UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

CENTRO UNIVERSITARIO VALLE DE CHALCO

AUTENTICACIÓN BIOMÉTRICA A TRAVÉS DE HUELLAS DIGITALES E IRIS EN UNA EMPRESA INDUSTRIAL.

TESINA

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A

JUAN CARLOS HERNÁNDEZ REYES

ASESORA:
DRA. ANABELEM SOBERANES MARTIN

Revisor: MTRO. HÉCTOR ENRIQUE GAONA FLORES

Revisor: MTRO. FRANCISCO RAÚL SALVADOR GINEZ

VALLE DE CHALCO SOLIDARIDAD, MÉXICO DICIEMBRE 2016.

AUTENTICACIÓN BIOMÉTRICA A TRAVÉS DE HUELLAS DIGITALES E IRIS EN UNA EMPRESA INDUSTRIAL.

ÍNDICE

I. RESUMEN

Necesitamos tener presente siempre que la tecnología va avanzando a una manera impresionante, cada vez es más necesario buscar la manera de implementar nuevos sistema de seguridad que tenga esa confiabilidad que el usuario necesita. Un claro ejemplo es nuestra vida cotidiana, lo que hacemos más común es el uso de algún sistema de seguridad para el control de acceso ya sea a nuestras propias casa o empresas, escuelas entre otras, y no solo de acceso sino también a las actividades que se están realizando dentro de estas, cuantas veces no ingresas algún instituto gubernamental y te requieren que te registres en un cuaderno donde tus datos básicos son registrados y también a que asunto es a lo que ingresas. Pero ¿un cuaderno es lo suficiente confiable o unas llaves, una tarjeta, un nip entre otras? Y la respuesta sin pensar es no, no es de total confiabilidad puesto existen mecanismo de falsificar los objetos o incluso de robar estos mismos.

Debido a esta falta de confiabilidad se requiera un mecanismo que esté bas.ado en las identificaciones biométricas, que posea una fiabilidad mayor a los mecanismos comunes. Actualmente existen en el mercado sistemas biometría de huella dactilar, biometría vascular, biometría facial, biometría de iris, de voz, retina, biometría de palma de la mano y firma. Las huellas dactilar es un método aceptado popularmente y de fácil adquisición, cumpliendo con las dos leyes básicas que regulan el nivel de viabilidad de todo sistema de identificación de la invariabilidad temporal y la variedad infinita de autentificado. La huella dactilar es una característica única de cada individuo, puesto desde que se nace hasta que envejece siempre tendrá las mismas líneas sin alterar el número, el grado de curvatura, ni la situación de las crestas presentes en la misma. No existen personas con la misma huella dactilar ni entre los gemelos existe la misma huella.

En este trabajo de investigación se realiza una propuesta que autenticación que lleve dos sistemas en uno es decir el sistema de autenticación por huella digital y por iris esto incrementara la confiabilidad para identificar un individuo. La herramienta que se utilizo es de fácil adquisición e instalación, no requiere utilización de memoria elevada permitiéndonos con esto utilizar el resto de la memoria para realizar el almacenamiento de usuarios.

El principal objetivo de este trabajo es realizar una identificación de personas por medio del reconocimiento digital de imágenes biométricas, este medio es porque a través de este sistema se puede hacer el reconocimiento de un rasgo corporal único, por lo que reconoce a las personas en función de quiénes son y no de lo que traen consigo como tarjetas, llaves, credenciales, entre otras, o en su defecto en lo que puedan recordar como lo son las claves personales de identificación (nip) que en algunos casos son olvidadas, además, que estas pueden ser robadas o clonadas para falsificar la identidad del individuo.

No existe sistema que al cien por ciento identifique un individuo pero si se puede realizar un sistema de control realmente eficiente y preciso de las personas, además de saber con toda certeza que la persona pasó por esta forma de reconocimiento. Es la persona a ser reconocida y no como sucede con firma, código de barras o banda magnética, que en determinado momento son fácilmente violables o pueden ser de una falsificación sencilla. Hay que recordar que las técnicas no son absolutamente seguras, pudiendo producirse ciertos errores, o igualmente se crean mecanismos o sistemas que hagan vulnerable los sistemas de autenticación. Este problema se aborda a través de la investigación y mejora de las técnicas actuales, lo cual permitiría mejorar el nivel de certeza.

I. IMPORTANCIA DE LA TEMÁTICA

Hoy en día la autentificación es importante en ciertas empresas que necesitan de personas responsables, de personas honestas y trabajadoras, hay muchas maneras para poder checar la hora de asistencia y poder acceder a ciertas áreas de la empresa. Se puede a través de una tarjeta como en muchos casos de utiliza. Con una credencial y hay una persona quien reciba o abra la puerta de acceso pero para hacer más autónoma y teniendo mayor seguridad se va implementar un sistema donde se pueda solucionar este problema.

En primera se escogió la huella digital puesto que es una parte del cuerpo que nos identifica como únicos, dos personas no pueden tener la misma huella digital, pero como pocas personas lo saben esto se puede falsificar entonces para esto se desarrolla el sistema con iris también, que también nos identifica como únicos, entonces sí se puede falsificar las huellas pero la iris no entonces tendremos mayor seguridad a nuestras áreas que queremos proteger y a la asistencia del personal en la empresa

Algunos otros puntos que se quieren llegar a realizar este sistema son para poder registrar horas de entradas y salidas, para poder identificar a cada persona que ingresa por medio de su huella dactilar, la cual es difícil de falsificar o duplicar también tener control de las asistencias y retardos de los empleados

Da un grado importante de seguridad ya que se puede aunar a este sistema una chapa digital de tal manera que no abra la puerta si no está registrada la persona. También se trata de ser ecológicos al elimina el uso de tarjetas de papel que son muy fáciles de hacer trampa.

II. PLANTEAMIENTO DE PROBLEMA

Los primeros antecedentes de los que se tiene referencia sobre la biometría datan de hace más de mil años en China, donde los alfareros comenzaron a incluir sus huellas dactilares en los productos que realizaban como símbolo de distinción o firma, lo que les permitía diferenciarse del resto.

Sin embargo, no fue hasta finales del siglo XIX cuando Alphonse Bertillon antropólogo francés que trabajó para la policía comenzó a dar a la biometría el carácter de ciencia, profesionalizando su práctica. Basaba su teoría en que una cierta combinación de medidas del cuerpo humano era invariable en el tiempo, lo que permitió dar solución al problema de identificar a los criminales convictos a lo largo de toda su vida.

Uno de los objetivos de la humanidad desde tiempos remotos, ha sido la búsqueda del medio o la manera para poder hacer identificación no ambigua de una persona. En los últimos años se han producido avances impresionantes en el sector tecnológico y sin embargo una función que ha sobrevivido sin cambios son las contraseñas como método de autenticación (Sánchez, 2000).

Los biométricos incluyen una gama de características que benefician a dueños, empleados y clientes, las compañías que adopten los biométricos en forma temprana gozaran de una ventaja competitiva. Sin lugar a dudas, su caso seguirá popularizándose. La retina del ojo humano es tan único como las huellas dactilares (Pachay, 2011).

Las preguntas que se plantean en la investigación de tesina son las siguientes:

- ¿Qué elementos de software y hardware son indispensables para el control del sistema?
- ¿Qué otras diferentes utilidades tendrá el sistema biométrico por huella digital e iris?
- ¿Qué importancia tiene validar la identidad de una persona?

III. MÉTODOS Y TÉCNICAS DE INVESTIGACIÓN EMPLEADAS

Este proyecto es el resultado de una investigación que se realizó en un primer momento de manera documental de carácter monográfico.

Para la manera documental es obtenida de diversas fuentes como son documentos, tesis, tesinas, libro y artículos web de páginas universitarias. En las que ofrecen información para el entendimiento de la biometría, los tipos de métodos biométricos para la autenticación de individuos, las ventajas y desventajas de estos métodos como conocer las áreas que puede implementarse una mayor seguridad y tener mejor información del personal que se encuentra laborando.

También de tipo experimental ya que se después se procedió a realizar el sistema de autenticación biométrica a través de huella dactilar e iris para una empresa industrial, la cual puede tener como fin el control de los accesos de las áreas a los empleados de la empresa así como el control de asistencia del personal.

IV. DESARROLLO TEMÁTICO

Para abordar el tema el desarrollo temático se inició definiendo biometría, para continuar con un poco de la historia de la biometría, mencionado los diferentes tipos de sistema biométricos que existen así con su clasificación que tiene los sistema. Por último se desarrolla una propuesta de autenticación biométrica combinando dos sistemas que son de los más altos en seguridad.

5.1 Biometría

La biometría es la tecnología que es basada en el reconocimiento de un carácter intransferible (físico) de una persona o de comportamiento. La biometría es basada en el principio cada persona es única y posee rasgos físicos distintivos o de comportamiento. La biometría es un sistema que reconoce a la persona basándose en "quién" es, no importando "el qué lleva puesto" o "lo que conoce" (kimaldi, 2016).

Es un excelente sistema de identificación de un individuo que principalmente es utilizada para la seguridad y comodidad. Ya que limita al individuo al poder utilizar dispositivos externos ya sea llaves, claves u tarjetas inteligentes entre otras. Entre las aplicaciones de la biometría esta principalmente el control de acceso, sistemas de seguridad de alta complejidad, incluso ya se instalan en mecanismos de armas como son algunas pistolas.

El hombre desde tiempos remotos ha tratado de tener el control de acceso, ya sea a información o lugares, para eso se utilizaban por ejemplo llaves o claves para tener el control de acceso. Ahora nuestros tiempos, a través de digitalización se han cambiado por contraseñas, números, códigos PIN (Personal Identification Number), patrones, certificaciones digitales, firmas digitales, tarjetas inteligentes entre otros, para darse cuenta que estos son mecanismo externos a

una persona, puede que sean únicos pero también hay mecanismos para poder falsificar o ser robados la información por ejemplo una tarjeta inteligente puede ser robada o clonada sin que el individuo de esa tarjeta se pueda dar cuenta.

La tecnología va evolucionando y así como se pueden crear mecanismos de control de acceso así mismo se crean mecanismo que falsifiquen, clonen o roben esa misma información.

Como dijo Paul Preston "Quien no conoce la historia está condenado a repetir sus errores", entonces la humanidad se dio cuenta que necesitaba un mecanismo que no dependiera de una llave, se dio cuenta que las personas somos únicos y tenemos rasgos únicos, lo que concluyeron que la llave seria la misma persona que se utilizaría para autenticarse.

5.1.1 Introducción a la biometría

El problema básico en la implantación de los métodos biométricos es la aceptación del usuario. Varias teorías al respecto están hoy enfrentadas. Parte de la sociedad rechaza de entrada la idea de identificarse mediante sus huellas o algún sistema que controle su anatomía porque creen que su intimidad es invadida, sienten que se les está espiando o controlando de algún modo, o simplemente creen que se les está tratando como criminales. Por otro lado, como vino a demostrar un estudio de la Universidad de Columbia, cada vez hay más gente (el 83%) que confía en la comodidad de no llevar cada vez más tarjetas diferentes, ni en tener que recordar diversos códigos de seguridad para cada una de ellas (seguridad online, 2014).

Lo cierto, básicamente, es que si nos centramos en el aspecto de la comodidad, más de una vez nos puede ocurrir que nos dejemos olvidada una tarjeta en casa, pero raro es que nos dejemos la mano o el ojo.

Otro punto de vista para la no aceptación de ciertos sectores es el de la salud. Los problemas médicos que pueden producir las técnicas de medida, tanto por un contagio como por una lesión, también influye sobre la aceptación de los métodos.

Estos aspectos requieren una mejora del proceso de medida y una fase de información al usuario que elimine cualquier sombra de duda que pueda tener ya que todo proceso de medida siempre debe incluir un consentimiento expreso por parte del usuario, Es recomendable que el área de la huella sea de 1 pulgada cuadrada y que la resolución de la imagen sea igual o superior a 500 dpi y 256 niveles de grises (100-500 Kbytes) (Ávila, s.f.).

La biometría es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos físicos intrínsecos. El término se deriva de las palabras griegas "bios" de vida y "metron" de medida.

La "biometría informática" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para “verificar” identidades o para “identificar” individuos.

La biometría, una de las diez tecnologías emergentes según un estudio (2001) del Massachussets Institute of Technology (MIT), es una ciencia que emplea métodos de identificación no tradicionales como la impresión de huella dactilar, la biometría dinámica de firma, la geometría del rostro o de la mano, el iris, la retina, así como el tipo de sangre y de ADN. En la actualidad debido a su sencilla implementación y bajo costo/beneficio, la biometría de huella dactilar es el método más utilizado y conocido; se emplean programas de lectura de huellas

digitales, relojes checadores de control biométrico o programas de control de ausentismo por lectura biométrica, estos sistemas son aquellos que utilizando lectores de huellas digitales integrados a una red de computadoras o bien lectores autónomos de huellas dactilares permiten verificar el ingreso, salida, ausentismo y otras situaciones relacionadas con el control de personal.

5.1.2 Historia de la biometría

1858 En primer lugar la captura sistemática de imágenes de mano para fines de identificación se registra. Sir William Herschel registro una huella de la mano en la parte posterior de un contrato por cada trabajador a distinguir esto para que distinguiera a los empleados cuando se realizaba el día de pago (Komarinski, 2004).

1870 Alphonse Bertillon desarrolla antropometría para identificar individuos. También llamado "Bertillonage" o antropométricas, este método basado en registro detallados de sus medidas corporales, descripción física y fotografías. Bertillon basado en que los delincuentes podrían cambiar sus nombres a menudo, excepto algún elemento de sus cuerpos. Las autoridades del mundo utilizaron este sistema hasta que se descubrió que las personas de comparten algunas mediciones de la misma.

1892 Galton desarrolla un sistema de clasificación de huellas digitales Sir Francis Galton detallado sobre las huellas dactilares en el que demostró un nuevo sistema de clasificación en la que básicamente utilizando la impresiones de los diez dedos. Hasta nuestros días se sigue utilizando este sistema mejor llamado como detalles de Galton.

1894 es publicado la tragedia de Pudd’nhead Wilson. En esta novela se mencionó por primera vez el uso de huellas dactilares para la identificación.

1896 Sir Edward Henry desarrolla un sistema de clasificación de huellas dactilares. Henry realizo la búsqueda de un método para identificación para aplicar simultáneamente a la sustitución, donde realizo su consulta de Galton en cuanto a las huellas dactilares como método de identificación de criminales. Henry fue el precursor para el sistema de clasificación utilizado durante muchos años por la Oficina Federal de investigaciones (FBI) y otras organizaciones de justicia criminal que realizan fichas dactilares búsquedas de huellas dactilares (Komarinski, 2004).

1903 Las prisiones de Nueva York comienzo a utilizar las huellas dactilares. Esta práctica fue adoptada por el sistema de prisión del estado de Nueva York donde las huellas digitales se utilizan para la identificación de criminales.

1903 Colapsos del sistema Bertillon. En la penitenciaria de Leavenworth, Kansas fueron condenados dos hombres que se determinan que eran gemelos idénticos ya que tenías las mismas según el sistema de Bertillon.

1936 Se propone el concepto de utilizar el patrón del iris para la identificación. Frank Burch propuso el concepto de uso de iris patrones como un método para reconocer a un individuo (Courts, Individual Biometrics: Iris Scan, 2005).

1960 El reconocimiento facial de se convierte en semi-automatizado. Bajo un contrato del gobierno se desarrolla el primer sistema ade reconocimiento facial semi automático por Woodrow W. Bledsoe. Su uso necesitaba de una persona que localizara las características tales como ojos, oídos, nariz y boca en las fotografías.

1960 Es creado el primer modelo de producción acústica de voz. Gunnar Fant publicó una descripción del modelo los componentes fisiológicos de la producción del discurso acústico. Los resultados se basaron en el análisis de rayos x de los individuos que sonidos fónicos especificados (Jhon, Nicholas, & Peter, 2003).

1965 Empiezan inicios de investigación con reconocimiento de firma automatizada. La aviación norteamericana desarrolló el primer reconocimiento de firma sistema.

1969 El FBI (traducción Oficina Federal de investigación) impulsa para hacer reconocimiento de huellas dactilares de un proceso automatizado. Rapidamente fue haciendo abrumadora y requiere muchas horas de trabajo. Se hizo contrató el Instituto Nacional de Normas y tecnología (NIST) para estudiar el proceso de automatización de identificación de huellas digitales (Jhon, Nicholas, & Peter, 2003).

