desarrollar aplicaciones. Arrastrados por la iniciativa de Microsoft, otras compañías como Intel han apostado por BAPI, licenciando este estándar para incluirlo en sus plataformas PC móviles y dotarlas de aspectos de seguridad.

En la actualidad el mundo de los estándares biométricos se encuentra dividido entre BAPI (apoyado por el consorcio Microsoft / Intel, en el que han colaborado otras compañías que también participan en el consorcio BioAPI) y BioAPI (considerado como el estándar de facto por agencias del gobierno de Estados Unidos para sus aplicaciones de seguridad). Esto nos conduce a una situación indeseada, contraria a la propia naturaleza de los esfuerzos encaminados a la generación de un único estándar. En los próximos años, BioAPI y BAPI deberán tener que ser considerados por todos los desarrolladores de aplicaciones hasta que ambos converjan en un único y definitivo

CBEFF (Common Biometric Exchange File Format)

Se ha desarrollado un estándar conocido como Formato de Ficheros Común para el Intercambio Biométrico (CBEFF), cuyo objetivo es definir los formatos de los patrones biométricos para facilitar el acceso y el intercambio de diferentes tipos de datos biométricos a los sistemas que integran esta tecnología o entre diferentes componentes de un mismo sistema. CBEFF establece un formato para la cabecera de los ficheros definiendo campos obligatorios y opcionales que proporcionan elementos comunes (opciones de seguridad, de integridad de los datos, fecha de creación del fichero, firma, tipo de parámetro biométrico, etc) para el intercambio de información entre los dispositivos biométricos y los sistemas que hacen uso de los mismos, además favorece la interoperatividad entre las aplicaciones biométricas y los sistemas, simplifica la integración del software y el hardware, y posibilita la compatibilidad futura frente a los nuevos avances tecnológicos que se vayan produciendo. CBEFF no busca soluciones de interacción con los dispositivos o con los procesos, sino un método común para manejar los datos biométricos.

La definición e implementación de este estándar está siendo considerada para su incorporación en dispositivos como las tarjetas inteligentes bajo los auspicios del grupo de trabajo NIST/BC Biometric Interoperability, Performance and Assurance Working Group.

Actualmente BioAPI y CBEFF se han unido para construir un frente común a la estandarización biométrica. Muchos fabricantes están adoptando este estándar ofreciendo soluciones compatibles CBEFF, lo que implica que los ficheros que contienen los datos de los patrones biométricos tienen esta cabecera común.

NCITS-B10.8 (National Committee for Information Technology Standars)

Existe un comité acreditado por el Instituto Nacional de Estándares Americano (ANSI) conocido como NCITS (Comité Nacional para los Estándares en Tecnología de la Información) o X3, cuyo objetivo es generar estándares consensuados, de forma voluntaria, teniendo en cuenta el mercado, en las áreas de multimedia, intercomunicación entre sistemas de información y computadoras, medios de almacenamiento, bases de datos, seguridad y lenguajes de programación. Toda la documentación que genera se conoce como ANSI NCITS, está formado por 35 comités, uno de los cuales se llama B10, que se dedica al desarrollo de estándares para las tarjetas de identificación y otros dispositivos relacionado ellas. Dentro de B10 un primer grupo de trabajo es B10.8 que se especializa en las licencias de los conductores y tarjetas de identificación similares. Una fuerza de trabajo dentro de B10.8 ha desarrollado un estándar biométrico de gran interés como es la definición de un método común para extraer y procesar las características conocidas como minucias de la imagen de una huella digitalizada. De esta forma la introducción de esta información biométrica en las licencias de los conductores, con el fin de verificar que las licencias pertenecen a quien las porta, está cada vez más cerca.

CDSA / HRS (Common Data Security Architecture Specification / Human Recognition Services)

Es una arquitectura que se encuentra parcialmente involucrada en el desarrollo de estándares biométricos, fue creada por Intel en Diciembre de 1997 con la participación de Netscape, JP Morgan, Shell, IBM, Motorola y HP. El CDSA / HRS está desarrollando una herramienta de Software multiplataforma y segura para aplicaciones que incluyan elementos de comercio electrónico, comunicaciones y contenido digital. Trabajan directamente con el consorcio BioAPI con el fin de maximizar el consenso sobre la herramienta que está bajo desarrollo. El CDSA está desarrollando una API común a la que los programadores puedan añadir funcionalidad de autenticación. El componente HR es una extensión de la arquitectura propuesta por el CDSA relacionada directamente con el proceso de autenticación. La adopción de esta arquitectura puede ser una gran ayuda en el desarrollo de la industria biométrica, que vería a los distintos sistemas y tecnologías como parte de un todo.

HA-API (Human Authentication Application Program Interface)

El Consosrcio Biométrico americano (US Biometric Consortium) dirige, de forma coordinada con el gobierno americano, los esfuerzos en biometría que se llevan a cabo en Estados Unidos desde 1993. Su principal logro ha sido el desarrollo de una Interfaz de Programación de Aplicaciones para la Autenticación de Personas (HA-API). La primera especificación de esta API se anunció a finales de 1997.

El proyecto se divide, esencialmente, en dos partes: la creación de una API biométrica genérica junto con la implementación de una prueba de concepto y la integración de la API en sistemas comerciales de autenticación que funcionan en red

NBCT (United States National Biometric Test Center)

Este centro fue creado por el Consorcio Biométrico del Departamento de Defensa Americano a finales de 1997. Su principal objetivo es llevar más lejos los esfuerzos en estandarización biométrica relacionados por el gobierno de los Estados Unidos, generando procedimientos estándares de prueba o validación y midiendo objetivamente el rendimiento de los sistemas biométricos implementados existentes en el mercado. Esa metodología permitirá comparar los sistemas biométricos entre sí, ofreciendo información sobre el avance real de la tecnología

Los atentados ocurridos el 11 de Septiembre de 2001 en los Estados Unidos, causaron una reacción en el gobierno americano respecto al camino que se estaba siguiendo en el desarrollo de la tecnología biométrica, con el fin de asegurar que el uso de esta información y tecnología fuese el adecuado. En Noviembre de 2001 el comité Técnico M1 del INCITS fue creado con el objetivo de establecer un foro para el desarrollo de estándares biométricos genéricos dentro de los Estados Unidos. Este comité ha retomado todos los esfuerzos llevados a cabo con anterioridad en esta área incluidos BioAPI, CBEFF y la estandarización de los formatos de los patrones biométricos.

Uno de los objetivos del Comité M1 es acelerar el empleo de los, cada vez mejores, sistemas de autenticación biométrica para entornos gubernamentales donde la seguridad de la nación, la defensa y la prevención de la usurpación de identidades falsas dentro y fuera del país. M1 actúa como el grupo consejero en la organización internacional ISO/IEC JCT 1/SC 37 en temas biométricos. Es responsable de establecer la posición del gobierno americano y de realizar contribuciones al SC 37 en todas las reuniones de este comité internacional. Además, M1 ha creado a su vez cuatro grupos de trabajo para poder controlar la creciente actividad en biometría de un modo racional y especializado:

M1.1: especializado en formatos de intercambio de datos biométricos (Biometric Data Interchange Formats).

M1.2: dedicado a las interfaces biométricas con un enfoque técnico (Biometric Technical Interfaces).

M1.3: trabaja en la interoperabilidad en los sistemas (Biometric Profiles). s

M1.4: cuyo objetivo es la evaluación y la generación de informes en los sistemas biométricos (Biometric Performance Testing and Reporting).

La AMBI fue creada en 2007 por el Ingeniero Mexicano Humberto López Gallegos con el objetivo de promover el uso de mejores prácticas que pudieran contribuir a lograr una mayor eficiencia y seguridad en el uso masivo de soluciones biométricas e identificación así como posicionar los desarrollos hechos en México en otros países, principalmente en Estados Unidos, en Europa y especialmente en Latinoamérica. Otro aspecto que el Ingeniero y actual presidente de la Asociación consideró crucial para su creación es el marco jurídico alrededor del uso de tecnología biométrica puesto que no existe nada escrito que regule en México el uso de los datos biométricos de las personas por lo que una de las iniciativas de la AMBI es la de participar activamente en la generación de estándares y normas de identificación para uso masivo de esta tecnología no solo en México sino en muchos otros países, convirtiendo a México en un modelo a seguir en esta disciplina.

La AMBI, cuenta con el apoyo de compañías como Bioscrypt, LG Iris, SAGEM, Digital Persona, Crossmatch, L1, Quometrics, HID, Kimaldi, Ingressio y Nitgen y tiene como misión la consolidación de la industria de tecnología biométrica e identificación conduciendo foros de discusión, coadyuvar como el brazo tecnológico de las principales asociaciones de verificación de identidad a nivel internacional, generar y divulgar masivamente contenidos relevantes al aprovechamiento de las tecnologías biométricas.

Entre los servicios que ofrece la AMBI se encuentran el Análisis de desempeño de Identificación, Certificación de Aplicaciones, Capacitación especializada a través de cursos básicos de biométrica con la posibilidad de tomarlos directamente con el fabricante de alguna tecnología biométrica, Asesorías especializadas para proyectos de Identificación, los cuales se pueden solicitar a la página de Internet de la Asociación , sin embargo para que la solicitud de servicio sea procesada se deberá de ser miembro de la AMBI.

Por el momento, y a pesar de contar con el apoyo de las compañías ya mencionadas, la AMBI no ha desarrollado ningún estándar para el uso de tecnología biométrica en el país y tampoco ha participado en la creación y/o mejora de estándares internacionales. En la página de Internet de la Asociación no se da información acerca de cuál es el plan o estrategia que la AMBI está llevando a cabo o implementará en un futuro para participar en la creación de estándares de manera nacional e internacional.

Norma Oficial Mexicana.

Conforme a la Ley Federal sobre Metrología y Normalización una Norma Oficial Mexicana es la regulación técnica de observancia obligatoria expedida por las dependencias competentes, conforme a las finalidades establecidas en el artículo 40, que establece reglas, especificaciones, atributos, directrices, características o prescripciones aplicables a un producto, proceso, instalación, sistema, actividad, servicio o método de producción u operación, así como, aquellas relativas a terminología, simbología, embalaje, marcado o etiquetado y las que se refieran a su cumplimiento o aplicación.

En materia de normalización esta ley tiene como objetivos:

1. Fomentar la transparencia y eficiencia en la elaboración y observancia de normas oficiales mexicanas y normas mexicanas. 2.

Instituir la Comisión Nacional de Normalización para que coadyuve en las actividades que sobre normalización corresponde realizar a las distintas dependencias de la administración pública federal.

3. Establecer un procedimiento uniforme para la elaboración de normas oficiales mexicanas por las dependencias de la administración pública federal.

4. Promover la concurrencia de los sectores público, privado, científico y de consumidores en la elaboración y observancia de normas oficiales mexicanas y normas mexicanas.

5. Coordinar las actividades de normalización, certificación, verificación y laboratorios de prueba de las dependencias de administración pública federal.

6. Establecer el sistema nacional de acreditamiento de organismos de normalización y de certificación, unidades de verificación y de laboratorios de prueba y de calibración.

Las normas mexicanas son elaboradas por los organismos nacionales de normalización, y a falta de estos, será la Secretaría de Economía la responsable de su elaboración, en términos de lo dispuesto por los artículos 51-A y 51-B de la Ley Federal sobre Metrología y Normalización.

Es necesario resaltar que las normas mexicanas son de aplicación voluntaria, salvo en los casos en que los particulares manifiesten que sus productos, procesos o servicios son conformes con las mismas y sin perjuicio de que las dependencias requieran en una norma oficial mexicana su observancia para fines determinados. El campo de aplicación de estas normas puede ser nacional, regional o local.

Existen algunos distribuidores de tecnología biométrica en México que aseguran cumplir con la Norma Oficial Mexicana, sin embargo no existe una NOM que abarque las reglas, especificaciones y atributos que deben cumplir estas tecnologías por separado o en conjunto. Las características que los distribuidores de este tipo de tecnología ofrecen a los consumidores abarcan características de suministro de voltaje y corriente, temperatura, humedad, las funciones para las cuales fue diseñada la tecnología, sus aplicaciones, y las normas que estos productos cumplen, que en su mayoría son normas Internacionales, por ejemplo normas de Comunicación como la FCC (Federal Comunications Commission) o de calidad como la ISO 9000, más nunca se mencionan los estándares internacionales y/o nacionales bajo los cuáles son creados y distribuidos los productos.

CAPÍTULO IV

BINSI (SISTEMA INTEGRAL BEOMETRICO)

4. 1 DEFINICIÓN DE BINSI

Es un sistema Biométrico que proporciona resultados precisos, razonables, permanentes y fáciles de recopilar y medir. Debe proporcionar resultados precisos bajo diversas circunstancias del entorno y no debe ser fácil de engañar, y su aspecto más importante es su aceptación para el público general, por razones evidentes.

Es decir, este sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada.

Algunas de estas características importantes de este tipo de sistema son:

Cualquier proceso de identificación personal que puede ser comprendido mediante un modelo simplificado. Este postula la existencia de tres indicadores que definen el proceso de identificación:

1.- conocimiento: la persona tiene conocimiento (un código)

2.- posesión: la persona posee un objeto (una tarjeta)

3.- Característica: la persona tiene una característica que puede ser verificada (una de sus huellas dactilares)

Cada uno de los indicadores anteriores genera una estrategia básica para el proceso de identificación personal, además pueden ser combinados con el objeto de alcanzar grados de seguridad más elevados y brindar, de esta forma, diferentes niveles de protección. Distintas situaciones requieren diferentes soluciones para la labor de identificación personal. Por ejemplo, con relación al grado de seguridad, se debe considerar el valor que está siendo protegido así como los diversos tipos de amenaza. También es importante considerar la reacción de los usuarios y el costo del proceso.

Característica de un indicador biométrico.

Un indicador biométrico es alguna característica con la que se pueda realizar biometría, cualquier indicador debe cumplir los siguientes requerimientos:

1.-Universalidad: cualquier persona posee esa característica

2.-Permanencia: la característica no cambia en el tiempo.

3.- Unicidad: la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña.

4.-Cuantificación: la característica puede ser medida en forma cuantitativa.

Los requerimientos anteriores sirven como criterio para descartar o aprobar a alguna característica como indicador biométrico. Luego de seleccionar algún indicador que satisfaga los requerimientos antes señalados. Es necesario imponer restricciones prácticas sobre el sistema que tendrá como misión recibir y procesar a estos indicadores.

4. 2 CARACTERÍSTICA DE BINSI

Las características básicas que un sistema biométrico para identificación de personal debe cumplir puede expresarse mediante las restricciones que deben ser satisfechas. Ellas apuntan, básicamente, a la obtención de un sistema biométrico con utilidad práctica. Las restricciones antes señaladas apuntan a que el sistema considere:

1.- el desempeño, se refiere a la exactitud, la rapidez, y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales u operacionales. El objetivo de esta restricción es comprobar si este sistema posee exactitud y rapidez aceptable con un requerimiento de recursos razonable.

2.- la aceptabilidad, que indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria. Es claro que el sistema no debe representar peligro alguno para los usuarios y debe inspirar confianza a los mismos. Factores psicológicos pueden afectar esta última característica.

3.- la fiabilidad, que refleja cuan fácil es burla al sistema. El sistema biométrico debe reconocer características de una persona viva, pues es posible crear dedos de latex,etc. Algunos sistemas incorporan métodos para determinar si la característica bajo estudio corresponde o no ala de una persona viva. Los métodos empleados son ingeniosos y usualmente más simples de lo podría imaginar.

Arquitectura de un sistema biométrico para identificación personal.

Los primeros dispositivos poseen tres componentes básicos, el primero se encarga de la adquisición análoga o digital de algún indicador biométrico de una persona, como por ejemplo, la adquisición de la imagen de la huella dactilar mediante un escáner. El segundo maneja la compresión, procesamiento, almacenamiento y comparación de los datos adquiridos con los datos almacenados.

El tercer componente establece una interfaz con aplicaciones ubicadas en el mismo sistema. La arquitectura típica de un sistema biométrico, esta se puede entenderse conceptualmente como dos módulos:

1.- Modulo de inscripción

2.- Modulo de identificación

El módulo de inscripción se encarga de adquirir y almacenar la información proveniente del indicador biométrico con el objeto de poder contrastar a esta con la proporcionada en ingresos posteriores al sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características.

El primero se encarga de adquirir datos relativos al indicador biométrico elegido y entregar una representación en formato digital de este. El segundo extrae, a partir de la salida del lector, características representativas del indicador. El conjunto de características anterior, que será almacenado en una base de datos central u otro medio recibirá el nombre de template. En otras palabras un template es la información representativa del indicador biométrico que se encuentra almacenda y que será utilizada en las labores de identificación al ser comparada con la información proveniente del indicador biométrico en punto de acceso.

El módulo de identificación es el responsable del reconocimiento de individuos, por ejemplo es una aplicación de control de acceso. El proceso de identificación comienza cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital, para que a continuación el extractor de características produzca una representación compacta con el mismo formato templates. La representación resultante denomida query es enviada al comparador de características que confronta a este con uno o varios templates para establecer la identidad.

El conjunto de procesos realizados por el módulo de inscripción recibe el nombre de fase de inscripción, mientras que los procesos realizados por el módulo de identificación reciben la denominación de fase operacional.

RATINGS

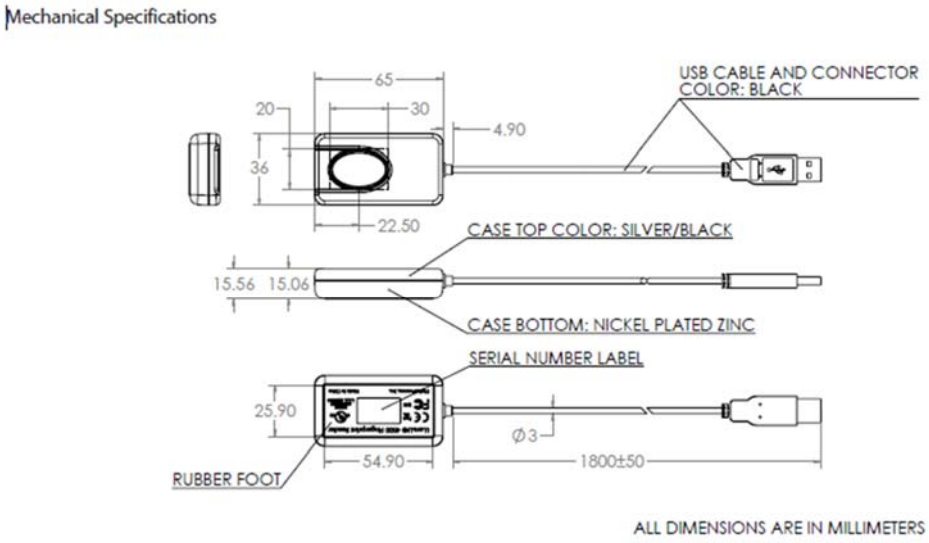
Supply Voltage	5.0V ±5% supplied by USB
Supply Current—scanning	< 100 mA (Typical)
Supply Current—idle mode	120 mA (Typical)
Supply Current—suspend mode	< 0.5 mA (Maximum)
ESD Susceptibility	>15 kV, mounted in case
Temperature, Operating	0 - 40 C
Humidity, Operating	20% - 80% non-condensing
Temperature, Storage	-10 - 60 C
Humidity, Storage	20% - 90% non-condensing
Scan Data	8-bit grayscale
Standards Compliance	FCC Class B, CE, ICES, BSMI, MIC, USB, WHQL
Weight	105 grams
Interface	USB 2.0 Full-speed High Power Device

Data subject to change without notice.