1970 El reconocimiento de rostros da un paso más hacia la automatización. Para esto Goldstein, Harmon y Lesk ulizaron marcadores 21 caracteres específicos como el color y labio grueso del pelo para automatizar el reconocimiento facial. Pero el problema con estas soluciones tenían que se manualmente los cálculos de las medidas y ubicaciones (Goldestein, Harmon, & Lesk, 1971).

1970 El primer modelo del comportamiento del habla. El modelo proporcionado más detallada la comprensión del complejo comportamiento y componentes biológicos del discurso (Jhon, Nicholas, & Peter, 2003).

1975 El FBI financia de desarrollo de sensores y tecnología de extracción de minucias. Estos primeros lectores utilizan técnicas capacitivas para recoger las huellas dactilares características. En las próximas décadas, NIST

enfocado y dirigido avances en métodos automáticos de digitalización entintado las huellas dactilares y los efectos de la compresión de imagen en imagen calidad, clasificación, extracción de minucias y el emparejar. Utilizado para limitar la búsqueda humana, este algoritmo producida un significativo conjunto más reducido de las imágenes que luego fueron entrenados y personal humano especializado para la evaluación (Jhon, Nicholas, & Peter, 2003).

1976 El desarrollo del primer sistema de reconocimiento de voz. Texas Instruments desarrolló un reconocimiento del altavoz de prototipo sistema, que fue probado por la fuerza aérea y el MITRE Corporación (Jhon, Nicholas, & Peter, 2003).

1977 Se concede la patente para la adquisición de la información de firma dinámica. Veripen, Inc. fue concedido una patente para una "Identificación Personal Aparato" era capaz de adquirir presión dinámica información. Este dispositivo permite la captura digital de las características dinámicas de la firma de una persona. El desarrollo de esta tecnología ha llevado a la pruebas de verificación de escritura automática (realizada por el MITRE Corporation) para la división de sistemas electrónicos de la Fuerza aérea de Estados Unidos (Jhon, Nicholas, & Peter, 2003).

1980 se establece el grupo de discurso NIST. El Instituto Nacional de estándares y tecnología (NIST) desarrolló el grupo de discurso de NIST para estudiar y promover el uso de técnicas de procesamiento del discurso. Bajo financiamiento de la Agencia de seguridad nacional, el grupo de discurso NIST ha acogido evaluaciones anuales, la evaluación de reconocimiento de locutor de NIST Taller para fomentar el avance continuado del altavoz comunidad de reconocimiento (Group N. S., 2005).

1985 Se propone concepto que no hay dos iris iguales. Los doctores Leonard Flom y Aran Safir, oftalmólogos, propusieron la concepto que dos iris no son iguales (Courts, Individual Biometrics: Iris Scan", 2006).

1985 Se crea patente para la identificación de la mano. La comercialización de la geometría de la mano data de la década de 1970 con uno de los primeros despliegues de la Universidad de Georgia en 1974. El ejército de los E.E.U.U. comenzó pruebas geometría de la mano para su uso en Banca en aproximadamente 1984. Estas implementaciones son anteriores el concepto de uso de la geometría de una mano para identificación como patentado por David Sidlauskas (Jhon, Nicholas, & Peter, 2003).

1986 El intercambio de datos estándar minucias de huellas dactilares se publica. La Oficina Nacional de estándares (NBS), ahora el nacional Institutos de estándares y tecnología (NIST), publicado en colaboración con ANSI, un estándar para el intercambio de huella digital datos de minucias (ANSI/NBS-ICST 1-1986). Este fue el primera versión de los estándares actuales de intercambio de huellas dactilares utilizado por agencias del orden público (K. & F., s.f.)

1987 Crea patente que indica que el iris se pueden usar para la identificación. Los doctores Leonard Flom y Aran Safir fueron concedidos una patente para su concepto que el diafragma podría ser utilizado para identificación. El Dr. Flom se acercó a Dr. John Daugman desarrollar un algoritmo para automatizar la identificación del iris humano (Jhon, Nicholas, & Peter, 2003).

1988 Primer sistema de reconocimiento facial semi-automatizado se despliega. Eigenface técnica se desarrolló para el reconocimiento facial. En 1988, la división de Lakewood del Sheriff de Condado de Los Ángeles Departamento comenzó a utilizar compuestos dibujos o imágenes de vídeo de un sospechoso para llevar a cabo una búsqueda en la base de datos digitalizada.

Kirby y Sirovich aplicaron análisis de componentes de principio, una técnica estándar de álgebra lineal, para el reconocimiento de la cara problema. Esto fue un hito porque demostró que menos de cien valores debían aproximar una convenientemente imagen de rostro alineado y normalizado (Angela, s.f.).

1991 Pioneros en la detección de la cara, haciendo posible el reconocimiento de rostros en tiempo real. Turck y Pentland descubrieron que al utilizar las técnicas eigenfaces, el error residual podría ser utilizado para detectar rostros en imágenes. El resultado de este descubrimiento significó confiable en tiempo real reconocimiento facial automatizado fue posible. Encontraron que este estaba algo limitada por factores ambientales, pero el descubrimiento causó una gran chispa de interés en el reconocimiento de la cara.

1992 Biométrico Consorcio se establece dentro de Gobierno de los EE.UU. Participación en el consorcio fue limitada originalmente a agencias de gobierno; miembros del sector privado y la academia se limitaron a asistir en calidad de observador. El Consorcio pronto amplió su membresía para incluir a estas comunidades y desarrollado numerosos grupos de trabajo para iniciar o ampliar los esfuerzos en la prueba, elaboración de normas, interoperabilidad y cooperación del gobierno. El Consorcio sí mismo sigue siendo activo como un enlace clave y discusión Foro entre gobierno, industria y comunidades académicas (Jhon, Nicholas, & Peter, 2003).

1993 Desarrollo de un prototipo de unidad de iris comienza. La Agencia Nuclear de defensa comenzó a trabajar con IriScan, Inc. para poner a prueba y una unidad de reconocimiento de iris de prototipo. También se inicia el reconocimiento de la cara Tecnología (FERET). La evaluación de tecnología cara de matrículas (FERET) fue patrocinado entre 1993 y 1997 por la investigación avanzada de defensa Productos de agencia (DARPA) y la tecnología de antidrogas del DoD Oficina del programa de desarrollo en un esfuerzo por

fomentar la desarrollo de algoritmos de reconocimiento facial y tecnología. Esto evaluación evaluar los prototipos de sistemas de reconocimiento de cara (Phillips, Moon, Rizvi, & Rauss, 2000).

1994 Primer algoritmo de reconocimiento del iris está patentado. El Dr. John Daugman fue concedido una patente para su reconocimiento de iris algoritmos. Propiedad de Iridian Technologies, el sucesor de IriScan, Inc., esta patente es la piedra angular de más comercial productos de reconocimiento de iris hasta la fecha.

1995 El prototipo Iris vuelve a estar disponible como un producto comercial. El proyecto conjunto entre la Agencia de defensa Nuclear y Iriscan dio lugar a la disponibilidad del primer producto comercial de iris.

1996 La geometría de la mano se implementa en los Juegos Olímpicos. Un uso público importante de la geometría de la mano se produjo en el Atlanta 1996 Juegos Olímpicos donde se implementaron sistemas de geometría de mano para controlar y proteger el acceso físico a la Villa Olímpica. Esto fue un logro significativo porque los sistemas de maneja la inscripción de más de 65.000 personas. Más 1 millón las transacciones fueron procesadas en un período de 28 días. (Jhon, Nicholas, & Peter, 2003)

1998 FBI lanza CODIS (base de datos de ADN forense) El FBI lanzó combinado ADN Índice sistema (CODIS) a digital almacenar, buscar y recuperar marcadores de ADN forense derecho efectos de la aplicación. La secuencia es un proceso de laboratorio entre 40 minutos y varias horas.

2000 En primer lugar el papel de investigación que describe el uso de patrones vasculares de reconocimiento es publicado. Múltiples agencias de gobierno de los E.E.U.U. patrocinado por el reconocimiento de la cara prueba del vendedor (FRVT) en el año 2000. FRVT 2000 sirvió como el primer abierto,

evaluación de la tecnología a gran escala de múltiples comercialmente sistemas biométricos disponibles.

También en el mismo año la Universidad de Virginia Occidental (WVU) y el FBI, en consulta con asociaciones profesionales como la Asociación Internacional para Identificación, estableció un programa de licenciatura en Sistemas biométricos en el año 2000. Aunque muchas universidades han tenido mucho tiempo cursos relacionados con biometría, este es el primero basado en la biometría Programa de grado. WVU anima a los participantes del programa para obtener un doble grado en Ingeniería Informática y sistemas biométricos como no está acreditado el grado de sistemas biométricos (Blackburn, 2006).

2001 El reconocimiento facial se utiliza en el Súper Bowl en Tampa, Florida. Se instaló un sistema de reconocimiento de cara en la Súper Bowl en Enero de 2001 en Tampa, Florida, en un intento de identificar individuos "quería" entrar en el estadio. La demostración no encontró a ninguna persona “buscada" pero administrado incorrectamente como muchos como una docena de inocentes los fanáticos de los deportes. Siguientes medios e Investigaciones del Congreso sirvieron para introducir ambos datos biométricos y sus preocupaciones de privacidad asociados en el sentido del público en general.

2002 Se establece la norma ISO / IEC normas subcomité de la biometría. La organización internacional de normalización (ISO) establece la norma ISO/IEC JTC1 Subcomité 37 (JTC1/SC37) para apoyar la estandarización de tecnologías biométricas genéricas. El Subcomité desarrolla normas para promover la interoperabilidad y el intercambio de datos entre aplicaciones y sistemas (Jhon, Nicholas, & Peter, 2003).

2002 Se utiliza la palma Imprimir documento de los servicios se trasladará a la Comisión de Servicios de Identificación. Sistema de identificación

automatizada de huellas dactilares (IAFIS) integrado capacidades de impresión de Palma fue sometido a la identificación Subcomité de servicios (es), servicios de información de Justicia Criminal División (CJIS) Advisory Policy Board (APB). El trabajo conjunto Grupo llamado "fuerte respaldo de la planificación, costeo, y el desarrollo de una capacidad integrada de impresión latente para Palmas en la división de CJIS de FBI." Como resultado de este respaldo y el otro negocio cambiante necesita derecho ejecución, el FBI anunció el IAFIS de siguiente generación (NGI) (NSTC Subcommittee on Biometrics, 2005).

2003 formal de coordinación de las actividades de gobierno de Estados Unidos comienza biométricos. El nacional de ciencia y tecnología Consejo, un gobierno de los Estados Unidos Consejo de nivel ministerial, establecido un Subcomité de biometría coordinar la biometría R&D, política, divulgación e internacional colaboración (Internacional, 2003).

2003 OACI adopta plan para integrar datos biométricos en viaje de lectura mecánica documentos. El Foro Europeo de la biometría es un europeo independiente organización apoyada por la Comisión Europea cuyo total la visión es establecer la Unión Europea como el líder mundial en Excelencia de biometría por abordar las barreras a la adopción y fragmentación en el mercado. El foro también actúa como el motor para la coordinación, apoyo y fortalecimiento de los organismos nacionales (Internacional, 2003).

2004 DOD implementa ABIS. El sistema biométrico automatizado en identificación (ABIS) es un Departamento de defensa (DoD) sistema implementado para mejorar la Capacidad del gobierno Estadounidense para rastrear e identificar seguridad nacional amenazas. Los sistemas de recogida asociados incluyen la capacidad de recoger, de combatientes enemigos, los insurgentes capturados y otros las personas de interés, diez rodado las huellas dactilares, hasta cinco tiros de taza desde diferentes ángulos, muestras

(expresiones), imágenes del iris, de voz y un hisopo bucal para recolectar ADN. (BIOMETRICS, 2013).

2004 Primera base de datos de impresión de la palma automatizada en todo el estado se despliega en los EE.UU. Connecticut, Rhode Island y California establecidas palma estatal imprimir las bases de datos que permiten la aplicación de la ley agencias en cada estado a presentar impresiones de Palma latente no identificados a se buscará de otra base de datos de delincuentes conocidos (Jhon, Nicholas, & Peter, 2003).

2005 Patente de Estados Unidos en concepto de reconocimiento de iris expira. La patente de los E.E.U.U. amplia que abarca el concepto básico de reconocimiento de iris expiró en 2005, proporcionando oportunidades de comercialización para otras empresas que han desarrollado sus propios algoritmos para iris reconocimiento (Jhon, Nicholas, & Peter, 2003).

5.2 Tipos de sistema biométricos

La biometría estudia las características de una persona para que esta pueda ser identificada, para lograr su objetivo, esta ciencia se divide en Biometría Estática y Biometría Dinámica (Hernández B. A., 2009).

La Biometría Estática se dedica al estudio de las características físicas de un individuo, con este se están basados en los sistemas biométricos de huellas dactilares, geometría de la mano, en el caso de la Biometría Dinámica desarrolla sus estudios en el comportamiento de los seres humanos para determinar que los hace únicos de los demás (ver diagrama 1).

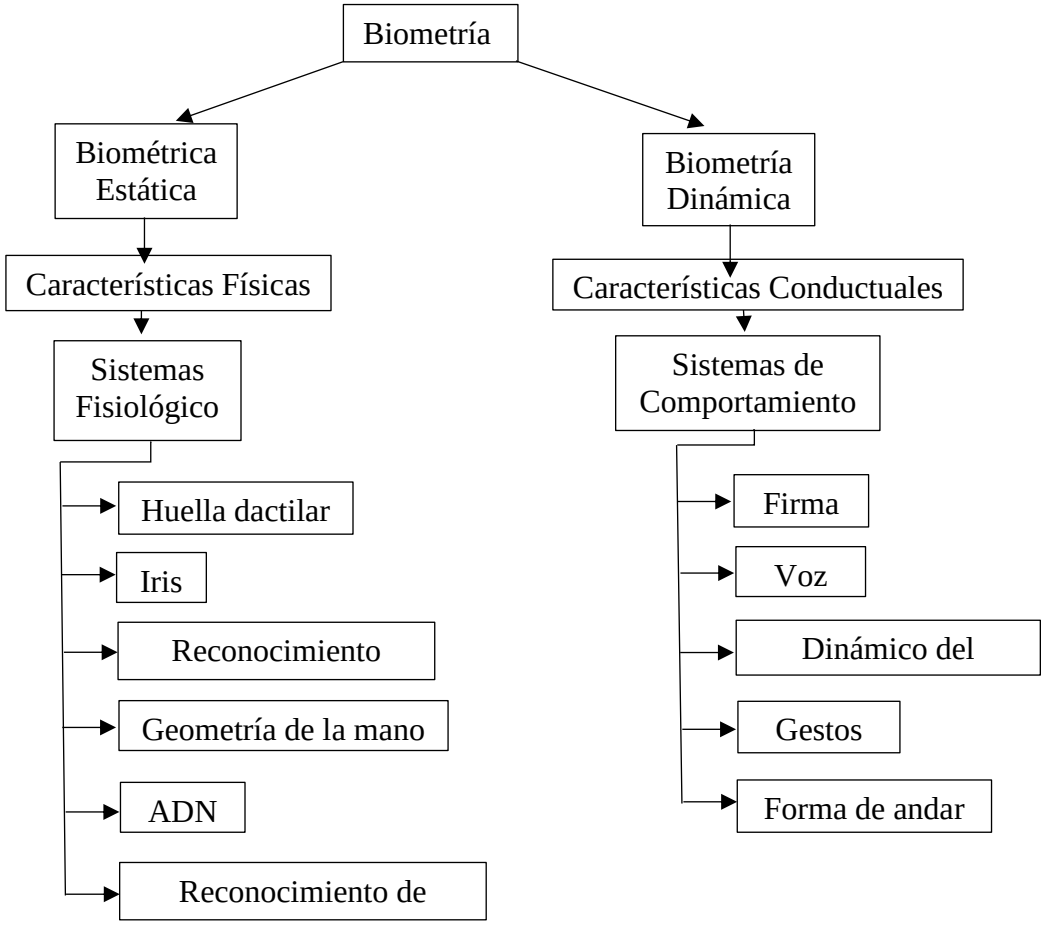


Diagrama 1. Las principales ramas de la biometría. Elaboración propia

5.2.1 Sistemas fisiológicos

Es basado en datos o particularidades del cuerpo humano de un individuo, ya que en su vida no va a variar sus rasgos físicos. Los más importantes son las huellas dactilares, sanguíneas, el iris, la retina, la mano. No por ser físicos vamos a decir que todos el cuerpo de un individuo es único, ya que se pueden tener cambios a lo largo de la vida del individuo, como la cara podemos notar que puede sufrir varios cambios ya se notan a simple vista como la cara los cuales pueden ser muy fácil de realizar a través del cabello y su peinado, bigote varaba, depilaciones.