Las características Mecánicas del Sistema Binsi son:

- en primer lugar registra una o más huellas dactilares.
- El sistema ahorra suficiente información única acerca de la huella dactilar.
- Crea una plantilla de modo lector para poder identificarse
- La huella digital no se almacena, su huella digital no puede ser reconstruida a partir de la plantilla que se creó y la queda almacenada.
- Cuando la personas se registren en el lector de huella digital se compara su huella con la plantilla creada durante el proceso de registro.

- Si hay información coincidente suficiente, usted estará autenticado sino el sistema nos pedirá que se haga su registro mediante un password.



Entre otros aspectos más importantes a analizar en este equipo, se consideran:

a) Fiabilidad: se suelen denominar también como rendimiento (performance) o nivel de exactitud. Referido al comportamiento de un sistema o dispositivo, se define como la probabilidad de que el dispositivo desarrolle determina función, bajo ciertas condiciones y durante un periodo de tiempo determinado. Esta característica hace referencia a la precisión del reconocimiento, los recursos requeridos y el entorno operativo. Los indicadores habitualmente usados para medir esta característica son ; la tasa de falsa aceptaciones que es la probabilidad de un sistema biométrico falle a la hora de identificar a un individuo autorizado.

b) Resistencia a ataques. Se suele denominar también como resistencia del sistema biométrico a ser burlado. El término se refiere a la preparación y disposición que se hace anticipadamente para evitar el riesgo ante posibles intentos de violación del sistema.

c) Aceptabilidad. Las pruebas de aprobación tiene como fin validar que el sistema cumple con los requisitos básicos de funcionamiento esperando y permitiendo que el usuario determine la aceptación del sistema. Por este motivo, estas pruebas son realizadas por el usuario final, durante este periodo de tiempo, debe plantear todas las deficiencias o errores que se encuentren antes de dar por aprobado el sistema definitivamente, significa que el grado de aceptación de las personas en base, al que hecho que no perjudique a las personas.

d) Costo aceptable. Los componentes del costo en cualquier sistema biométrico incluyendo hardware y software asociado para capturar la biometría, investigación y testeo del sistema biométrico, instalación, encargado de implementación, montaje, conexión e integración del sistema de usuarios, capacitación de los mismos, alternativas para usuarios que no puedan registrarse, proceso de excepción del sistema, administración de la base de datos y poder de procesamiento del programa de respaldo.

e) No intrusividad. Un sistema biométrico es no intrusivo si el individuo no necesita contacto físico con un sensor o no tiene una connotación negativa, es decir, los datos pueden ser adquiridos, incluso, sin que el sujeto se percate de ello. Por el contrario, un sistema biométrico es intrusivo si necesita que el individuo toque un sensor, se coloque un sensor cerca de su cuerpo o participe de una manera que no es confortable desde un sentido emocional o psicológico.

Por otro lado, se prestara especial atención a los actores que serán parte de la implementación. Para los empleados, las soluciones basadas en biometría, pueden en algunos de los casos originar nuevos paradigmas respecto de la invasión a la privacidad de cada individuo.

En este proyecto, los dispositivos biométricos, solo se utilizan con fines administrativos como ser el seguimiento de entradas y salidas del personal para calcular las horas efectivas de trabajo y llevar un informe.

Se propone utilizar BINSI como dispositivo más fiable, además este dispositivo se personalizara para adecuarse a los procedimientos de entrada- salida para poder colectar, no solo la información referente a horarios de acceso de las personas, sino también, información estadística sobre el funcionamiento de este dispositivo que permita por un lado calcular indicadores de fiabilidad de los dispositivos.

Beneficiarios.

Como beneficiario primario de este proyecto, se tiene al personal de la Unidad de Asuntos Legales y Derechos Humanos, sin embargo es intención aplicar los resultados de otras áreas y otras instituciones públicas.

Además, la investigación de los dispositivos biométricos y en particular el estudio comparativo presentado, permitirá ofrecer a diferentes empresas de la región, soluciones de identificación para aquellas áreas críticas de las organizaciones que así lo requieran.

Relevancia.

Las instituciones pertenecientes al Gobierno Federal, han planteado como objetivo prioritario incrementar la vinculación con la comunidad con el fin de mantener un contacto más fluido, transparentar la gestión y poder canalizar mas eficientemente las inquietudes que surgen y dar pronto respuesta a sus necesidades. En este sentido, la utilización de las herramientas informáticas, deben jugar un rol importante como medio de comunicación.

No hay duda que la demanda social de información crece y que la mencionada transparencia representada cada vez más un compromiso de calidad en la gestión. Los espacios digitales están siendo gran oportunidad para divulgar información mediante el acceso en línea a documentos públicos y abriendo espacios de interacción antes impensados o inviables. El valor de la participación depende de la calidad de la información y no hay duda que este reto importante para los actores públicos. Además, en la medida que produce más participación, esta genera proximidad entre la administración y los ciudadanos y, a su vez confianza en las instituciones. La confianza con las instituciones se gana asegurando que los ciudadanos estén informados implicados e influyentes.

Así se encuentran implementados, aplicativos que permiten a los ciudadanos, realizar trámites “on line” utilizando para ello, las conexiones web (consulta de expedientes, presentación de declaraciones juradas, guías de trámites, etc.) no cabe duda que los servicios brindados a estos usuarios, deben encontrarse operativos en todo momento y responder eficientemente a los requerimientos por los cuales son utilizados.

La importancia de este proyecto tiene relación con la mejora directa de la seguridad de la información de esta área, en lo que se refiere al control de acceso de las personas destina para albergar los servidores donde se encuentra alojada esta información.

Además los resultados obtenidos del análisis, así como también, la experiencia de la implementación, permitirá brindar asesoramiento y servicios en sistemas biométricos para la reproducción de esta solución en distintos entes gubernamentales.

4.3 ESTUDIO DE FACTIBILIDAD

Los avances tecnológicos con los que se relaciona la gente hoy en día están sujetos a cambios constantes, por tal razón motivan a las diferentes entidades o personas a estar a la vanguardia.

Es importante que una institución este consiente de este avance, compare el nivel tecnológico está ubicada y esté dispuesta a realizar los cambios necesarios. La tecnología brinda herramientas para establecer distintos niveles de seguridad en empresas contra fenómenos naturaleza, seguridad informática e identificación y acceso personal.

Enfocado con respecto a la identificación y acceso de personal, las compañías están implementando sistemas que faciliten el acceso con información propia de cada usuario, dentro del campo existen varias alternativas que brindan soluciones para cada una de las necesidades, cabe mencionar métodos como (escaneo de huella digital) escaneo de iris, reconocimiento de voz y reconocimiento a través de tarjetas magnéticas.

La identificación biométrica es uno de los avances más importantes dentro del control y reconocimiento de personal perteneciente a una identidad sin importar su actividad económica, por tal motivo es necesario conocer a que se refiere cuando se habla de biometría.

El concepto de biometría proviene de la palabra bio (vida) y metria (medida), por lo tanto con que ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona.

La biometría es una tecnología basada en el reconocimiento de una característica de seguridad y en reconocimiento de característica física e intransferible de las personas, como por ejemplo la huella digital. Todos los seres humanos tenemos características morfológicas únicas que nos diferencian. La forma de la cara, la geometría de partes de nuestro cuerpo como las manos, nuestros ojos y tal vez la más conocida, la huella digital, son algunos rasgos que nos diferencian del resto de los humanos.

La medición biometría se ha venido estudiando desde tiempo atrás y es considerada en la actualidad como el método ideal de identificación humana. Estos avances en la identificación de huellas han abierto un gran campo en área de seguridad. Muchos sistemas requieren el ingreso masivo de personal a instalaciones en donde algunas personas deben acceder o ser restringidas. Los sistemas de identificación dactilar presentan una solución a este problema.

4. 3 PROPOSITO Y ALCANCES DEL PROYECTO.

Este estudio proveerá de información de factibilidad técnica económica y normativa sobre BINSI.

En el estudio técnico se propone el control de acceso a dos tipos de usuarios:

- Control de acceso a personal de la U.A.L.D.H
- Ingreso a vigilante

En el estudio de control de acceso biométrico se requiere adquirir conocimientos de tecnologías que van a ser implementadas que permitan escoger una serie de alternativas que guiaran al proyecto por el camino más viable sin incurrir en lo exagerado dando como escogido métodos que no puedan estar al alcance de quienes pretenden desarrollarlo, permitiendo motivar el empleo de estos métodos en las instituciones que lo requieran.

Dentro de las ventajas en la implementación de control de acceso biométrico encontramos:

- Elimina las suplantaciones de identidad de los empleados.
- Organiza las horas de ingreso y salida de los empleados.
- Disminuye costos de funcionamiento.
- No existe riesgos de falsificación.
- El medio de identificación es única y personal.
- Método seguro de identificación, pues no existe dos huellas digitales iguales en el mundo.
- Bajo costo de implementación permitiendo instalaciones en ciertas etapas interactuando con otros tipos de controles de seguridad.

4.4.1 MARCO REFERENCIAL.

Dentro de los términos más relevantes que se mencionan en el desarrollo de este diseño se encuentra el significado de la biometría que no es más que la medida de un patrón único en cada ser humano para este caso será la huella digital.

La criptologia que es un método milenario utilizado en las tecnologías actuales para disfrazar datos a los que solamente cierta cantidad de personas podrá tener acceso por medio del cifrado de los datos en cuestión.

Cuando se hace referencia a los dispositivos captadores son aquellos encargados del reconocimiento de la huella y envió de los datos con los que los usuarios se validaran o no dentro de la institución, este dispositivo hace parte del hardware o parte física del cual se compone el control de acceso.

Por otra parte es importante hablar sobre el hardware y el software, que en este caso es la parte lógica o intangible del prototipo dentro de este sistema se encuentra la base de datos, motores de búsqueda (encargado de buscar y comparar en la base datos el tren de bis proveniente del lector de huellas) y programa para la inserción de cada huella digital.

Para que exista una debida transferencia de datos entre el software y el hardware es necesario la utilización de protocolos de comunicación que se encargaran de que ambas partes se entiendan, realizando la transferencia de diferentes niveles de voltaje a niveles lógicos de 0 voltios (nivel bajo) y 5 voltios (nivel alto) así se garantiza que se lleven a cabo las acciones para las que el sistema fue diseñado.

También se pueden encontrar los elementos actuadores finales que se encargan del accionamiento de motores, electroimanes o solenoides para el movimiento de barras físicas, las cuales impiden que alguien pueda entrar a la institución sin antes de hacer su reconocimiento.

Otro concepto de gran importancia dentro de los sistemas de seguridad basados en identificación biométrica son los dispositivos de señalización audio-visual que permite al usuario conocer en qué estado está el proceso de validación para su acceso. Se hacen referencia a dispositivos que generan señales lumínicas (semáforo) y auditivas (buzzer) así el usuario puede reconocer si su validación dentro del sistema fue exitosa o no.

El software y el hardware siempre estará interactuando uno con respecto al otro, esto quiere decir que si uno falla el otro también y todo el sistema saldrá de su correcto funcionamiento.

4.4.2 MARCO TEORICO.

Los orígenes de la biometría se remontan a los años setenta, cuando la empresa NEC comienza a trabajar junto al FBI en algunos estudios de como automatizar biométricamente algunas características del ser humano. De esa forma se comienza a desarrollar una serie de algoritmos matemáticos con la finalidad de representar, por ejemplo, una huella dactilar. Cabe mencionar que aún no se ha comprobado que existan dos huellas digitales totalmente iguales.

Estos sistemas incluyen un dispositivo de captación que en segundos obtiene una muestra biométrica de la persona y compara con una base de datos, donde se analiza si corresponde o no a la identidad de la persona en cuestión. La inserción de todas estas tecnologías y métodos automáticos generan cambios en la manera de vivir de las personas.

La forma en que el mundo ha ido automatizándose ha sido a través de los sistemas de seguridad donde la prioridad de los sectores en el mundo ha ido cambiando de tal forma que la eficiencia y la efectividad ha sido enfocadas en la medida que se posee un buen sistema de cómputo para prestar mejor servicio, así como los sistemas de seguridad han ido evolucionando de lo digital o lo biométrico.

Para proteger la privacidad de las personas ha sido necesario idear toda una nueva infraestructura que aunque ha costado millones, en estos momentos se están desarrollando tecnologías basadas en la biometría como pueden ser los patrones de huella digitales.

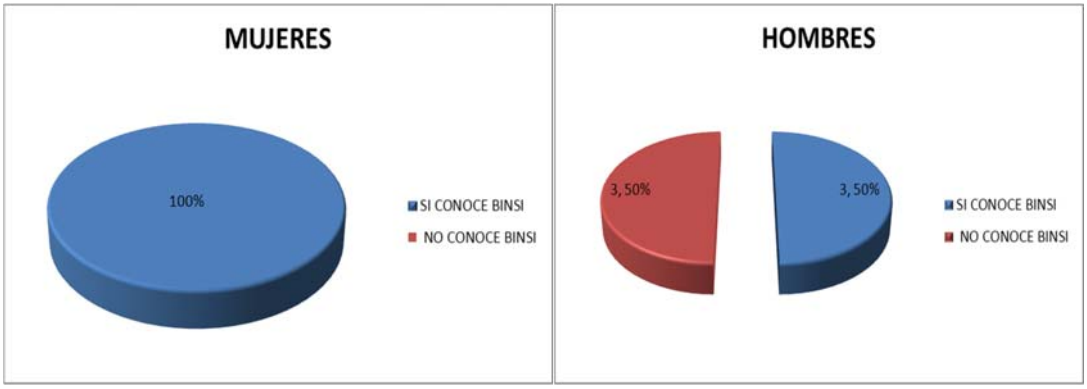
Los sistemas biométricos de seguridad están basados en documentos, archivos de información relacionada con la identidad de las personas, estableciendo los patrones necesarios para el desarrollo de esta tecnología. Estos métodos biométricos ya están siendo utilizados en varios ambientes y principalmente con el propósito de reemplazar a los que ya existen como password, tarjetas, etc.

4.4.3 EVALUACION TECNICA

Existen diferentes métodos para desarrollar soluciones de control de acceso en este caso acceso a un sector, las características que hacen parte de estas soluciones cambian unas con respecto a las otras por este motivo no todas son las más optimas o menos vulnerables, dentro de estos métodos se encuentran los lectores de códigos de barras, validación por medio de tarjetas magnéticas, tarjetas inteligentes y tarjetas de proximidad.
La mayoría están remplazándose, pues ahora se implementan sistemas que brinden un mayor grado de seguridad en comparación con sistemas que no son eficientes y se prestan a vulnerabilidad mayor. Puesto que todas necesitan de un papel o cartón plástico para la autenticación. Los elementos físicos a los que se hacen referencia están expuestos a hurtos o perdidas ocasionales esto conlleva a suplantaciones de personas.

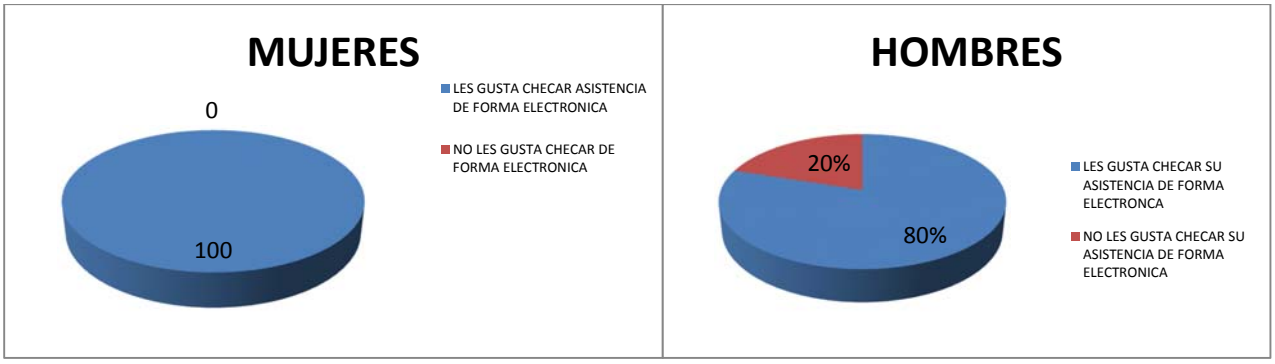
BINSI se enfocó en un sistema de control de acceso biométrico debido a que posee un grado de vulneración muy baja, ya que el came o llave de acceso la tenemos incorporada dentro de nosotros o es propia de cada uno, este sistema tiene un costo razonable teniendo en cuenta el nivel de seguridad que se presta.

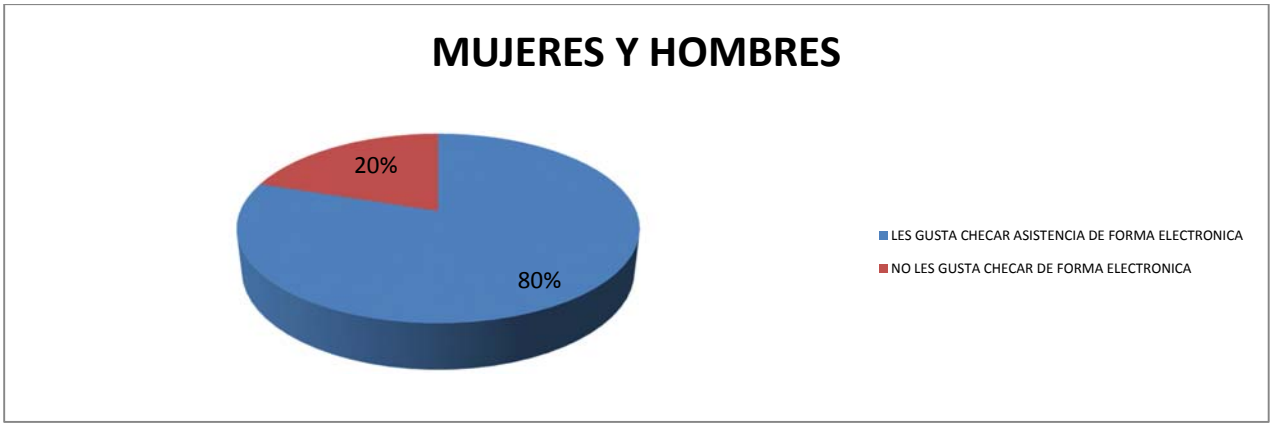
GRAFICA 1.- ¿Usted ha escuchado hablar de (BINSI) Sistema Integral Biometrico?



En esta gráfica, se determina que el 100% de las mujeres y el 50% de los hombre conocen a BINSI Sistema Integral Biométrico, por lo que el total de una población de 10 Empleados, el 70% conoce esta aplicación, reportando un resultado favorable para el objetivo del tema propuesto.

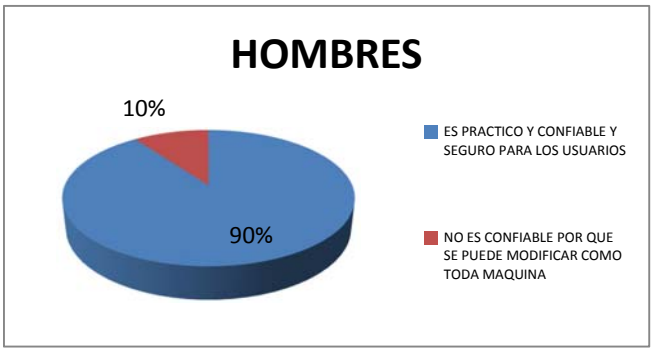
GRAFICA 2.-¿Le gustaría checar su asistencia en forma Electrónica?