Ahora con la tecnología que se va desarrollando a paso acelerado ya se pueden hacer cambios estético, como por ejemplo en la cara se pueden realizar transformaciones de nariz, de piel, tratamientos para la piel entre otro.

5.2.1.1 Biometría facial

El método más común de reconocimiento de un individuo es la cara, ya que es el más usado por la humanidad el reconocimiento visual. El reconocimiento facial es un método biométrico que reconoce a una persona a partir de una imagen anteriormente ya creada a través de una cámara.

Los algoritmos de reconocimiento faciales antes utilizados eran basados en modelos geométrico simples, a través de los años ha madurado y se han creado en representaciones matemáticas y procesos de coincidencia.

Hay dos métodos esenciales para el reconocimiento de rostro:

- Imágenes basadas en 2D.
  En estos métodos se toma una fotografía de la cara del individuo y se mide la distancia que hay entre las diferentes características de la cara del individuo para la creación de platillas de identificación. La ventaja es que es un mecanismo que no toma mucho tiempo se du captura de rostro.

- Imágenes basadas en 3D.
  En estos métodos la comparación que hay con los 2D que elimina la posibilidad de que la imagen pueda ser capturada de una hoja de papel.

El mecanismo en estos métodos hace que el proceso sea algo tardado por la captura de rostro.

La autenticación de rostro principalmente se divide de dos categorías (J., 2008):

Reconocimiento de características: este método se basa en las relaciones geométricas como las áreas, distancias y ángulos que pueden existir entre las características particulares de la cara.

Reconocimiento de apariencia: esta técnica usa las propiedades globales de la imagen del rostro para determinar los patrones de verificación, esto lo hace utilizando vectores procesados por una computadora para representar el rostro de manera eficiente. Este método es el más utilizado dentro de la industria biométrica. En seguida se mencionan los algoritmos más populares utilizados para la autenticación biométrica (Jain, Flynn, Abraham, 2009, págs. 45-70):

- Análisis de los Principales Componentes (PCA por sus siglas en inglés).
  La técnica se basa en la aplicación de algoritmos de compresión que eliminara información que no es necesaria por ejemplo el color de la piel y cabello a través de la obtención del rostro del individuo, para obtener la información básica para la identificación de la persona (ver figura 1).
  De esta manera se obtiene una imagen muy reducida que contiene toda la información necesaria para identificar a la persona.

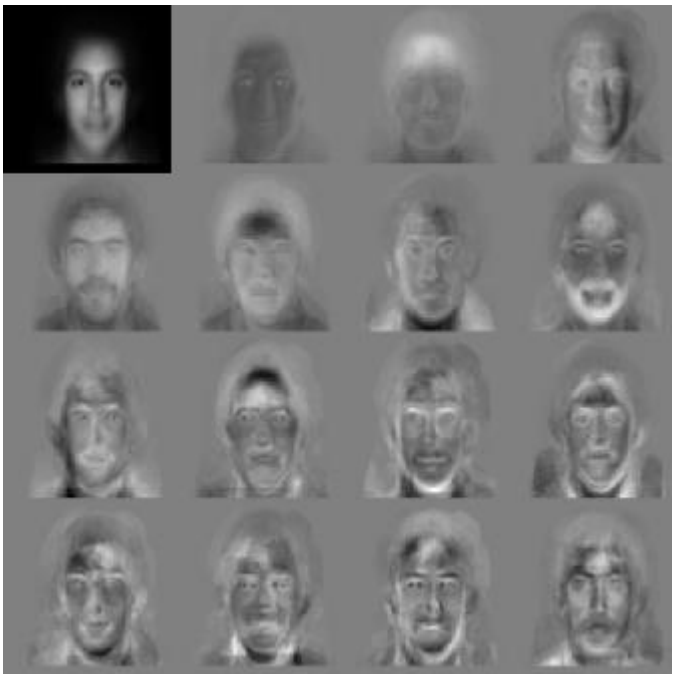


Figura 1. Técnica de análisis de componente básico (Standard Eigenfaces). (Group M. M., 2002)

- Análisis por Discriminación Lineal (LDA por sus siglas en inglés).
  Método de análisis que a través de una variedad de imágenes (caras del individuo) aunque no sean exactamente las mismas, logra decidir que la persona de las fotos sea la misma o es otra persona (ver figura 2).

Figura 2. 6Seis personas diferentes cada una con 5 fotos de la misma persona aunque con diferencias. (Lu, 2002)

- Análisis de Rasgos Locales (LFA por sus siglas en inglés).

Reconocimiento a partir de múltiples coincidencias (EBGM por sus siglas en inglés). Método el cual su base de un algoritmo utiliza un filtro de Gabor, el cual es utilizado para la detección de formas utilizando procesamiento de imagen. El Jet Gabor es un nodo en la planilla elástica, manifestado por círculos en la imagen debajo. El cual describe el comportamiento de la imagen alrededor de un píxel. (RECONOCIMIENTO FACIAL, 2006).

Lo básico de este algoritmo es localizar puntos en el rostro, respecto a un punto de referencia (ver figura 3).

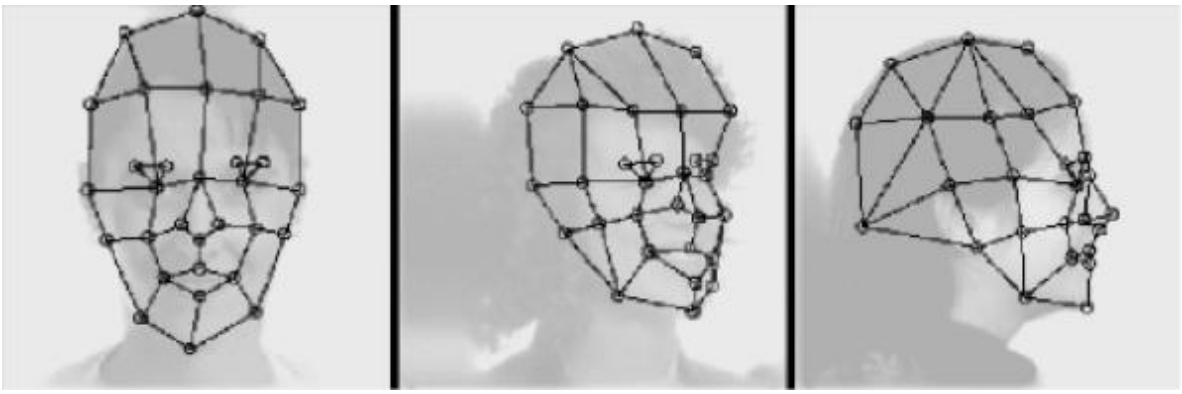


Figura 3. Aplicación de algoritmo para la obtención de puntos especifico. (Biometric Computer Technology in Healthcare Forensics, s.f.)

Pero ya que la cara es una parte del cuerpo que va envejeciendo y se notan sus cambios tales como arrugas, caída de cabello, expresiones faciales, variaciones de posición, o igual no tanto por el tiempo sino puede pasar algún accidente al individuo y puedan cambiar características de la cara ya no sería igual, entonces es difícil que se crea un mecanismo que pueda ser una autenticación biométrica facial. Puesto para crear el mecanismo se tendría que estar actualizando a ciertos años.

5.2.1.2 Biometría mano

Los sistemas de autenticación biométrica por la mano tiene la ventaja de ser sistemas rápidos y con poca posibilidad de error, algunos sistemas en segundos son capaces de determinar la autenticación de la persona.

La obtención de la imagen es simple ya que solo se requiere el sistema que el capture la imagen de la mano del individuo, estaba basado en la información presentada en una impresión. Pero para estos sistemas se necesitan escáneres de mano con un precio elevado.

Para obtener los datos biométricos necesarios en este tipo de tecnología se hace uso de una cámara digital de baja resolución. La mano se coloca con la palma hacia abajo sobre una superficie plana que tiene 5 clavijas, que ayudan a alinear los dedos de la mano para asegurar una lectura exacta (ver figura 4). La cámara captura entonces la imagen de la palma de la mano y su sombra. En la parte izquierda de la superficie plana, se coloca un espejo formando un ángulo de 60 grados; este espejo refleja hacia la cámara el perfil lateral de la mano (ver figura 5). (Perez, s.f.)

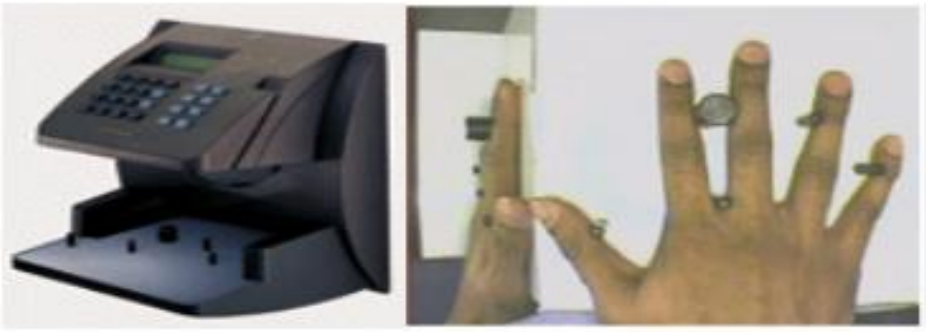


Figura 4. Ejemplo de escáner biométrico para la mano. (Alexei, 2011)

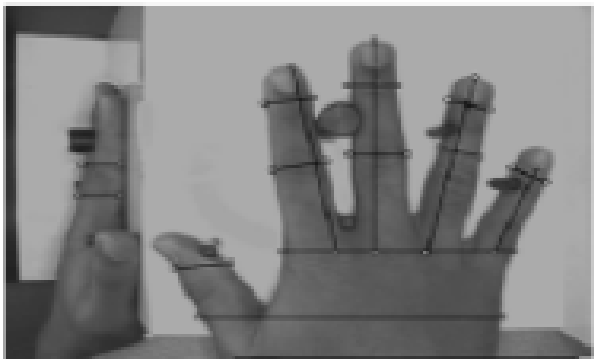


Figura 5. Características de la geometría de obtención de la mano. (Alexei, 2011)

En la captura completa de la mano por lo general se deben realizar tres o cuatro tomas según el estándar ANSI INCITS 396-2005 Hand Geometry Interchange Format (Biometrics, Hand Geometry, 2006).

Debido a la poca capacidad para distinguir a diferentes usuarios y debido los costos que puede generar la obtención de un sistema de estos, este método solo se utiliza en procesos de verificación.

5.2.1.3 Biometría ADN

La técnica se basa en que dos seres humanos tienen una gran parte de su secuencia de ADN en común y para distinguir a dos individuos se puede explotar la repetición de secuencias altamente variables llamada microsatélites. Dos seres humanos no relacionados será poco probable que tengan el mismo número de microsatélites en un determinado locus.

En el SSR/STR de perfiles (que es distinto de impronta genética) la reacción en cadena de polimerasa (PCR) se utiliza para obtener suficiente ADN para luego detectar el número de repeticiones en varios Loci. Es posible

establecer una selección que es muy poco probable que haya surgido por casualidad, salvo en el caso de gemelos idénticos, que tendrán idénticos perfiles genéticos pero no las huellas dactilares.

La huella genética se utiliza en la medicina forense, para identificar a los sospechosos con muestras de sangre, cabello, saliva o semen. También ha dado lugar a varias exoneraciones de condenados. Igualmente se utiliza en aplicaciones como la identificación de los restos humanos, pruebas de paternidad, la compatibilidad en la donación de órganos, el estudio de las poblaciones de animales silvestres, y el establecimiento del origen o la composición de alimentos. También se ha utilizado para generar hipótesis sobre las migraciones de los seres humanos en la prehistoria.

El ADN es un rasgo ampliamente utilizado en entornos forenses y policiales. No obstante, presenta una serie de inconvenientes que limitan su uso en otras aplicaciones. Incluso hay autores que por esa razón no lo consideran un rasgo biométrico propiamente dicho. En primer lugar, presenta problemas de privacidad importantes, ya que a partir del ADN puede extraerse información sobre ciertas enfermedades. Por otro lado, el reconocimiento ha de realizarlo un experto en un laboratorio químico, proceso que puede llevar al menos varias horas. Es por ello que en este momento no hay posibilidad de tener un sistema totalmente automático, barato y que permita operar en tiempo real.

- ADN: El ácido desoxirribonucleico es el código unidimensional que caracteriza al individuo por excelencia, excepto a dos gemelos idénticos, que tienen el mismo
- ADN. Normalmente, se usa en la identificación de personas en aplicaciones forenses, pero no se puede emplear en aplicaciones de tiempo real debido a que se necesita un tiempo de unas horas en un laboratorio para aislar correctamente el ADN.

- ADN y extraer la información básica. Además, el uso de la información del ADN suele preocupar a las personas porque se puede extraer el conocimiento de que una persona sufre ciertas enfermedades o es susceptible de que las sufra.

5.2.1.4 Biometría huella digital

Este sistema de biométrica por huella digital es el más utilizado para la autenticación de una persona, ya que solo se necesita de la mano (específicamente los dedos de la persona), se sabe que la huella es única, ni los gemelos tienen la misma huella dactilar. Desde que se nace a los primeros días en el registro de nacimiento se utiliza la huella para identificar al niño e igual es utilizada por los forenses para detectar si la persona que falleció es la misma que presuntamente de ha identificado.

La huella dactilar es una característica de la persona que nunca va a cambiar ni con el paso del tiempo, ya que existen estudios científicos donde se comprueba esto.

Las huellas dactilares son características que distinguen a los seres humanos de manera única. La ciencia que se dedica a estudiar este rasgo es la dactiloscopia (Hernández A. , 2009). Los sistemas dactiloscópicos están basados en principios (Instituto de Ciencias Forenses, 2010):

- Inmutabilidad: las huellas dactilares no son modificadas durante el desarrollo físico de una persona y no pueden ser afectadas por una enfermedad, en caso de que las huellas sean afectadas por un desgaste involuntario estas tienen la capacidad de regenerarse tomando su forma original en un periodo de 15 días.

- Variabilidad, No existen dos personas con la misma huella dactilar, son únicas e irrepetibles, se encuentra genéticamente ligadas y contiene más de 20 puntos característicos
- Clasificabilidad: las huella tienen patrones que se forman con sus crestas que hace posible la clasificación esto se utiliza para la localización fácilmente.

Agrupamiento que conforman el sistema Crestales

1. Basilar: Situada en la base de la yema del dedo, creado de crestas transversales, a partir de este se hacen las características principales para su jerarquía en la huella dactilar (ver figura 6).

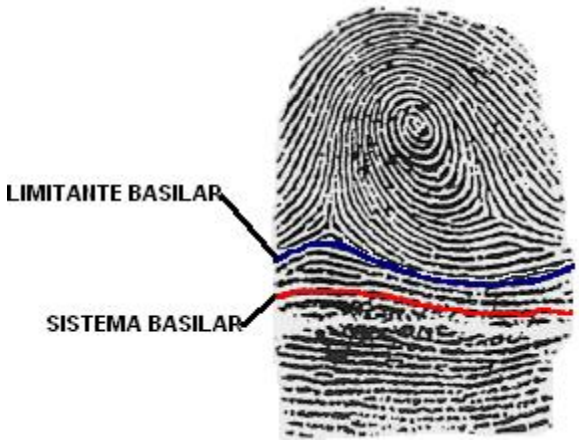


Figura 6. Parte y limitante de basilar (Ballester, s.f.)

2. Nuclear. Situada en la parte central de la yema del dedo, entre la basilar y marginal, son las crestas más internas llamada también generatriz de núcleo (ver figura 7).