En esta gráfica, se determina que el 100% de las mujeres y el 80% de los hombre les gusta checar de manera electrónica, por lo que el total de una población de 10 Empleados, el 80% no les incomoda o les gusta checar de manera electrónica y solo el 20% no les gusta hacer este registro de manera electrónica, reportando un resultado favorable para el objetivo del tema propuesto.

GRAFICA 3.- Que piensas de un sistema electrónico para checar su asistencia?

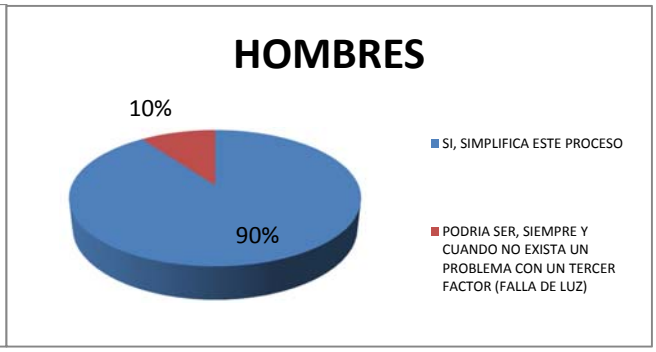


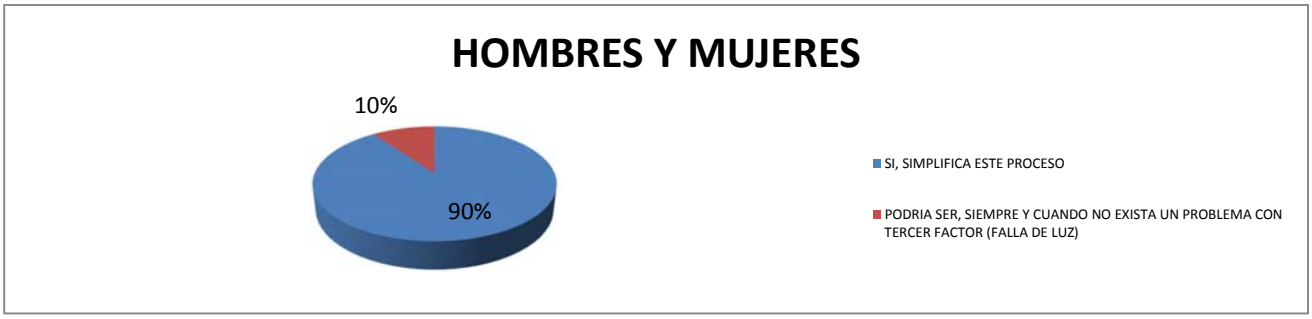
En esta gráfica, se determina que el 100% de las mujeres y el 90% de los hombre creen que es una herramienta es practica confiable y seguro checar de manera electrónica, por lo que el total de una población de 10 Empleados, el 90% creen que es una herramienta práctica, confiable y seguro checar de manera electrónica y solo el 10% crees que es una herramienta no confiable por que como todo equipo electrónico puede ser manipulable, reportando un resultado favorable para el objetivo del tema propuesto.

GRAFICA 4.- El uso de algún equipo tecnológico te facilita el uso del Sistema Biométrico?

En esta gráfica, se determina que el 100% de las mujeres y el 90% de los hombre creen el uso de cualquier herramienta tecnológica facilita el uso del sistema biométrico, por lo que el total de una población de 10 Empleados, el 90% creen que el uso de cualquier herramienta tecnológica hace más práctica el uso del sistema biométrico, reportando un resultado favorable para el objetivo del tema propuesto.

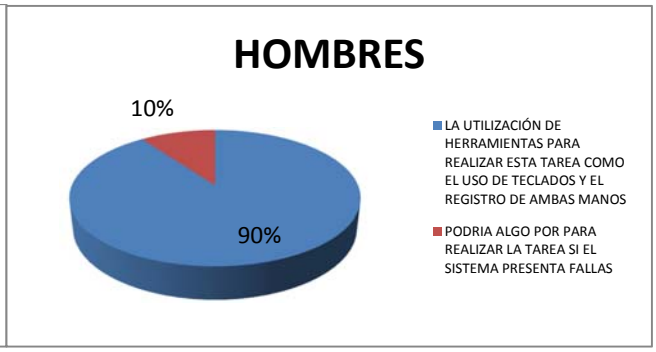
Grafica 5.-Estas de acuerdo que este sistema simplifique el registro de entrada-salida?

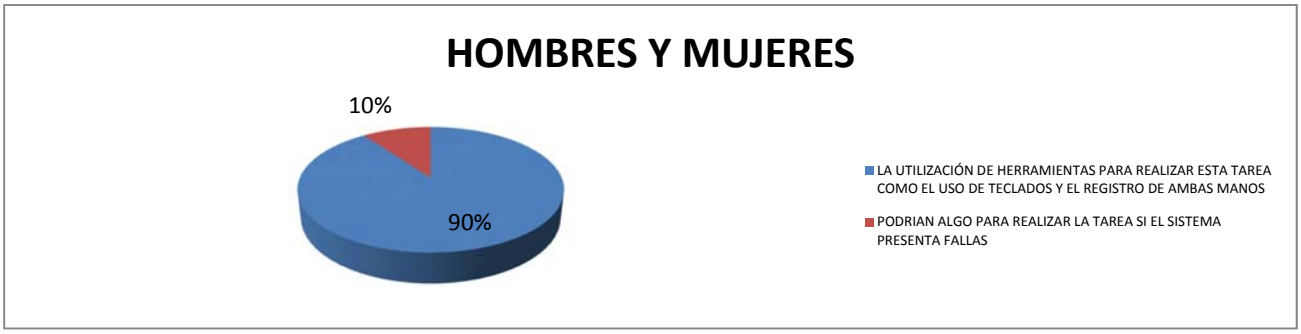




En esta gráfica, se determina que el 100% de las mujeres y el 90% de los hombre creen que haría más fácil este proceso, por lo que el total de una población de 10 Empleados, el 90% creen que el uso de este facilitaría la tarea de registro de entrada- salida y solo el 10% tendría problemas si se presentara alguna falla en este sistema ya que por experiencias pasadas tenían algún método que no podría tener falla por la intervención de un tercer elemento que pueda impedir este proceso, reportando un resultado favorable para el objetivo del tema propuesto.

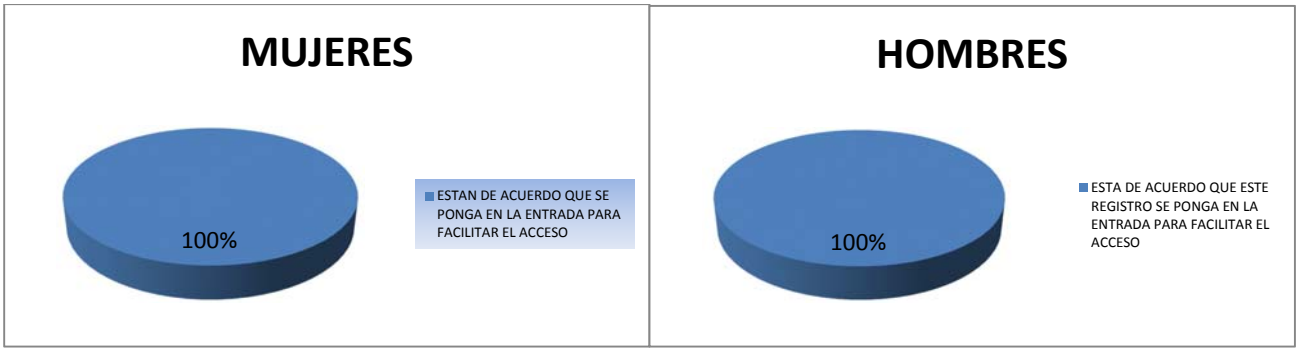
Grafica 6.- Que podría aportar los usuarios para el buen funcionamiento de este sistema?





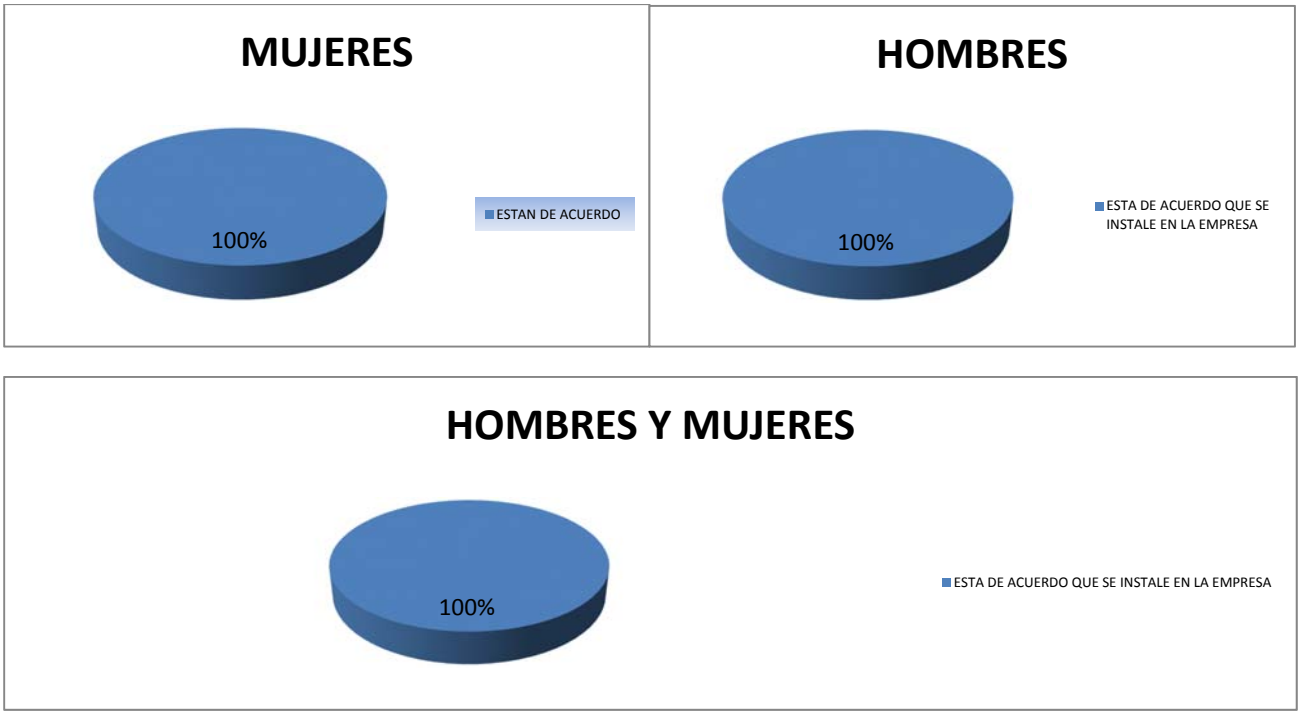
En esta gráfica, se determina que el 100% de las mujeres y el 90% de los hombre creen que haría falta algunas herramientas que facilitaría más este proceso, por lo que el total de una población de 10 Empleados, el 90% creen que el uso de estas herramientas facilitaría la tarea de registro de entrada-salida como poner teclados alfa numéricos para que así los usuarios al poner su número de empleado puedan registrar esta tarea y solo el 10% tendría problemas si se presentara alguna falla en este sistema y cree que algún método antes conocido por él podría hacer esta tarea por que no confía en el uso de tecnología, reportando un resultado favorable para el objetivo del tema propuesto.