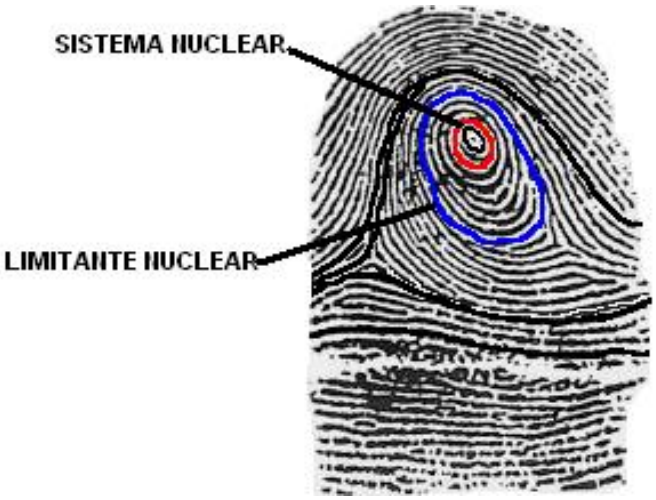


Figura 7. Parte limitante y sistema nuclear. (Ballester, s.f.)

3. Marginal. Situada en la parte superior de la huella, formada por crestas arqueadas siguiendo su curso a la uña (ver figura 8).

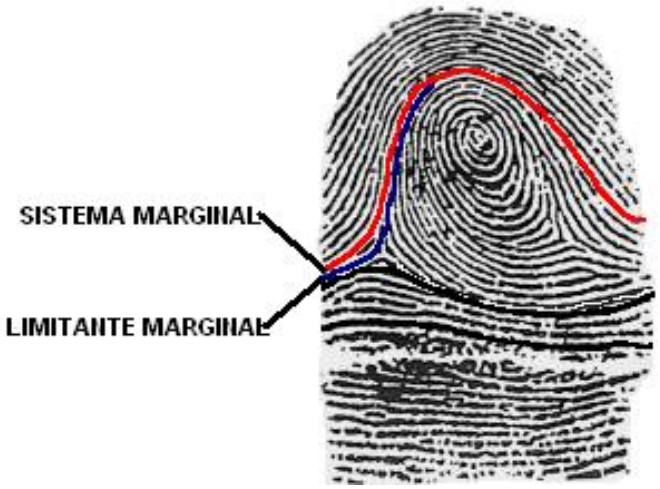


Figura 8. Parte Limitante marginal y sistema marginal. (Ballester, s.f.)

Francis Galton realizo un detallado estudio de las huellas dactilares y establece los puntos característicos necesarios para la asociación de huellas dactilar en 1888. (García, s.f.) Estos puntos su principal característica es la definición por

puntos, las líneas son las terminan o se bifurcan es mejor conocido como la técnica minucias (ver figura 9).

Figura 9. Tipos de Minucias

Al igual hay otros puntos de la huella dactilar donde la curvatura de las rugosidades es máxima se les llama como núcleos y deltas. Su principal característica tanto las minucias como los puntos de la huella dactilar que son únicos en cada persona y nunca se alteran en el transcurso de los años (ver figura 10).

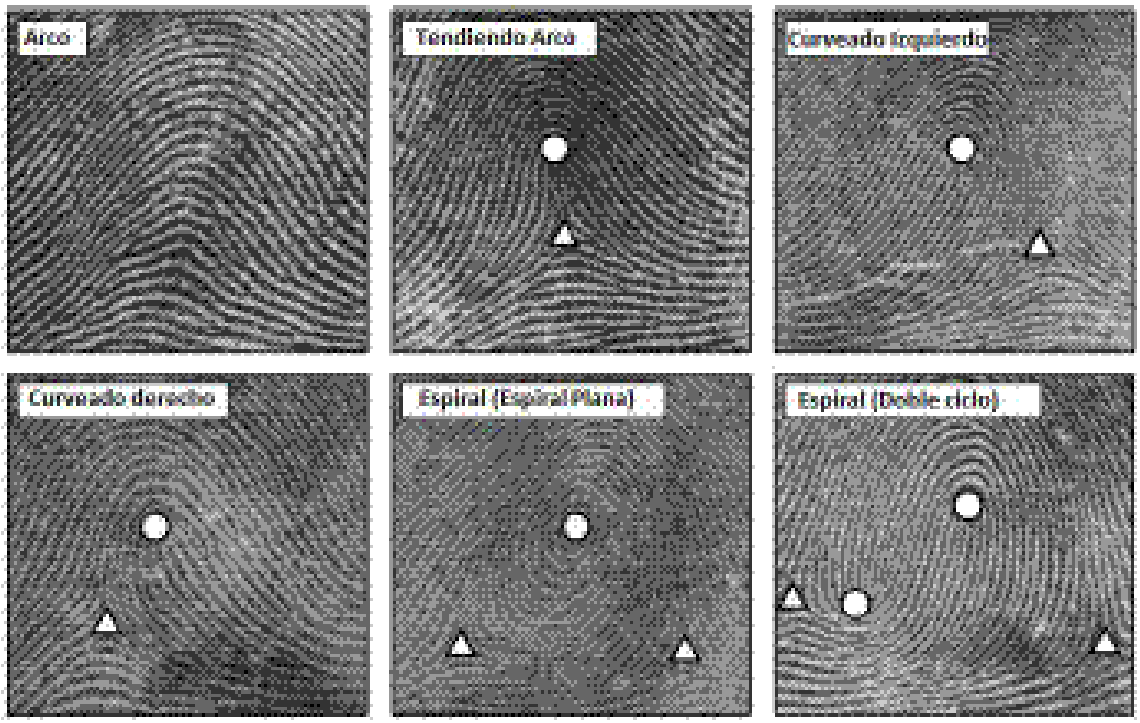


Figura 10. Característica globales (Flores, 2014)

Los Arcos se basan por no tener deltas en su dibujo y sus crestas corren de un lado a otro sin volver en sí mismas. Los Arcos teniendo área son parecidos al arco normal la diferencia que cuenta con un delta y una curva que asemejan una casa de campaña.

Las curveada izquierda son llamadas también como presillas internas, estas se caracterizan por tener un delta a la derecha y por qué el núcleo nace a la izquierda y corren hacia la derecha dando vuelta sobre sí mismas, para salir al mismo lado de salida.

La curveada derecha son llamadas presillas externas, se caracterizan por que cuentan con un punto delta que se ubica a lado izquierdo y porque el núcleo nace a la derecha y su recorrido es a la izquierda para dar vuelta sobre sí mismas y regresar al mismo punto de partida

La espiral doble y espiral doble ciclo son llamadas como Verticilo, ya que su dibujo en algunas ocasiones son similares a las flores, cuentan con dos puntos delta, uno del lado derecho y otro de lado izquierdo, su núcleo puede adoptar formas circulares, elípticas y espirales. En este tipo de dibujos se puede dividir en verticilos simples y verticilos dobles, su característica principal es que en el núcleo del primero sólo se encuentran una curva mientras en el segundo se encuentran dos.

5.2.1.1 Biometría retina

La retina es la capa de tejido sensible a la luz que se encuentra en la parte posterior globo ocular. Las imágenes que pasan a través del cristalino del ojo se enfocan en la retina. La retina convierte entonces estas imágenes en señales eléctricas y las envía por el nervio óptico al cerebro. (Tango, 2015)

Ya que la estructura de las venas que están dentro de la retina es muy compleja hace hacerla única para cada persona, es tan compleja que ni dos personas (gemelos) tiene la misma retina. Al igual que el iris esta tecnología ha sido muy efecto en el momento de autenticar un individuo. Principalmente se basa en la lectura de las pequeñas venas que se encuentran dentro de la retina, la cual es la que capta la luz que estamos observando.

La base de los identificadores biométricos para retina es mapear los patrones únicos de la retina. La función es cuando los vasos sanguíneos de la retina absorben la luz con un gran rapidez para identifica con mayor facilidad ina iluminación apropiada.

Para la identificación de una persona aplicando el sistema de retina la persona debe mirara través de unos binoculares, donde debe mirar en un punto

fijo para que no mueva la mirada (ver figura 11). El sistema escanea la retina con una radiación infrarroja de poca intensidad en forma de espiral, donde detecta las características de la retina (nodos y ramas de la retina), el sistema verifica si estas características coinciden con una que este en encuentra en su base de datos.

La desventaja de esta tecnología que es cara puesto que para la captura de la imagen de la retina se debe realizara a través de una luz infrarroja a la cual es una tecnología cara y poco aceptable. Otra desventaja y esta son mas de confianza puesto las personas no confían en que un rayo analice su ojo, entre que les puede dañar el ojo y como alunas personas conocen que a través de este medio se puede conocer algunas enfermedades de la persona en cuestión.

Figura 11. Sistema donde se escanea la retina. (Introducción a la Seguridad Biométrica, 2015)

5.2.1.2 Biometría iris

El iris es la parte coloreada del ojo, estas se encuentra entre la córnea y el cristalino. La abertura redonda y central del iris se denomina pupila. Músculos muy pequeños dentro del iris hacen que la pupila se haga más pequeña y más grande para controlar la cantidad de luz que entra al ojo. Esto le permite ver bien en condiciones más iluminadas o más oscuras (Tango, 2015).

La autenticación de iris emplea técnicas matemáticas para reconocimiento de patrones en imágenes de una persona, ya que los patrones son único y se pueden distinguir a cierta distancia. Este utiliza tecnología de cámara con una sutil iluminación infrarroja para adquirir imágenes de las intricadas estructuras del iris (ver figura12).

Las matrices digitales codificadas de esos patrones mediante algoritmos matemáticos y estadísticos permiten la identificación positiva de un individuo. La búsqueda en las bases de datos de las matrices registradas se realiza mediante motores de asociación a velocidades que se miden en millones de matrices por segundo, y las tasas de falsa coincidencia son cifras infinitesimales (Trade, 2014)

El reconocimiento de iris es más moderna que el reconocimiento por retina, para la captura de la imagen del iris se hacía en blanco y negro, esta imagen es sometida a deformaciones pupilares y aquí es cuando se extraen los patrones que a su vez se realizan trasformaciones matemáticas para obtener cierta cantidad de datos para en un futuro se realice su autenticación.

Para la imagen del iris se requiere el uso de una cámara digital de alta calidad. De hoy comercial iris cámaras típicamente utilizan luz infrarroja para iluminar el iris sin causar daño o malestar al sujeto. En proyección de imagen un iris, una wavelets de Gabor 2D filtros y mapas de la segmentos del iris en fasores.

Estos fasores incluyen información sobre la orientación y la frecuencia espacial (ver figura 13).

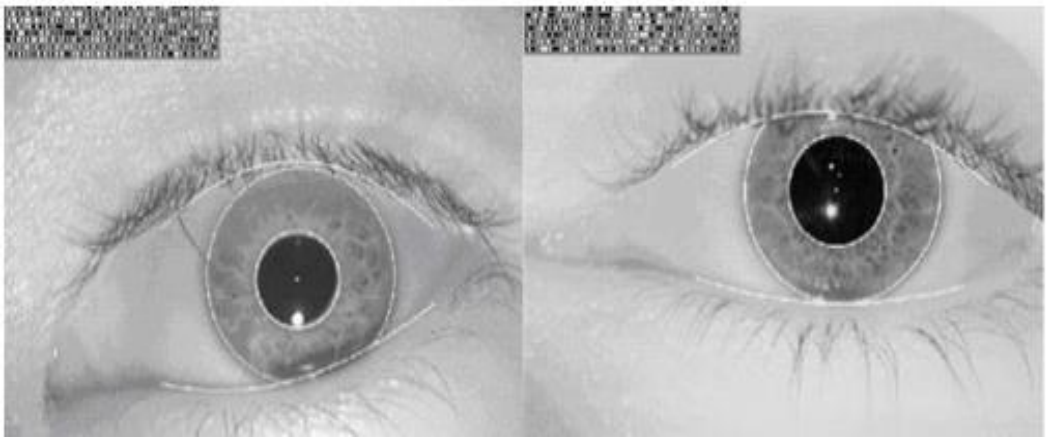


Figura 12. Ubicación de iris con IrisCode (Biometrics, DynamicSig, 2006)

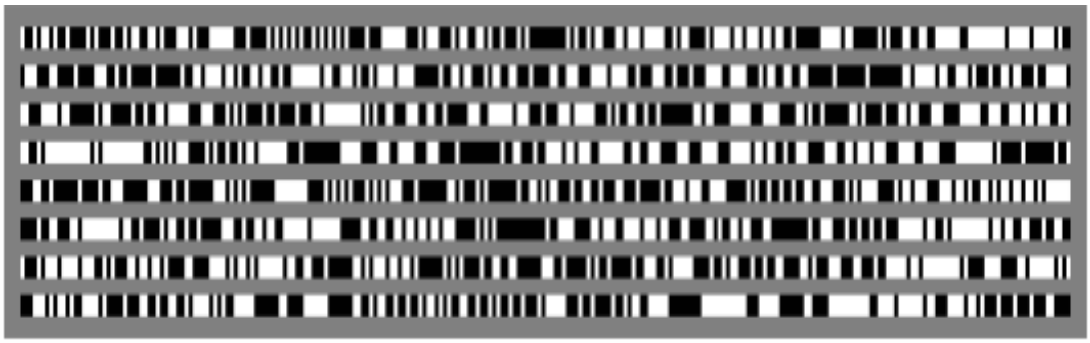


Figura 13. Representación de IrisCode. (Biometrics, DynamicSig, 2006)

5.2.2 Sistema de comportamiento

Este sistema es basado en acciones del individuo ya que a lo largo de su vida puede tener muchas alteraciones, pero es necesario tomarlo en cuenta en estas

técnicas ya que aún pude ser identificada una persona aunque ya haya habido ciertos cambios. Un ejemplo es la firma de la persona, por lo regular la manera de realizar la firma va hacer la misma.

5.2.2.1 Biometría firma o escritura

Hay que recordar que dentro de la biometría la firma o escritura no es una característica especial pero dentro de esta categoría sistemas de comportamiento, básicamente en este método se autentican ciertos rasgos como su rúbrica no tanto su interpretación de lo que escribe el individuo, la forma que un individuo escribe es un rasgo biométrico.

Las firmas han sido un mecanismo de autenticación de la persona que ha sido utilizado desde la antigüedad. Y ahora en nuestro tiempo se sigue utilizando, puesto la firma es como la huella digital de la persona que deja. Aunque la firma en algunos individuos varía en ciertas ocasiones, la simetría es lo que hace la autenticación. Una desventaja de este mecanismo es que puede ser falsificado de manera fácil, puesto que existen personas en falsificar firmas que al ojo humano son idénticas.

Existen dos grandes técnicas para la adquisición de la firma.

- Técnica off-line: son las firmas que se realizan sobre papel, ya que esta firma no se realiza en un sistema para la obtención de sus características.es decir se realiza la firma en un tiempo y la captura de esta firma de da en otra ocasión.
- Técnica on-line: son las firmas que se realizan en dispositivos como pueden ser tabletas digitalizadoras o acelerómetros acoplados a bolígrafo he incluso ya se realizan en algunos Smartphone. Es esta técnica al momento de realizar la firma los datos también son capturados y no se tiene que ser en otro momento indeterminado.

El patrón que se debe tomar en cuenta para la identificación de una firma son (Biometrics, DynamicSig, 2006):

- Estáticos o geométricos: se debe consideran una serie de coordenadas (X , Y , Z), las coordenadas X y Y determinan dentro de un plano cartesiano la posición de los diferentes símbolos de la firma mientras que la coordenada Z determina si se despegó la pluma de la pizarra (ver figura 14).

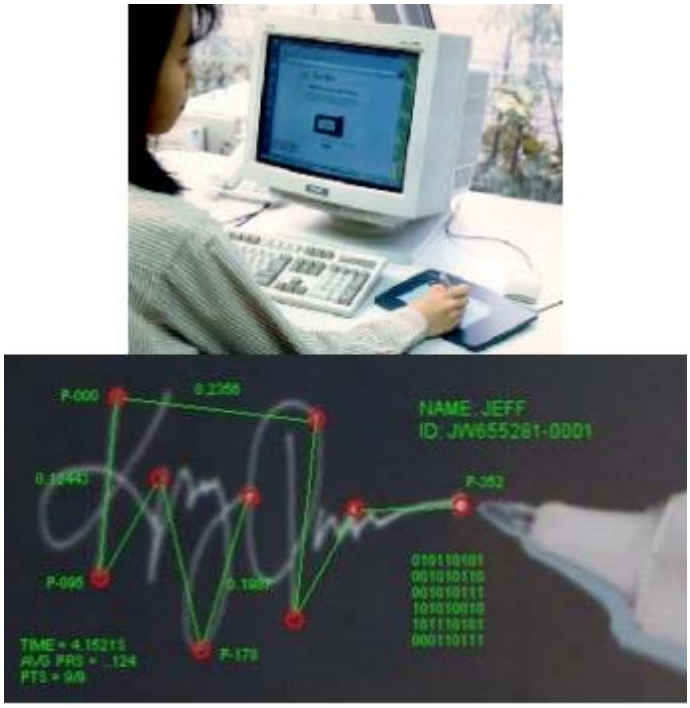


Figura 14. Ejemplo de hardware y software, donde se realiza una firma electrónica y se tiene diversas mediciones y se procesan comparacione (Biometrics, DynamicSig, 2006)

- Dinámicos: en este caso se considera características tales como la velocidad, la aceleración, el tiempo, la presión y la dirección, como también algunos también determinan el ángulo con el que se tomó la pluma, estas características son tomadas mientras el individuo realiza la firma (ver figura 15).

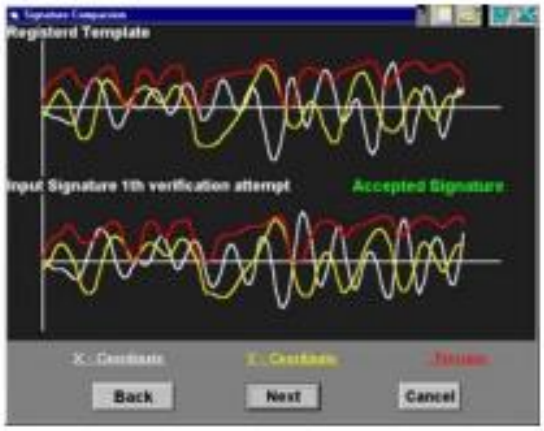


Figura 15. Grafica de las características dinámicas de la firma (Biometrics, DynamicSig, 2006).

Esta técnica es autenticación a través de la firma o escritura es muy utilizada, para realiza cualquier trámite por lo regular en los bancos o tramites gubernamentales se piden que realicen una firma a través de un dispositivo para tener guardad la información de su firma, para en un futuro si se realiza otros tramite se pueda autenticar que es la persona que dice que es.

5.2.2.2 Biometría de voz

Este sistema es de los más fáciles de realizar el proceso de obtención de datos ya que en este mecanismo el individuo no espera a una cantidad de fotografías que se le debe tomar como la biometría facial.

Para realizar la autenticación del individuo con este mecanismo se debe tener en cuenta varias condiciones para la mayor calidad de audio que se pueda tener tratando de eliminar ruidos, ecos entre otras cosas.

En el momento que el individuo dese acceder al sistema debe de pronunciar una frase la cual ya tuvo que a ver obtenido los datos de la voz, como mecanismo de seguridad se guarda una frase para que se puede ingresar con la misma frase por ejemplo el nombre completo del individuo, u otra frase. El sistema debe ser capaz de almacenar una o más frases dependiendo la capacidad al que se le configuro.

Existen dos modalidades para el reconocimiento de voz, las cuales son (Recognition, 2006)

- Dependiente del texto (modo limitado): esta modalidad el sistema utiliza una frase determinada para que el individuo la pueda decir como contraseña por ejemplo “Mi contraseña es 12345”.
  Esta frase después que fue capturada se transforma de mono analógico(a través de un micrófono) a digital, después se obtiene las características para continuar en la creación de un modelo gráfico.

  En la mayoría de los sistemas utilizan el concepto de Modelos Markov Ocultos (HMMs), que básicamente son modelos que proveen de una representación estadística a los sonidos producidos por el individuo. El HMM utiliza la voz para crear un número de vectores de estado que representan las variaciones de las formas del sonido, que son características de la fisiología y el comportamiento de un individuo. Una vez que se a tomado una muestra y ha sido guardada en una base de datos un individuo puede ser identificado cuando este pronuncia la frase guardada, se consideran las mismas características de calidad, duración, volumen y tono para extraer los patrones y compararlos con el modelo de la identidad, o hipotética identidad. Si el modelo de voz identificado no es reconocido se le denomina anti voz. La muestra de la voz es comparada para producir un radio de similitud, si el individuo es legítimo la prueba será

positiva de lo contrario se indicará que la voz no es reconocida (ver figura 16).

- Independiente del texto (modo ilimitado): Este modelo en lugar de tomar una frase o frases para ser identificadas, toma las características generales del espectro de Marco teórico Biometría 44 voz. Para realzar el análisis se deben considerar los niveles bajos y niveles altos del espectro. Las investigaciones actuales en el área de reconocimiento de voz independiente del texto están concentradas mayormente en el nivel bajo. Dentro del nivel bajo se consideran las características básicas de la señal captada tales como: amplitud, periodo de muestreo, frecuencia, etc. Mientras que las de alto nivel incluyen: funciones prosódicas como el ritmo, la velocidad, la modulación y entonación, tipos de personalidad e influencia parental, semántica, pronunciación, relaciones con el lugar de nacimiento, estatus socio-económico, etc. La fusión de características de alto nivel con la información de bajo nivel de espectro se está convirtiendo en una técnica muy popular en los laboratorios ya que ha permitido mejorar los métodos de reconocimiento de voz para texto independiente.

Una desventaja de este sistema es que la persona puede que varié dependiendo a diversos factores s como por ejemplo la salud del individuo digamos que puede estar enfermo de la garganta, una gripe entre otras cosas que se le provoque que en ese momento su voz sea más grave de lo normal. También es un sistema el cual puede ser engañado ya que hay mecanismo que pueden grabar la voz de un individuo y replicarla con las palabras que dese decir. Entre otro factor es que hay personas que son buenas imitando voces a lo que lleva a fraudes.

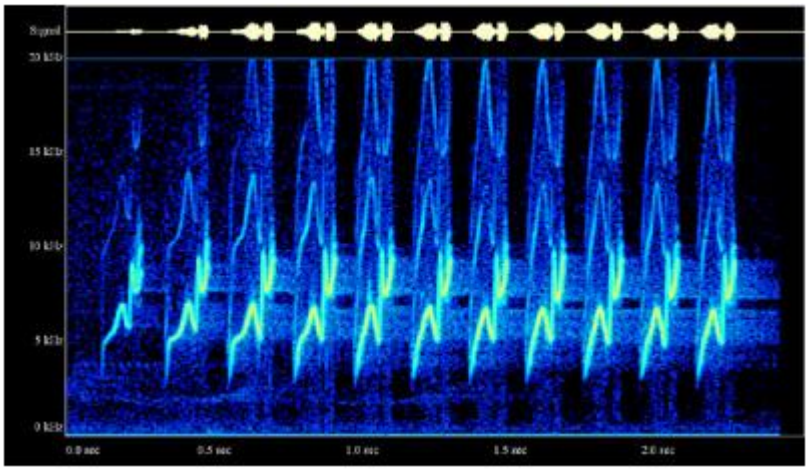


Figura 16. Representación de una voz entrante (parte superior de la imagen) muestra el volumen de entrada con respecto al dominio del tiempo (parte azul de la imagen) . (Recognition, 2006)

5.2.2.3 Otras

Formas de andar.

Las personas tienen una manera particular de andar también es un rasgo biométrico espacio-temporal. Aunque pueda ser una forma muy rara de autenticar una persona, cada persona tiene una manera de andar particular, así como puede caminar muy rápido como una manera lenta, si mueve un pierna más que otra pierna, las personas tenemos a balancearnos más de una pierna que otra,

Es utilizada más para el seguimiento e identificación de una persona pues para este sistema se necesita hacer la medición y comportamiento a distancia. La gran desventaja de este sistema es que la forma de andar puede variar mucho

por ciertas situaciones, ya que puede tener una lesión que hace que una persona camine coja, lesión en una articulación o por el mismo paso del tiempo (envejecimiento).

5.3 Aplicaciones

Los sistemas biométricos se piensan más para las organizaciones que buscan métodos de autenticación más seguros para el acceso del usuario, para comercio electrónico y otras aplicaciones de seguridad.

Algunas de las tecnologías biométricas que se manejan anteriormente son consideradas para diferentes segmentos de mercado. Las más conocidas son las huellas dactilares, reconocimiento de cara y reconocimiento de iris. La tabla 1 se maneja las diferentes tecnologías, las posibles aplicaciones y los principales mercados que se pueden utilizar ya sean en el sector privado o público que ofrece la industria biométrica.

Algunos nuevos usos de estas técnicas todavía se ampliaran más dado que la fiabilidad del sistema está presentado como un ejemplo en año 2016 se maneja el sistema de autenticación de iris y huella digital en un Smartphone.

Tabla 1. Diferentes Tecnologías en la Industria Biométrica

Tecnología	***Aplicación Horizontal***	***Principales mercados verticales***

AFIS/Lifescan	Controles de Vigilancia	Servicios policiales y militares
Reconocimiento de cara	Identificación sin contacto	Farmacéuticas, Hospitales, Industria pesada y Obras
Geometría de Mano	Identificación Criminal	Hospitales y Sector Salud
Reconocimiento de iris (ojo)	Acceso a sistemas	Industria manufacturera
Reconocimiento de Voz	Acceso a instalaciones	Viajes y Turismo
Escritura y Firma	Vigilancia	

Fuente: (Newzzniper, 2015)

Otros usos

Seguridad en la movilidad y accesos Aeropuertos, fronteras, centrales eléctricas, centros de control de suministro, instalaciones industriales, instituciones públicas, control hospitalario de neonatos

Seguridad en las transacciones: comercio electrónico y banca como por ejemplo cajeros automáticos, verificación de uso de tarjetas de crédito en comercios, pago por Internet.

Seguridad en el acceso y firma de documentos electrónicos como por ejemplo sector sanitario, industrial, administración pública, comercio, actas notariales. Validación de firma digital, sistemas de voto electrónico y voto por internet.

Seguridad en el acceso a equipos industriales como por ejemplo maquinaria que sólo deba ser utilizada por personal específicamente formado.

Aplicaciones comerciales como por ejemplo las tecnologías tradicionales de las que disponemos utilizan sistemas basados en el conocimiento y en muestras.

5.4 Comparativo de sistemas

La tabla 2 es la recolección de las diferentes características de los sistemas biométricos.

Tabla 2. Características de los sistemas biométricos con pros y contra de acuerdo al sistema biométrico.

Características	*Aceptación del Usuario*	*Facilidad de uso*	*Cote*	*Utilidad (identificación)*	*Utilidad (Verificación)*	*Estabilidad*	*Intrusismo*	*Fiabilidad*
ADN	Baja	Baja	Alto	✓	✓	Alta	Muy alto	Alta
Dinámica de escritura	Alta	Alta	Bajo	✗	✓	Baja	No	Baja
Firma	Media	Alta	Bajo	✗	✓	Media	No	Baja
Geometría de la mano	Media	Alta	Alto	✗	✓	Media	No	Media
Huella dactilar	Media	Alta	Bajo	✓	✓	Alta	No	Alta
Iris	Media	Media	Alto	✓	✓	Alta	No	Alta
Reconocimiento facial	Media	Media	Bajo	✗	✓	Media	Bajo	Media
Retina	Media	Baja	Alto	✓	✓	Alta	Alto	Alta
Voz	Alta	Alta	Bajo	✗	✓	Media	No	Baja

Fuente: Elaboración Propia

La tabla 3 es la recolección de nivel de seguridad para las diferentes características de los sistemas biométricos

Tabla 3. Nivel de seguridad de los sistemas biométricos.

Característica	*Nivel de Seguridad*	*Ratio de error*	*Precisión*	*Errores*	*Falso Positivo*	*Falso Negativo*
ADN	Alto	Sin datos	4	No conocido.	5	5
Dinámica de escritura	Medio	Sin datos	1	Lesiones de mano, cansancio.	4	1
Firma	Medio	1/50	2	Cambios de escritura.	2	1
Geometría de la mano	Medio	1/500	3	Edad, lesiones varias.	4	2
Huella dactilar	Alto	1/500	4	Sequedad, suciedad, edad.	5	5
Iris	Alto	1/131,000	4	Iluminación inadecuada.	4	4
Reconocimiento facial	Medio	Sin datos	3	Pelo, gafas, edad, iluminación	3	1
Retina	Alto	1/10^6	4	Gafas, lentillas	5	5
Voz	Medio	1/50	2	Ruidos ronquera, resfriado	2	1

Fuente: Elaboración Propia

El mercado en la actualidad tiene muchas opciones de tecnología biométrica, en el cual puede variar dependiendo las necesidades del cliente. En la figura 17 se muestra las principales tecnologías biométricas y que porcentaje abarca en el mercado.

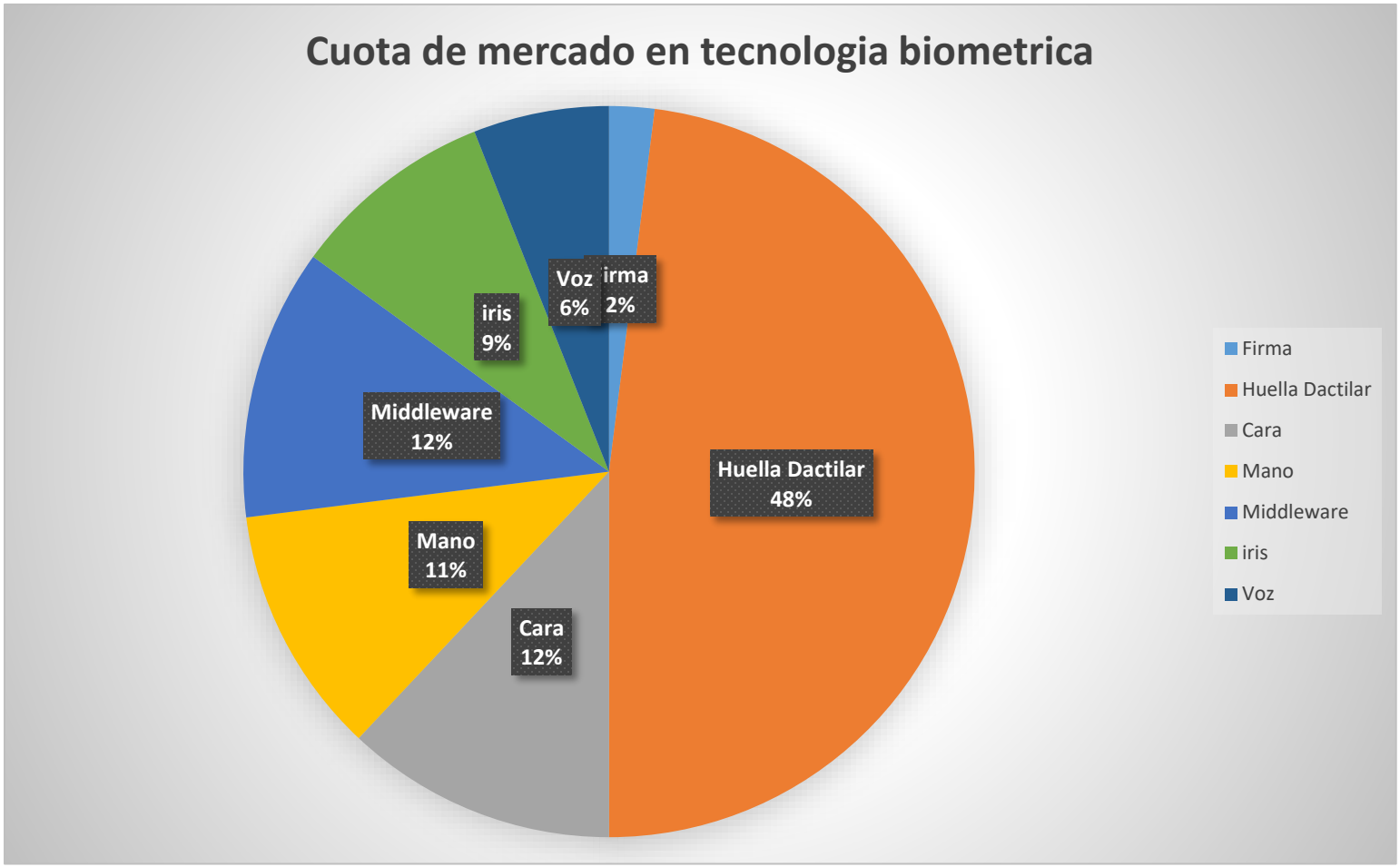


Figura 17. Cuota del mercado en tecnología biométrica al sistema biométrico.