Grafica 7.- En que parte de tu Área laboral pondrías el sistema?



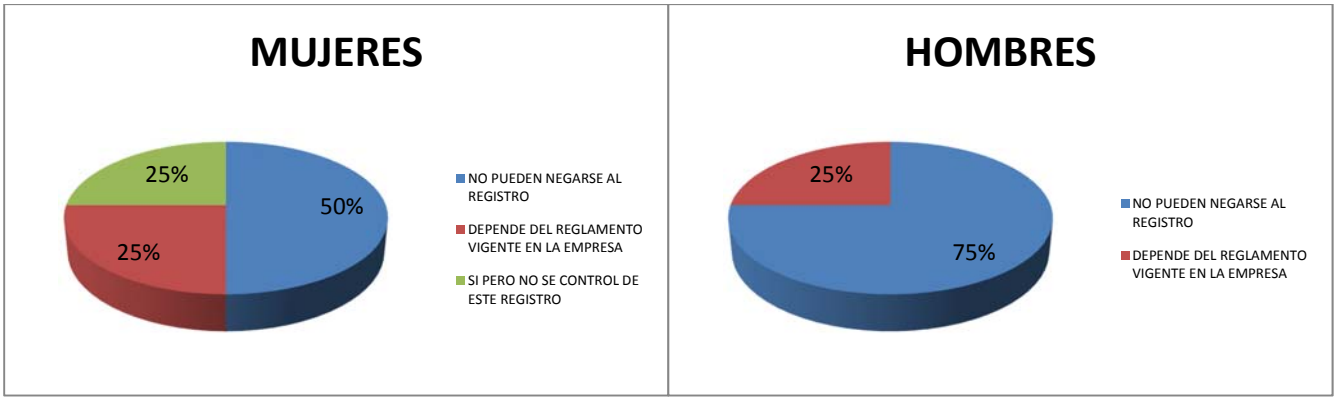
En esta gráfica, se determina que el 100% de las mujeres y el 100% de los hombre creen que el sistema biométrico que registra entrada-salida se instalara en la entrada ya que para ellos facilitaría este proceso, por lo que el total de una población de 10 Empleados, el 100% creen que el uso de estas herramientas facilitaría la tarea de registro de entrada- salida, reportando un resultado favorable para el objetivo del tema propuesto.

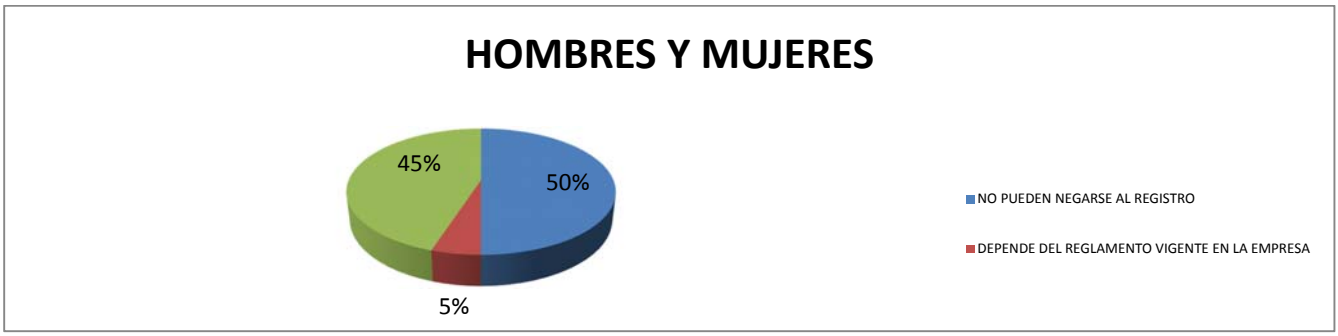
Grafica 8.- Estas de acuerdo que se instale este sistema en la empresa?



En esta gráfica, se determina que el 100% de las mujeres y el 100% de los hombre están de acuerdo en la instalación de sistema biométrico, por lo que el total de una población de 10 Empleados, el 100% creen que el uso de estas herramientas facilitaría la tarea de registro así como en la certeza de la información, reportando un resultado favorable para el objetivo del tema propuesto.

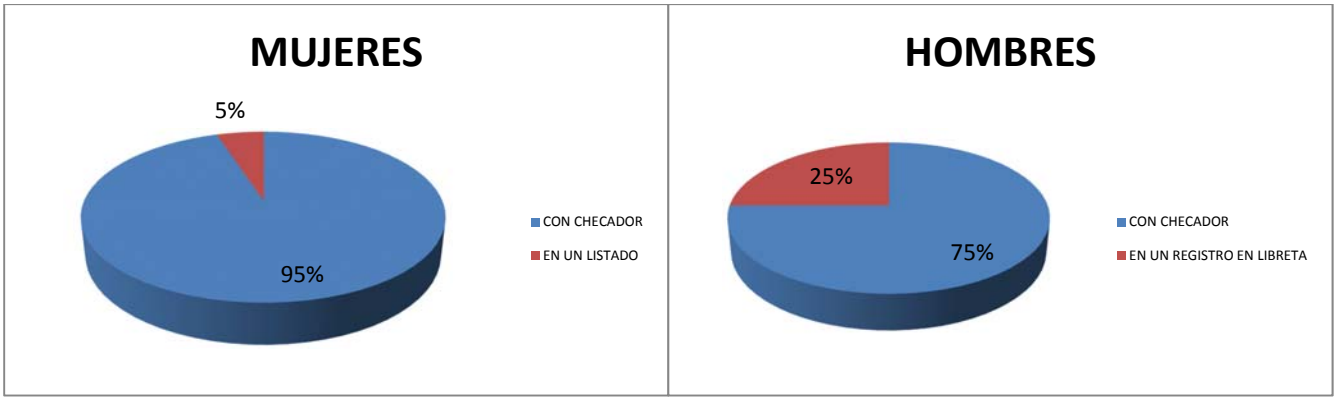
Grafica9.- Un usuario puede negarse a realizar este registro?