5.5 Propuesta de diseño del sistema

La intención de la tecnología de huella digital es identificar de manera precisa y única a una persona por medio de su huella digital. Certificando la autenticidad de las personas de manera única e inconfundible por medio de un dispositivo electrónico que captura la huella digital y de un programa que realiza la verificación.

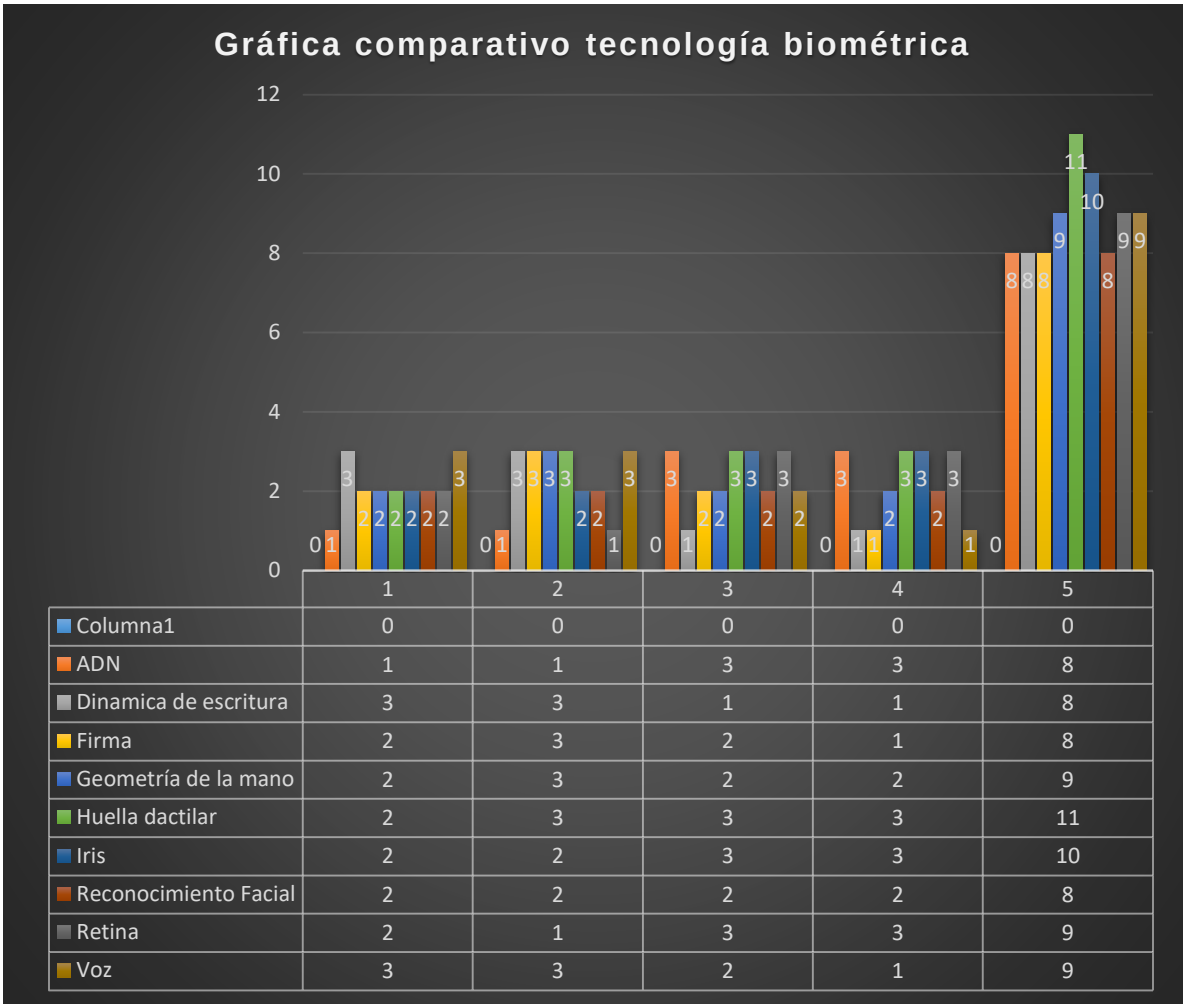
La tecnología de huella digital ha ido avanzando rápidamente, y cada vez es más asequible para muchas aplicaciones y cada vez, es más exacta y difícil de falsificar. Cada vez es más común encontrar sensores de huella digital para asegurar la autenticidad de una persona. La huella digital se utiliza desde relojes checadores hasta acceso a información confidencial e incluso, existen ya, celulares que identifican al usuario propietario de un teléfono celular (Huella digital, 2014)

En esta etapa se desarrollara el sistema después de haber realizado previamente el análisis del conjunto de características necesarias para poder implementar la propuesta del sistema de control asistencia y de acceso. Se utilizara el modelo lineal secuencial del desarrollo del software que cuenta con el análisis, diseño, implementación y pruebas.

Dentro de la investigación se concluye que la propuesta del sistema de control de autenticación para el control de asistencia y control de acceso cuenta con una gran utilidad y apoyo al personal correspondiente de la seguridad de la empresa ya que facilita el control sin contar con mucho personal que pueda corrompió con sus deberes y de acceso a la manipulación de la información como por ejemplo en la manipulación del control de asistencia, que el encargado pueda manipular la tarjeta u el reloj checador para otorgar un horario que es erróneo y así no tener consecuencias de su retardo del empleado.

Al mismo tiempo el sistema contara con un reporte previamente digital que las personas encargadas de la asistencia y control de acceso puedan tener acceso

a ellas previamente haber iniciado sesión como administradores, asi se ahorrar en papel que anteriormente se ocupaba en el registro de las listas.



	1	2	3	4	5
Columna1	0	0	0	0	0
ADN	1	1	3	3	8
Dinamica de escritura	3	3	1	1	8
Firma	2	3	2	1	8
Geometría de la mano	2	3	2	2	9
Huella dactilar	2	3	3	3	11
Iris	2	2	3	3	10
Reconocimiento Facial	2	2	2	2	8
Retina	2	1	3	3	9
Voz	3	3	2	1	9

Figura 18. Grafica comparativa tecnología biométrica.

A partir de esta tabla se puede deducir que al combinar dos sistemas de autenticación se podrá tener un mejor control de autenticación biométrica. En esta propuesta se toma los dos sistema que contiene una calificación más alta en la comparación, se utilizara la tecnología biometría de Iris y huella dactilar (ver figura 18).

Para el desarrollo de un Sistema Automático de Identificación de huellas dactilares se deben de considerar principalmente al menos cuatro etapas designadas: adquisición, representación, extracción de características y asociación.

Adquisición. En esta primera etapa se obtiene la imagen de la huella dactilar, para lo cual se pueden emplear dos métodos: fuera de línea y escaneo en vivo, paso siguiente la imagen se debe de representar en un formato apropiado para su posterior procesamiento.

Representación. Esta etapa constituye la esencia de la verificación de huellas dactilares y se refiere a la representación obtenida ya que en esta la información invariante y discriminatoria contenida en la imagen de la huella dactilar es capturada. Representaciones de la imagen de la huella dactilar basadas en escala de grises prevalecen entre los sistemas de verificación que emplean asociación óptica. Sin embargo el desempeño de los sistemas usando este tipo de representación puede estar limitada por factores que afectan la calidad de la imagen, tales como variaciones de brillo, cicatrices, distorsiones globales, etc. Esto a consecuencia de que estos sistemas usualmente recurren a plantillas estratégicas de asociación.

Extracción de Características. El extractor de características del sistema tiene la finalidad de encontrar y localizar los puntos característicos contenidos en la imagen entrante de la huella dactilar. Si las rugosidades pueden ser perfectamente localizadas el proceso de extracción de minucias es solamente una tarea trivial de extracción de puntos característicos sobre el mapa de rugosidades. Sin embargo, debido a un gran numero de factores tales como aberrantes formaciones de la epidermis en las rugosidades de los dedos, marcas postnatales, marcas ocupacionales, imperfecciones adquiridas por el escáner, etc., en las imágenes obtenidas de las huellas dactilares puede que no siempre este bien definida la estructura de las rugosidades, además de que no siempre es posible obtener un mapa perfectamente definido de rugosidades.

Debido al efecto de estas circunstancias, el desempeño del algoritmo de extracción de minucias va a depender fuertemente de la calidad de las imágenes obtenidas. Por lo que bajo estas circunstancias, los algoritmos de extracción de minucias se convierten en problemas de gran complejidad con un alto costo computacional.

Asociación. En esta etapa dos imágenes de huellas dactilares dadas llamadas prueba y referencia, los componentes de asociación del sistema determinaran si las imágenes almacenadas son impresiones del mismo dedo. Usualmente en este modulo se determina una medida de similitud entre las dos huellas dactilares y se define un umbral para decidir si el par de huellas dactilares empleadas pertenecen o no a la misma persona.

5.5.1 Herramientas

Después de un análisis de los diferentes dispositivos que existen actualmente en el mercado se tomaron para el lector de huella dactilar el BioEntry Plus ya que cuenta con características que son factor para una mejor seguridad y también habla en costo no es muy alto a comparación de otros dispositivos.

BioEntry Plus

Control de acceso seguro, rápido y fácil de administrar con funcionamiento autónomo o en red. Opcionalmente modelo BioEntry W con protección IP65.

Suprema BioEntry Plus es un terminal de control de acceso biométrico de huella dactilar, fácil de instalar y utilizar (ver figura 19).

El terminal biométrico BioEntry Plus incluye identificación por huella dactilar y tarjeta de radiofrecuencia y cubre una amplia variedad de aplicaciones de control de acceso, desde un simple control de entrada autónomo hasta una compleja red de control de acceso.

Figura 19. Imagen de lector de huella dactilar BioEntry Plus.

Iris UltraMatch

La serie ANVIZ ULTRAMATCH posee un diseño elegante y de rendimiento robusto. Adoptando el algoritmo BioNano, el sistema proporciona el más preciso, estable y rápido reconocimiento del iris al tiempo que ofrece seguridad de alto nivel en la inscripción biométrica, identificación individual y control de acceso (ver figura 20).

Contiene un sistema de patrón complejo y aleatorio ya que el sistema de iris es único y estable ya que presenta menos afectaciones/daños físicos durante la vida del usuario. El reconocimiento del iris se convierte en la opción más precisa y más rápida para autenticar a alguien con certeza.

Figura 20. UltraMatch modelo S1000. (Kimaldi Electronics, s.f.)

5.5.2 Recopilación de datos

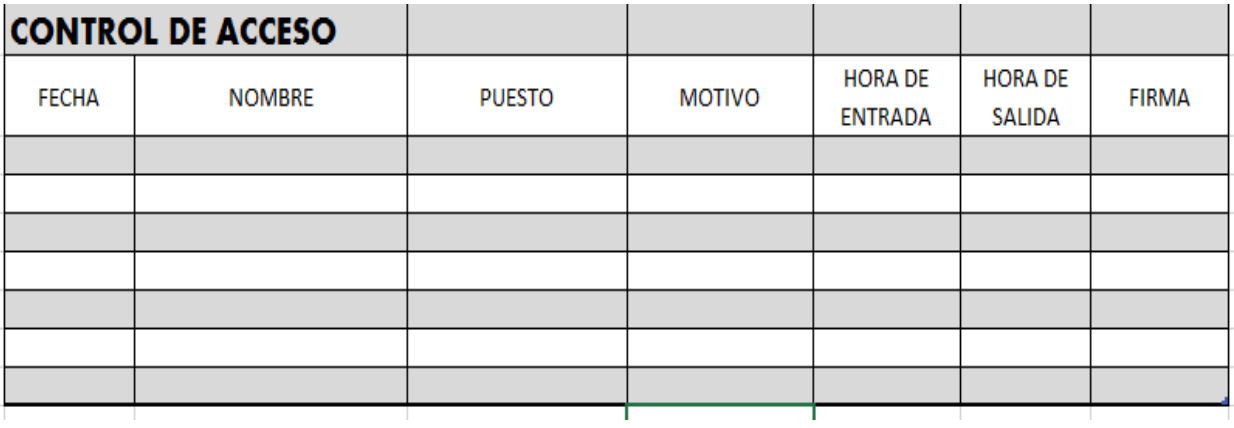
Dentro de esta fase anteriormente se manejaba el formato (ver figura 22) para el control de asistencia lo cual a simple vista no cuenta con algún respaldo de la autenticación de la información y del empleado que se presenta a elaborar.

HOJA DE CONTROL DE ASISTENCIA

FECHA	N. EMPLEADO	NOMBRE	HORA DE ENTRADA	FIRMA DE EMPLEADO	HORA DE SALIDA	FIRMA DE EMPLEADO

Figura 22. Formato de hoja de control de asistencia

En el caso para el control de acceso se utilizaba el formato (ver figura 23) en el cual se confirma que no cuenta con algún respaldo de la autenticación de la información y del empleado que está ingresando.



CONTROL DE ACCESO

FECHA	NOMBRE	PUESTO	MOTIVO	HORA DE ENTRADA	HORA DE SALIDA	FIRMA

Figura 23. Formato de control de acceso a ciertas áreas del inmueble.

En ambos caso necesitamos de la descripción del empleado que labora dentro de la empresa para poder tenerlo identificado en caso de alguna infracción realizada para esto se toman en cuenta los siguientes puntos

- Nombre completo
- Numero de Empleado
- Puesto que labora
- Sucursal
- Hora de jornada (entrada y salida)

Ya teniendo estos datos que son principales se puede identificar y buscar en la base de datos de la empresa para obtener sus datos personales del empleado.

5.5.3 Propuesta de interface

El sistema está contemplado para que sea manipulado por una persona el encargado de registro de altas, cambios, eliminación y creación de reportes de los empleados de la empresa pero también será para un súper administrador que será el que tenga el control de todo el sistema y pueda realizar consultas desde internet en una página web.

Control de Acceso

Primeramente se tendrá un control de acceso para el sistema con un Login. Donde este es proporcionado ya anteriormente con una precargar para asignar a los administradores (ver figura 24).

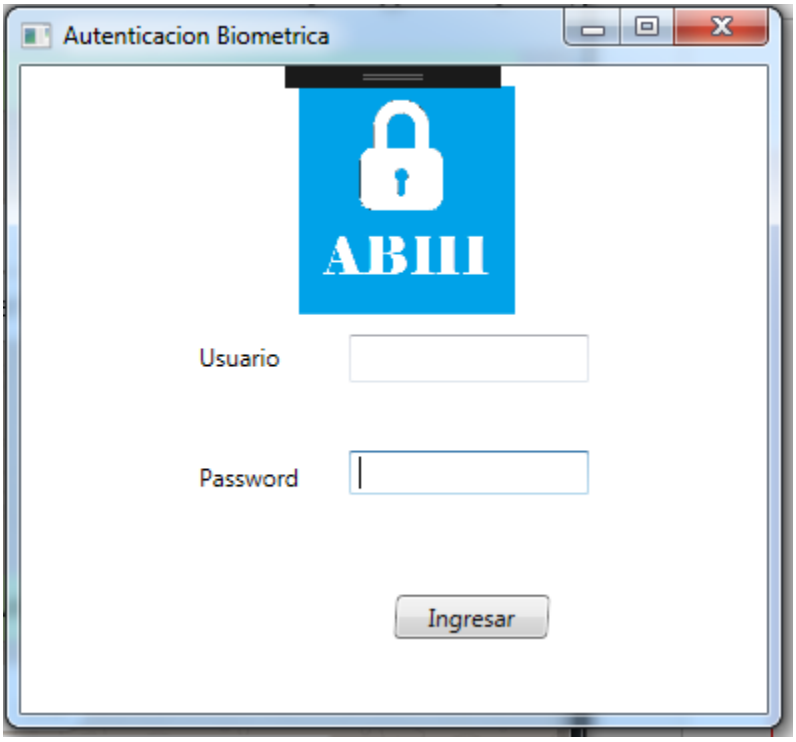


Figura 24. Login Aplicación de autenticacion biometrica

Menú Principal

El cual tendrá las opciones de dar de alta a un empleado así como su respectiva baja, modificación o Reportes de los empleados (ver figura 25).

Figura 25. Interfaz menú principal de ABHI

Registro de Empleado

Para el alta de empleado se maneja tres partes, la primera se pueden introducir los datos de cada individuo en la segunda parte ingresara los datos de la huella digital y por último los datos del Iris. Dentro de los datos generales se manejara el tipo de persona que se registra si es Administrador o Usuario y el tipo de Acceso que es el que va a definir el acceso a las áreas dentro de la empresa que se esta laborando (ver figura 26).