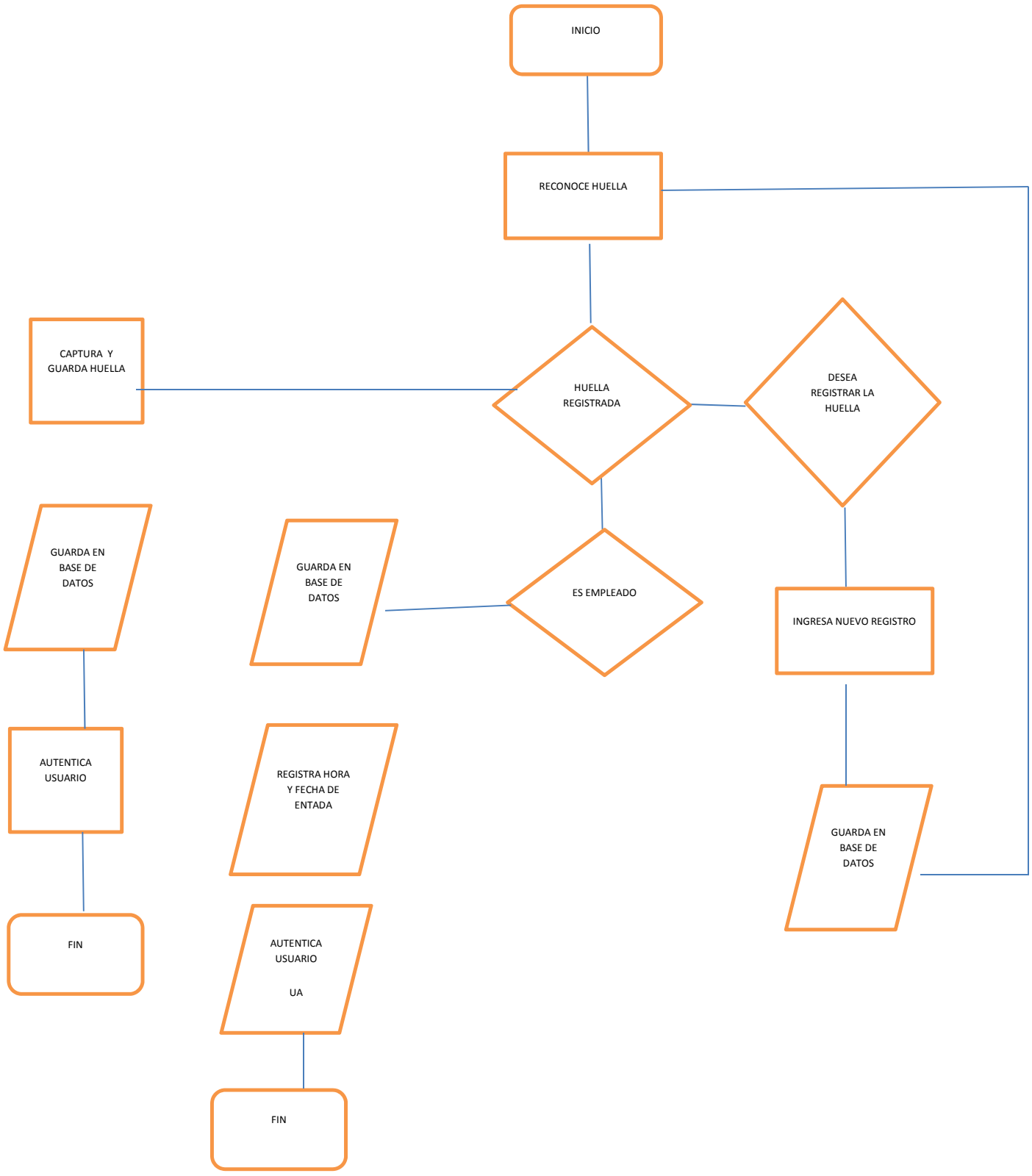


En esta gráfica, se determina que el 25% de las mujeres hacen referencia de si están obligadas a checar su entrada y salida y fundamentan esto en el reglamento vigente de la empresa, el otro 25% comenta en que no se registrarían pero ven que no se tendría control de esta tarea, el otro 50% comenta que no podría negarse a realizar esta tarea. El 75% de los hombre no se pueden negar a realizar esta tarea y solo 25% también hace referencia al reglamento de vigente de la empresa, por lo que el total de una población de 10 Empleados, el 50% no pueden negarse a realizar este registro, el 45% consideran negarse a realizar esta tarea pero comentan que no tendría control alguno de este registro y solo el 5% considera negarse basándose en reglamento vigente de la empresa, reportando un resultado favorable para el objetivo del tema propuesto.

Grafica10.- Que clase de registro tenías antes del registro biométrico?



En esta gráfica, se determina que el 95% de las mujeres realizaban este proceso anteriormente con un checador y solo el 5% lo realizaba en base a un listado, la gráfica que hace referencia a los hombres indica que el 75% realizaba este proceso con checador y solo el 25% lo realizaba en base a un listado, por lo que el total de una población de 10 Empleados, el 70% de los empleados realizaban este proceso mediante un checador y el 30% restante lo hacía en base a un listado prediseñado por cada una de las áreas, reportando un resultado favorable para el objetivo del tema propuesto


INICIO
RECONOCE HUELLA
CAPTURA Y GUARDA HUELLA
HUELLA REGISTRADA
DESEA REGISTRAR LA HUELLA
GUARDA EN BASE DE DATOS
GUARDA EN BASE DE DATOS
ES EMPLEADO
INGRESA NUEVO REGISTRO
AUTENTICA USUARIO
REGISTRA HORA Y FECHA DE ENTADA
GUARDA EN BASE DE DATOS
FIN
AUTENTICA USUARIO
UA
FIN

4.4.4 BUSCAR Y COMPARAR HUELLA

Debido a lo extenso del Código solo detallaré las dos Clases Principales: DBCass (Donde Buscamos y Comparamos el Resultado que arroja el lector y Comparamos, Con los Registros en la Base de Datos y la Clase "Util.vb" que es la que control del Lector de Huellas.....

```
Imports System.Data.SqlClient
Imports System.Runtime.InteropServices

Public Class TTemplate
 Public tpt(GrFingerXLib.GRConstants.GR_MAX_SIZE_TEMPLATE) As Byte
 Public Size As Long
End Class

Public Structure TTemplates
 Public ID As Integer
 Public Cedula As Integer
 Public template As TTemplate
End Structure

Public Class DBClass
 Dim connection As New SqlConnection

 Public Function OpenDB() As Boolean
 Try
 connection = New SqlClient.SqlConnection(My.Settings.AccesoConnectionString)
 Return True
 Catch
 Return False
 End Try
 End Function

 Public Sub closeDB()
 connection.Close()
 End Sub

 Public Sub clearEmpleadoDB(ByVal Cedula As Integer)
 Dim sqlCMD As SqlCommand = New SqlCommand("DELETE FROM Biometrica where Cedula=" & _
        Cedula, connection)
 sqlCMD.Connection.Open()
 sqlCMD.ExecuteNonQuery()
 sqlCMD.Connection.Close()
 End Sub

 Public Function AddTemplate(ByRef template As TTemplate, _
        ByVal Cedula As Integer, ByVal contDed As Integer) As Long
 Dim da As New SqlDataAdapter("select RowID, Cedula, Template from Biometrica", _
        connection)
 da.InsertCommand = New SqlCommand( _
        "INSERT INTO Biometrica (cedula, template) Values(" & _
        Cedula & ", @template)", connection)
```

```
da.InsertCommand.CommandType = CommandType.Text
da.InsertCommand.Parameters.Add("@template", SqlDbType.VarBinary, _
        template.Size, "template")

connection.Open()

Dim TBio As DataSet = New DataSet
da.Fill(TBio, "Biometrica")

Dim newRow As DataRow = TBio.Tables("Biometrica").NewRow()
newRow("Cedula") = Cedula
newRow("template") = template.tpt
TBio.Tables("Biometrica").Rows.Add(newRow)
' ContHuellas += 1
Select Case contDed
Case 1
If Principal.ActiveForm.Name = "Wizard" Then
Wizard.PBDedos.Image = My.Resources.Indice
Else
AgregarHuellas.PBDedos.Image = My.Resources.Indice
End If
da.Update(TBio, "Biometrica")
connection.Close()
Case 2
If Principal.ActiveForm.Name = "Wizard" Then
Wizard.PBDedos.Image = My.Resources.Indice
Else
AgregarHuellas.PBDedos.Image = My.Resources.Indice
End If
da.Update(TBio, "Biometrica")
connection.Close()
Case 3
If Principal.ActiveForm.Name = "Wizard" Then
Wizard.PBDedos.Image = My.Resources.Indice
Else
AgregarHuellas.PBDedos.Image = My.Resources.Indice
End If
da.Update(TBio, "Biometrica")
connection.Close()

End Select
Return newRow("ID")
End Function

Private Sub OnRowUpdated(ByVal sender As Object, ByVal args As SqlRowUpdatedEventArgs)

End Sub

Public Function getTemplates() As TTemplates()
Dim ds As New DataSet
Dim da As New SqlDataAdapter( _
        "select RowID, Cedula, Template from Biometrica order by Cedula Desc", _
```

```
        connection)
Dim ttpts As TTemplates()
Dim i As Integer

da.Fill(ds)
Dim tpts As DataRowCollection = ds.Tables(0).Rows
ReDim ttpts(tpts.Count)
If tpts.Count = 0 Then Return ttpts
For i = 1 To tpts.Count - 1
ttpts(i).template = New TTemplate
ttpts(i).ID = tpts.Item(i).Item("RowID")
ttpts(i).Cedula = tpts.Item(i).Item("Cedula")
ttpts(i).template.tpt = tpts.Item(i).Item("template")
ttpts(i).template.Size = ttpts(i).template.tpt.Length
Next
Return ttpts
End Function

Public Function getTemplate(ByVal Cedula As Long) As Byte()
Dim ds As New DataSet
Dim da As New SqlDataAdapter( _
        "select ID, Cedula, Template from Biometrica where Cedula = " & _
        Cedula, connection)
Dim tpt As New TTemplate
da.Fill(ds)
Dim tpts As DataRowCollection = ds.Tables(0).Rows
If tpts.Count <> 1 Then Return Nothing
Return tpts.Item(0).Item("template")
End Function
```