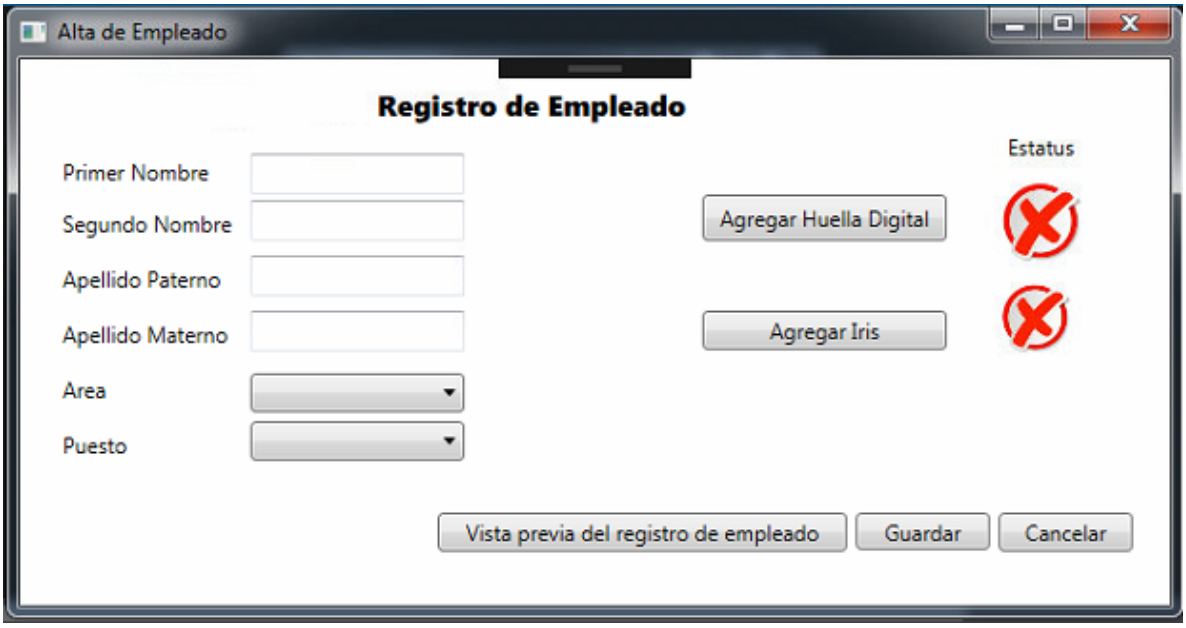


Figura 26. Interfaz Registro de empleado

Eliminar Empleado

El administrador tendrá la oportunidad de eliminar algún empleado que ya no este laborando dentro de las instalaciones correspondientes. Para esto tendrá la opción de buscar el empleado ya sea por su nombre, apellido paterno o su apellido materno incluso haciendo combinación de ello (ver figura 27).

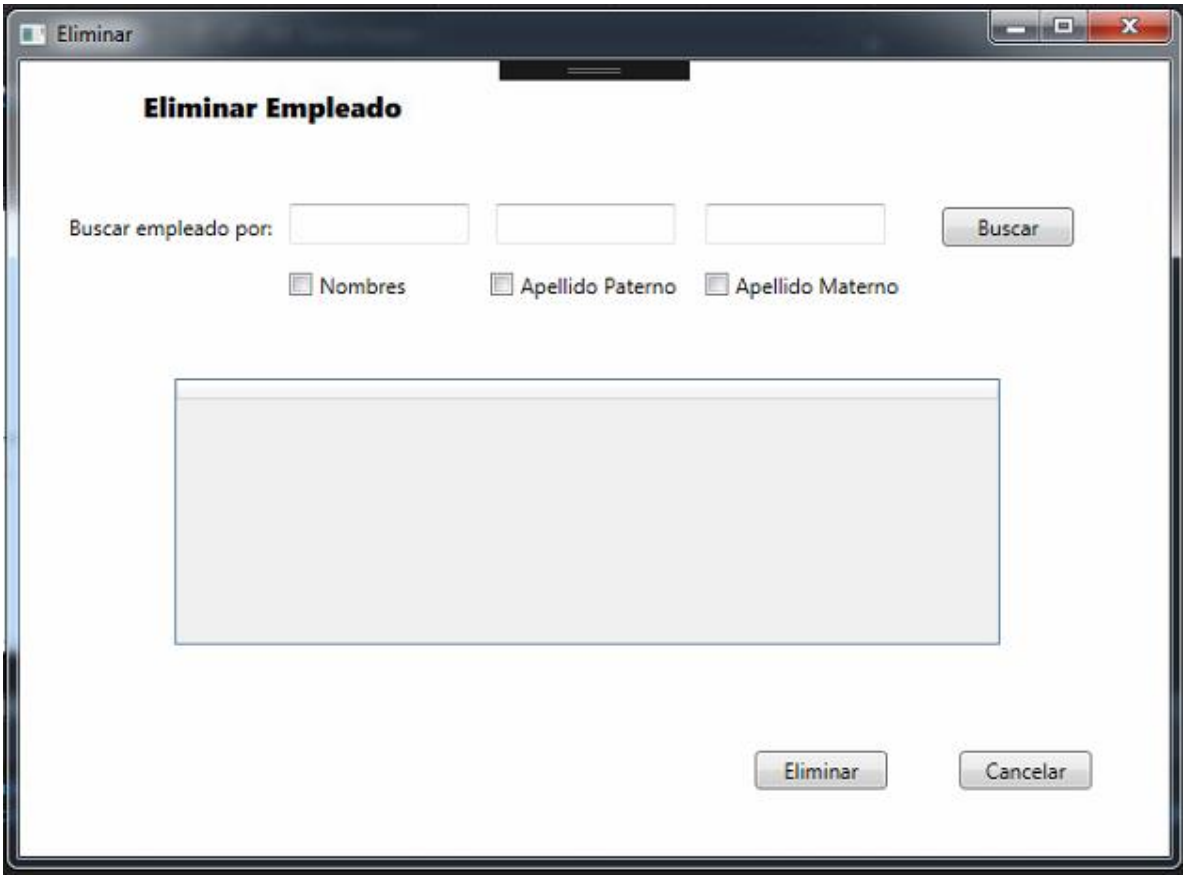


Figura 27. Interfaz Eliminar empleado

Modificación de Empleado

El administrador tendrá la opción de hacer modificaciones del empleado ya sea por algún dato personal o por su tipo de acceso que se le modifica o si tiene algún problema con la detección de alguna autenticación biométrica llámese Iris o huella digital (ver figura 28).

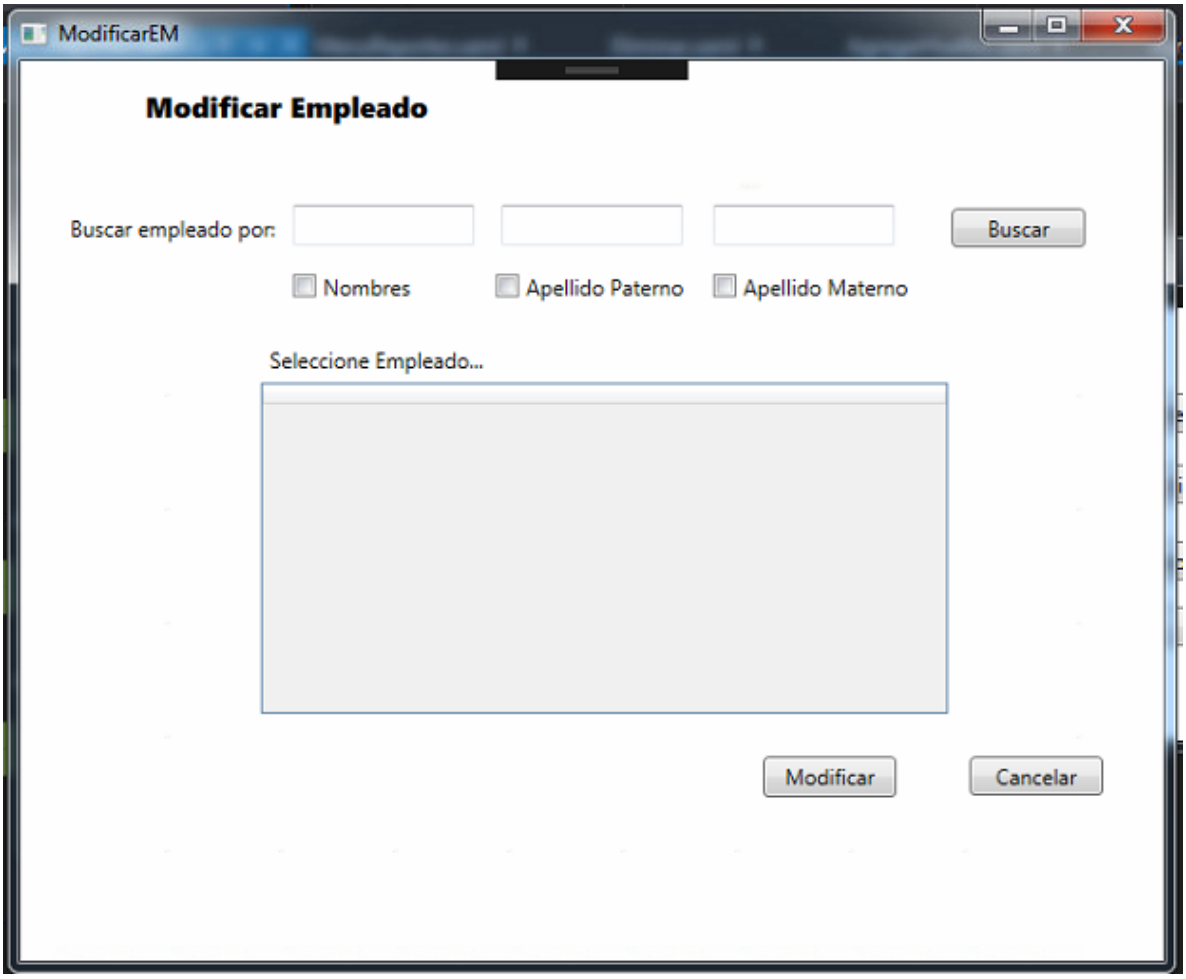


Figura 28. Interfaz de modificación de datos del empleado, haciendo primeramente la búsqueda

Reportes

Por último la interfaz de reportes donde el administrador podrá hacer diferentes tipos de reportes ya sea por empleado, área de acceso, fechas o por el puesto que esta laborando, además se realizara el reporte a través de un filtro de fechas para ser mas exactos en el reporte que se desea obtener. El administrador podrá decidir en

qué manera quiere realizar su reporte con estos filtros que se son los principales (ver figura 29).

Figura 29. Diseño de la interfaz de los filtros para la realización de Reportes.

5.5.4 Implementación

Control de seguridad

El sistema ABHI por sus siglas Autenticación Biométrica por Huella digital e Iris con sus respectivos mecanismos de seguridad mínimos (ver figura 30), donde mostrara un mensaje cuando inicie sesión con datos correctos (ver figura 32), también si se inicia sesión con datos erróneo se mostrara un mensaje donde indicara que ya sea el usuario o password no coinciden y regresando a la pantalla para que nuevamente se pueda iniciar sesión (ver figura 31).

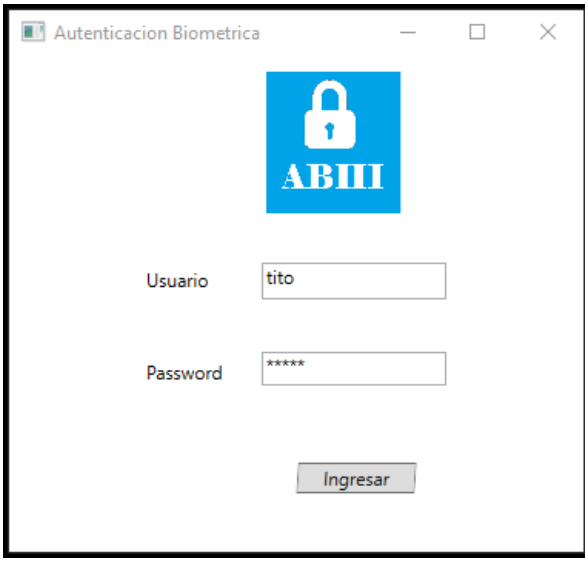


Figura 30. Login de sistema de ABHI

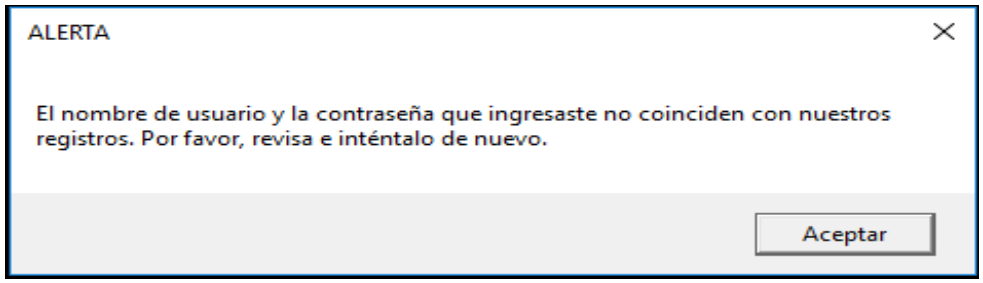


Figura 31. Interfaz de Inicio de sesión donde el Inicio de sesión es erróneo.

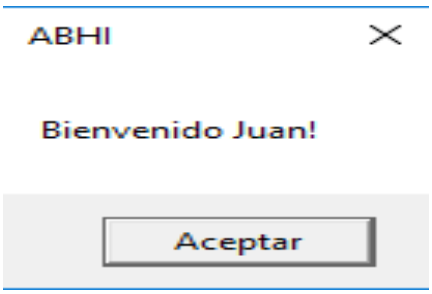


Figura 32. Interfaz de Inicio de sesión donde el Inicio de sesión es correcto.

Menú Principal

Una vez iniciado sesión correctamente con el Usuario y Password correctos el sistema mostrara su siguiente pantalla con el menú principal del sistema, donde se despliega un menú de posibles opciones donde el administrador tendrá opción de ir ya sea, registro empleado, eliminar empleado, modificar empleado y por ultimo Reportes (ver figura 33).

Figura 33. Interfaz del menú principal

Alta de Empleado

Para el alta de empleado se maneja tres partes, la primera se pueden introducir los datos de cada individuo en la segunda parte ingresara los datos de la huella digital y por último los datos del Iris. Dentro de los datos generales se manejara los datos

básico del empleado asi como seleccionar su área y puesto de la empresa. Para agregar la huella se da click en el botón Agregar Huella Digital (ver figura 34).

Figura 34. Dsieño de iniciar sesion de administaror

La segunda parte del alta del empleado se maneja el agregar la huella digital, este apartado maneja los datos de la huella digital que en compañía del lector de huellas se registrara en la base de datos las características de la huella digital del empleado. Para su registro tendrá la opción de seleccionar que dedo de la mano desea guardar como huella dactilar. Luego de seleccionar el dedo deberá colocar el dedo en el lector de huella una vez puesto el dedo seleccionado la pantalla muestra una imagen de una huella color rojo haciendo referencia que esta leyendo la huella (ver figura 35).

Figura 35. Captura de datos del empleado

Para su registro correcto de la huella digital el icono de la huella digital debe de cambiar de color de rojo a verde indicando que se guardo las caracteristicas de la huella digital correctamente y tambien el numero de veces que va a registra va cambiando (ver figura 36). En este caso se muestra el numero el de color verde y asi continuamente se quita el dedo del lector de huella digital hasta que nuevamente se muestre en rojo la imagen de la huella (ver figura 37).

Figura 36. Interfaz de huella guardado correctamente.