4.4.5 COMPARACION DE HUELLA CON LA BASE.

El Código de la Clase: DBClass.vb

```
Imports System.Data.SqlClient
Imports System.Runtime.InteropServices

Public Class TTemplate
 Public tpt(GrFingerXLib.GRConstants.GR_MAX_SIZE_TEMPLATE) As Byte
 Public Size As Long
End Class

Public Structure TTemplates
 Public ID As Integer
 Public Cedula As Integer
 Public template As TTemplate
End Structure

Public Class DBClass
 Dim connection As New SqlConnection

 Public Function OpenDB() As Boolean
 Try
 connection = New SqlClient.SqlConnection(My.Settings.AccesoConnectionString)
 Return True
 Catch
 Return False
 End Try
 End Function

 Public Sub closeDB()
 connection.Close()
 End Sub

 Public Sub clearEmpleadoDB(ByVal Cedula As Integer)
 Dim sqlCMD As SqlCommand = New SqlCommand("DELETE FROM Biometrica where Cedula=" & _
        Cedula, connection)
 sqlCMD.Connection.Open()
 sqlCMD.ExecuteNonQuery()
 sqlCMD.Connection.Close()
 End Sub

 Public Function AddTemplate(ByRef template As TTemplate, _
        ByVal Cedula As Integer, ByVal contDed As Integer) As Long
 Dim da As New SqlDataAdapter("select RowID, Cedula, Template from Biometrica", _
        connection)
 da.InsertCommand = New SqlCommand( _
        "INSERT INTO Biometrica (cedula, template) Values(" & _
        Cedula & ", @template)", connection)
 da.InsertCommand.CommandType = CommandType.Text
```

```
da.InsertCommand.Parameters.Add("@template", SqlDbType.VarBinary, _
        template.Size, "template")

connection.Open()

Dim TBio As DataSet = New DataSet
da.Fill(TBio, "Biometrica")

Dim newRow As DataRow = TBio.Tables("Biometrica").NewRow()
newRow("Cedula") = Cedula
newRow("template") = template.tpt
TBio.Tables("Biometrica").Rows.Add(newRow)
' ContHuellas += 1
Select Case contDed
Case 1
If Principal.ActiveForm.Name = "Wizard" Then
Wizard.PBDedos.Image = My.Resources.Indice
Else
AgregarHuellas.PBDedos.Image = My.Resources.Indice
End If
da.Update(TBio, "Biometrica")
connection.Close()
Case 2
If Principal.ActiveForm.Name = "Wizard" Then
Wizard.PBDedos.Image = My.Resources.Indice
Else
AgregarHuellas.PBDedos.Image = My.Resources.Indice
End If
da.Update(TBio, "Biometrica")
connection.Close()
Case 3
If Principal.ActiveForm.Name = "Wizard" Then
Wizard.PBDedos.Image = My.Resources.Indice
Else
AgregarHuellas.PBDedos.Image = My.Resources.Indice
End If
da.Update(TBio, "Biometrica")
connection.Close()

End Select
Return newRow("ID")
End Function

Private Sub OnRowUpdated(ByVal sender As Object, ByVal args As SqlRowUpdatedEventArgs)

End Sub

Public Function getTemplates() As TTemplates()
Dim ds As New DataSet
Dim da As New SqlDataAdapter( _
        "select RowID, Cedula, Template from Biometrica order by Cedula Desc", _
        connection)
```

```
Dim ttpts As TTemplates()
Dim i As Integer

da.Fill(ds)
Dim tpts As DataRowCollection = ds.Tables(0).Rows
ReDim ttpts(tpts.Count)
If tpts.Count = 0 Then Return ttpts
For i = 1 To tpts.Count - 1
ttpts(i).template = New TTemplate
ttpts(i).ID = tpts.Item(i).Item("RowID")
ttpts(i).Cedula = tpts.Item(i).Item("Cedula")
ttpts(i).template.tpt = tpts.Item(i).Item("template")
ttpts(i).template.Size = ttpts(i).template.tpt.Length
Next
Return ttpts
End Function

Public Function getTemplate(ByVal Cedula As Long) As Byte()
Dim ds As New DataSet
Dim da As New SqlDataAdapter( _
        "select ID, Cedula, Template from Biometrica where Cedula = " & _
        Cedula, connection)
Dim tpt As New TTemplate
da.Fill(ds)
Dim tpts As DataRowCollection = ds.Tables(0).Rows
If tpts.Count <> 1 Then Return Nothing
Return tpts.Item(0).Item("template")
End Function

End Class
```

4.4.6 COMPARACION DE HUELLA

El Código de la Clase: DBClass.vb

```
Imports System.Data.SqlClient
Imports System.Runtime.InteropServices

Public Class TTemplate
 Public tpt(GrFingerXLib.GRConstants.GR_MAX_SIZE_TEMPLATE) As Byte
 Public Size As Long
End Class

Public Structure TTemplates
 Public ID As Integer
 Public Cedula As Integer
 Public template As TTemplate
End Structure

Public Class DBClass
 Dim connection As New SqlConnection

 Public Function OpenDB() As Boolean
 Try
 connection = New SqlClient.SqlConnection(My.Settings.AccesoConnectionString)
 Return True
 Catch
 Return False
 End Try
 End Function

 Public Sub closeDB()
 connection.Close()
 End Sub

 Public Sub clearEmpleadoDB(ByVal Cedula As Integer)
 Dim sqlCMD As SqlCommand = New SqlCommand("DELETE FROM Biometrica where Cedula=" & _
        Cedula, connection)
 sqlCMD.Connection.Open()
 sqlCMD.ExecuteNonQuery()
 sqlCMD.Connection.Close()
 End Sub

 Public Function AddTemplate(ByRef template As TTemplate, _
        ByVal Cedula As Integer, ByVal contDed As Integer) As Long
 Dim da As New SqlDataAdapter("select RowID, Cedula, Template from Biometrica", _
        connection)
 da.InsertCommand = New SqlCommand( _
```

```
        "INSERT INTO Biometrica (cedula, template) Values(" & _
        Cedula & ", @template)", connection)
da.InsertCommand.CommandType = CommandType.Text
da.InsertCommand.Parameters.Add("@template", SqlDbType.VarBinary, _
        template.Size, "template")

connection.Open()

Dim TBio As DataSet = New DataSet
da.Fill(TBio, "Biometrica")

Dim newRow As DataRow = TBio.Tables("Biometrica").NewRow()
newRow("Cedula") = Cedula
newRow("template") = template.tpt
TBio.Tables("Biometrica").Rows.Add(newRow)
' ContHuellas += 1
Select Case contDed
Case 1
If Principal.ActiveForm.Name = "Wizard" Then
Wizard.PBDedos.Image = My.Resources.Indice
Else
AgregarHuellas.PBDedos.Image = My.Resources.Indice
End If
da.Update(TBio, "Biometrica")
connection.Close()
Case 2
If Principal.ActiveForm.Name = "Wizard" Then
Wizard.PBDedos.Image = My.Resources.Indice
Else
AgregarHuellas.PBDedos.Image = My.Resources.Indice
End If
da.Update(TBio, "Biometrica")
connection.Close()
Case 3
If Principal.ActiveForm.Name = "Wizard" Then
Wizard.PBDedos.Image = My.Resources.Indice
Else
AgregarHuellas.PBDedos.Image = My.Resources.Indice
End If
da.Update(TBio, "Biometrica")
connection.Close()

End Select
Return newRow("ID")
End Function

Private Sub OnRowUpdated(ByVal sender As Object, ByVal args As SqlRowUpdatedEventArgs)

End Sub

Public Function getTemplates() As TTemplates()
Dim ds As New DataSet
```

```
Dim da As New SqlDataAdapter( _
        "select RowID, Cedula, Template from Biometrica order by Cedula Desc", _
        connection)
Dim ttpts As TTemplates()
Dim i As Integer

da.Fill(ds)
Dim tpts As DataRowCollection = ds.Tables(0).Rows
ReDim ttpts(tpts.Count)
If tpts.Count = 0 Then Return ttpts
For i = 1 To tpts.Count - 1
ttpts(i).template = New TTemplate
ttpts(i).ID = tpts.Item(i).Item("RowID")
ttpts(i).Cedula = tpts.Item(i).Item("Cedula")
ttpts(i).template.tpt = tpts.Item(i).Item("template")
ttpts(i).template.Size = ttpts(i).template.tpt.Length
Next
Return ttpts
End Function

Public Function getTemplate(ByVal Cedula As Long) As Byte()
Dim ds As New DataSet
Dim da As New SqlDataAdapter( _
        "select ID, Cedula, Template from Biometrica where Cedula = " & _
        Cedula, connection)
Dim tpt As New TTemplate
da.Fill(ds)
Dim tpts As DataRowCollection = ds.Tables(0).Rows
If tpts.Count <> 1 Then Return Nothing
Return tpts.Item(0).Item("template")
End Function

End Class
```

CAPÍTULO V

PROPUESTA

5.1 PROPUESTA

En este proyecto Informática realizado para la Unidad de Asuntos Legales se presenta el desarrollo de un sistema electrónico digital para el control de acceso basado en la tecnología de autenticación biométrica de huella dactilar. Este sistema pretende facilitar el acceso a los usuarios, que en lugar de utilizar los métodos convencionales, solo tendrán que desplazar el dedo sobre lector de huella dactilar. De este modo también se incrementa la certeza de que se tiene un registro, al ser la huella dactilar mucho más difícil de duplicar como objeto llave.

5.2 OBJETIVO DE LA PROPUESTA.

Se diseñó este sistema controlador de acceso en el que se dispone de los modos de autenticación de identificación y verificación del usuario mediante huella dactilar la cual será capturada por un lector de huella dactilar térmico por desplazamiento. En todo momento este dispositivo ejercerá el control de acceso entrada-salida.

5.3 EXPANDIR EL USO DE BINSI

Se propone expandir el uso de BINS en dependencias gubernamentales, asi mismo de otros modulos para el fin de agilizar este proceso.

5.4 EVALUACION DE LA PROPUESTA

1.- ¿Usted ha escuchado hablar de (BINSI) Sistema Integral Biométrico?

2.- ¿Le gustaría checar su asistencia en forma electrónica?

3.- ¿Qué piensa de un sistema electrónico para checar su asistencia?

4.- ¿El uso de algún equipo tecnológico te facilita el uso del Sistema Biométrico?

5.- ¿Estás de acuerdo que este sistema simplifique el registro de entrada-salida?

6.- ¿Qué podría aportar los usuarios para el buen funcionamiento de este sistema?

7.- ¿en qué parte de tu área laboral pondrías este sistema?

8.- ¿Estás de acuerdo que este sistema se instale en la entrada de la empresa?

9.- ¿Un usuario puede negarse a realizar este registro?

CONCLUSIONES

Así mismo se debe fomentar la investigación sobre los recursos tecnológicos en ámbito empresarial para atender la diversidad; juntar los esfuerzos alrededor de grupos de referencia de calidad ya conocida.

Por lo tanto hay que promover el uso de las nuevas tecnologías, incluyendo en ella la manera de que todos puedan aportar mejoras en este sistema que permite la flexibilidad de las nuevas tecnológicas.

BIBLOGRAFIA

ANEXOS

SISTEMA DE AUTENTICACION BIOMETRICA DE HUELLA DACTILAR ASISTIDO POR VOZ.

DIGITAL PERSONAL.

DIGTITAL PERSONAL 4500 CARACTERISTICAS.

ESCUELA DE INFORMATICA Y CIENCIAS DE LA COMPUTACION.

ESTUDIO DE FACTIBILIDAD PARA EL CONTROL DE ACCESO BIOMETRICO.

BUSCAR Y COMPARAR HUELLA

COMPARACION DE HUELLA CON LA BASE

COMPARACION DE HUELLA.

TECNOLOGIAS BIOMETRICAS APLICADAS A LA SEGURIDAD.

SEGURIDAD INFORMATICA.