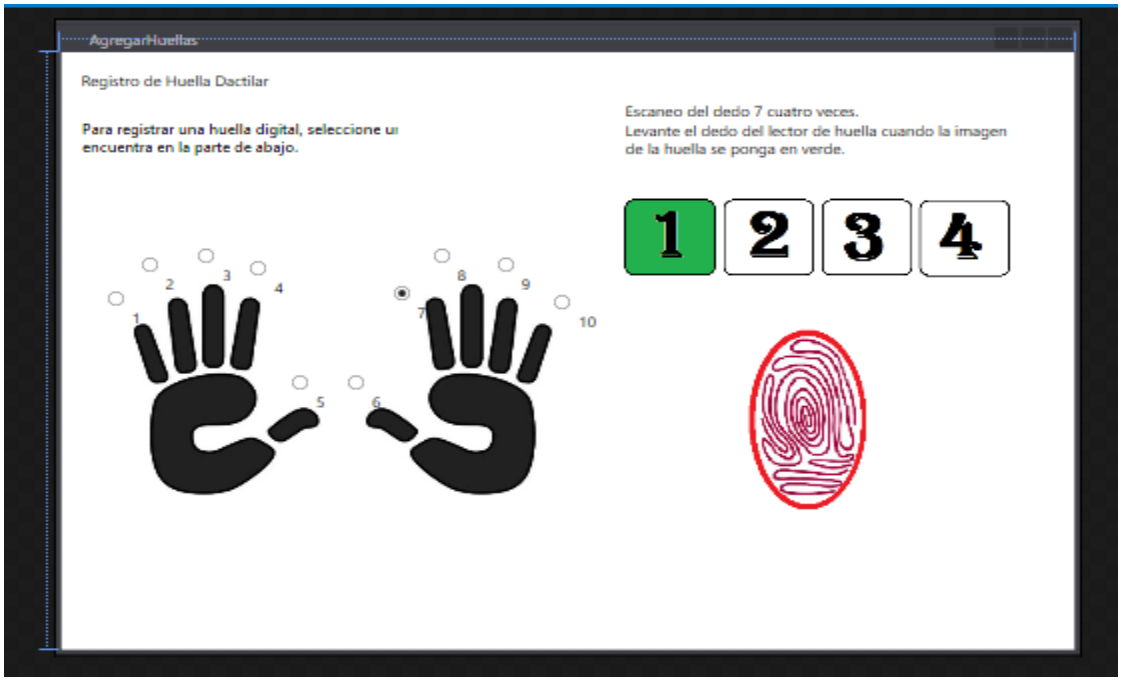


Figura 37. Interfaz de huella esperando la captura 2 de la huella.

Cuando se muestre la imagen de la huella en rojo vuelve a colocar el dedo en el lector de huella digital para hacer la captura número 2 de 4 (ver figura 38).

Figura 38. Interfaz de captura huella guardado correctamente número 2 de 4.

Figura 39. Interfaz de captura huella guardado correctamente número 3 de 4.

Nuevamente al realizar la operación por tercera vez y es correcto el numero 3 so colocara en verde y la huella de color verde indicando que fue correcto la captura de la huella dactilar (ver figura 39). Por último se debe mostrar los cuatro numero de color en verde y la imagen de la huella digital en verde el cual nos confirma que se obtuvieron correctamente las cuatro capturas de la huella (ver figura 40).

Figura 40. Interfaz donde se registró correctamente las 4 veces la huella digital.

La última parte del registro de empleado es el escaneo de iris. No se necesita mucho tiempo para el registro del Irisa a comparación de la huella digital y en este solo se toma una captura de Iris, al darle click en Guardar para registrar las capturas de la huella digital se mostrar un mensaje verificando que se guardó correctamente la huella (ver figura 41).

Figura 41. Mensaje verificando que se guardó correctamente la huella

Se regresara la pantalla al registro de empleado con los datos que anteriormente se habían registrado y ahora en el estatus de huella digital con una paloma, para informar que la huella digital fue guardada exitosamente (ver figura 42).

Figura 42. Interfaz de registro de empleado con la huella digital guardada.

Ahora en la tercera parte se debe agregar el iris de la persona para eso se da click en el botón Agregar Iris, donde mostrara la pantalla donde se indican las instrucciones que son sencillas, el empleado debe colocar la cara a la altura del lector de iris y colocar los ojos como muestra el ejemplo dentro de la cámara. Al no guardar nada el estatus aparecerá una imagen con un tache. Al agregar las características del iris correctamente cambiara el estatus con una paloma y al darle click en guardar también mostrara un mensaje corroborando que se guardó correctamente el Iris del empleado.

Nuevamente se regresara la apantalla de registro de empleado, ahora con el cambio de paloma en Iris que fue lo nuevo que se agregó, los datos que se registraron primeramente se siguen conservando y los estatus tanto como huella digital e Iris están en aprobadas o palomas. Se puede dar click en Vista previa del

registro del empleado para verificar los datos del empleado a registrar (ver figura 43).

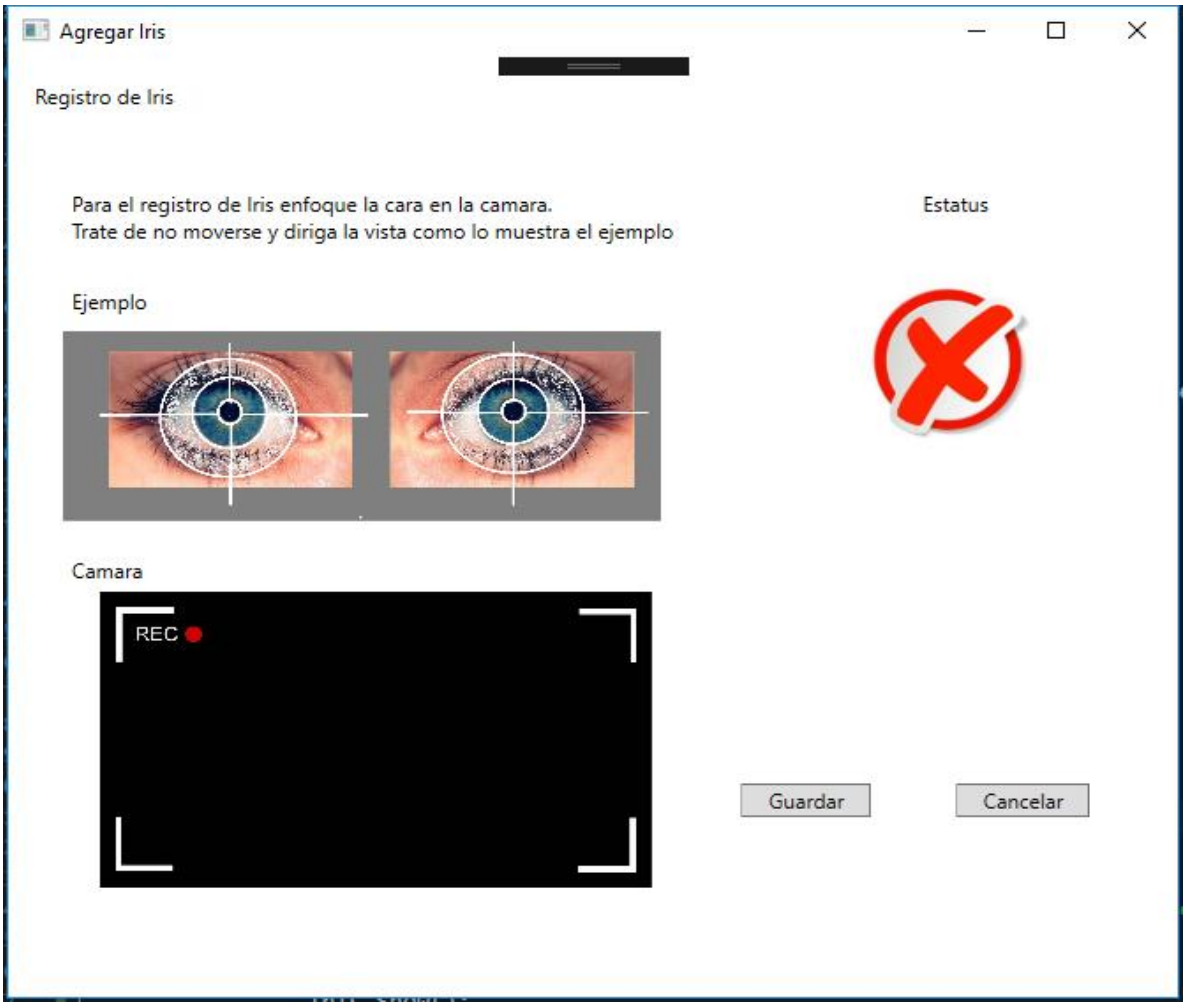


Figura 43. Interfaz de registro de Iris del empleado.

Figura 44. Mensaje que corrobora que se guardó exitosamente el Iris

Si la captura del iris fue correcta se mostrar un mensaje indicando que el iris fue guardado correctamente de lo contrario no se mostrar ningún mensaje indicando que se tiene que volver a realizar el proceso de captura (ver figura 44).

Nuevamente, regresa la pantalla de registro de empleado ahora con los dos estatus de Huella digital e Iris con aprobado o paloma y los datos que primeramente se registraron (ver figura 45), en este paso se tiene la opción de la vista previa del registro de empleado donde nos resumen los datos que se agregaron los datos del empleado (ver figura 46).

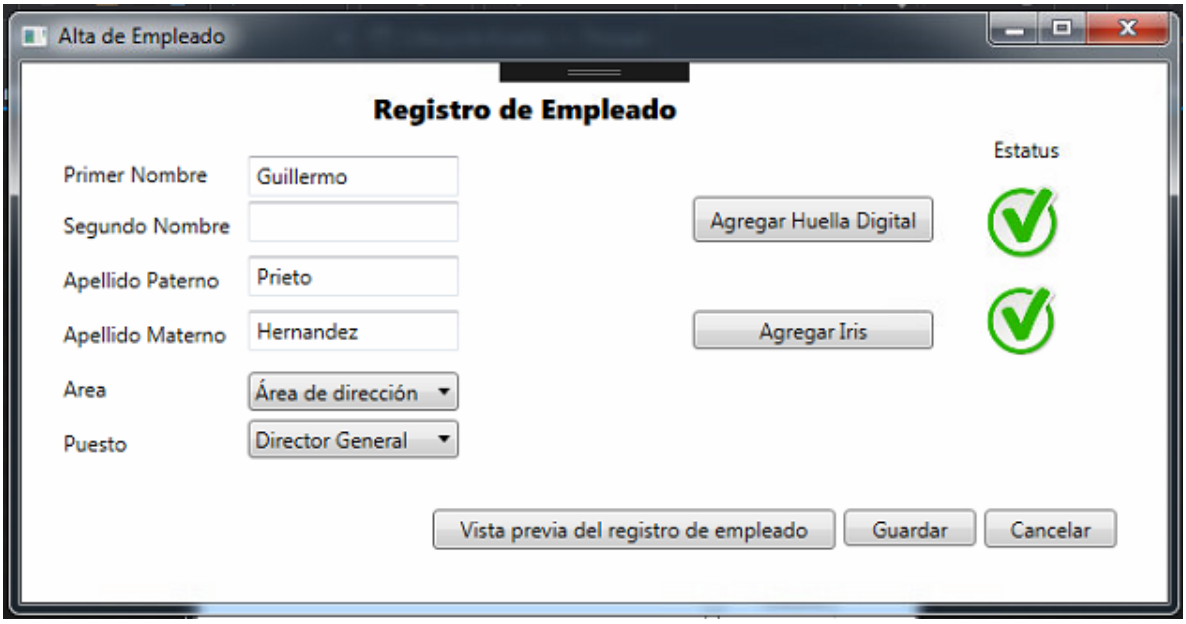


Figura 45. Interfaz de registro empleado ya con todos los campos solicitados.

Figura 46. Interfaz de vista previa cuando no se ha agregado nada en el registro el empleado.

En el caso que se registre todos los datos la interfaz de vista previa estar toda llena con los datos del empleado que se está registrando (ver figura 47). En el caso que llegara a faltar algún registro de se verá en estatus general en tache con esto nos damos cuenta que falta de registrar algún campo (en el caso de segundo nombre puede estar sin dato).

Figura 47. Interfaz de la vista previa de registro de usuario cuando está listo para ser guardado el registro del empleado

Eliminar Empleado

Para la interfaz Eliminar empleado se puede hacer un filtro de búsqueda ya sea con nombre, apellido paterno, apellido materno, o combinación de estos 3 filtros si se tiene el nombre completo del empleado (ver figura 49). Al hacerle click en buscar en el caso de que no se ingrese ningún campo para el filtrado se va a mostrar todos los campos existentes en la base de datos. Para eliminarlo solo se selecciona el empleado colocando el puntero en la fila del empleado a eliminar y se da click en el botón eliminar (ver figura 48). Se mostrara un mensaje confirmando si se desea eliminar el registro con el nombre del empleado.

Figura 48. Interfaz de eliminar empleado.

Figura 49. Interfaz de eliminar empleado con el filtro de Nombre.

También se puede realizar el filtrado por el apellido paterno (ver figura 50) para eliminar al empleado si solo al principio solo se conoce el apellido patero, en el caso que conozca el apellido materno también se puede realizar el filtrado (ver figura 51).

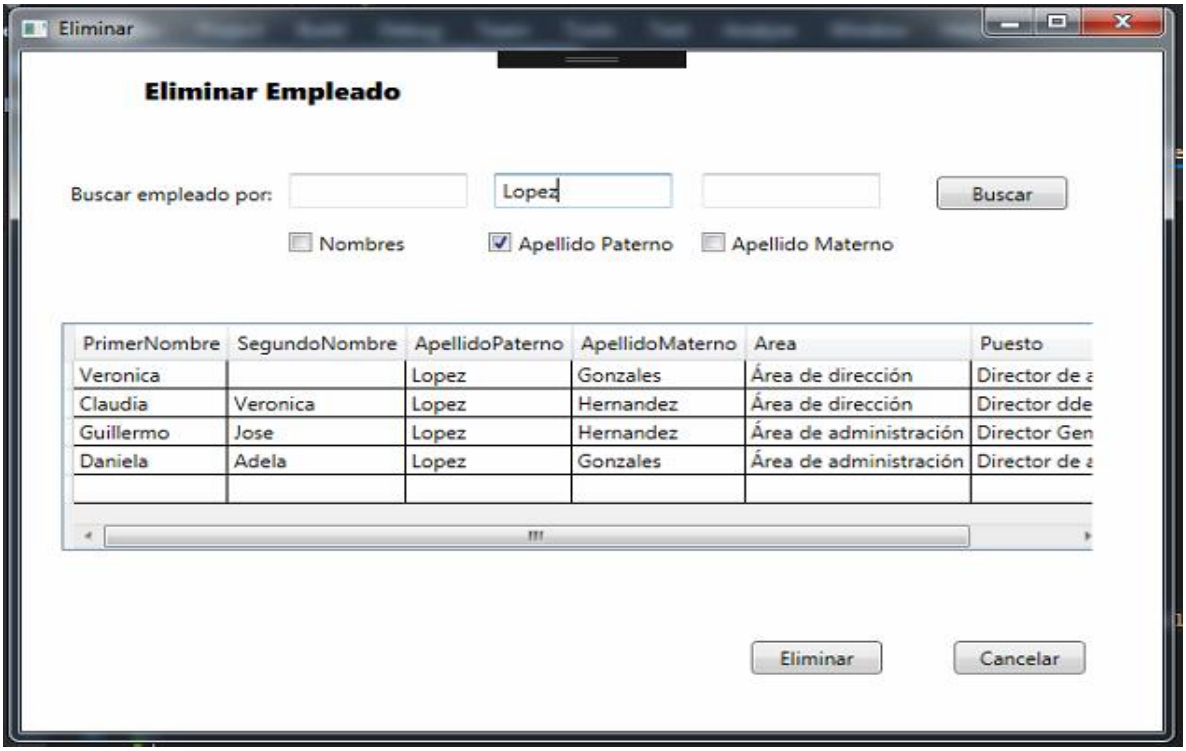


Figura 50. Interfaz de eliminar empleado con el filtro de apellido paterno.

Figura 51. Interfaz de eliminar empleado con el filtro de apellido materno.

Existe el caso que se puede hacer combinación de filtrado para tener más preciso el nombre completo del empleado que se desea eliminar (ver figura 52). Después de conocer el empleado a eliminar se selecciona en cualquiera de sus campos se pondrá toda la fila del empleado color azul indicando que es el empleado que se desea eliminar (ver figura 53). Al darle click en eliminar saldrá un mensaje indicando si estamos de acuerdo eliminar al empleado con el nombre del empleado tenemos tres opciones, el SI eliminara el empleado, el NO y cancelar interrumpe la eliminación del empleado (ver figura 54).

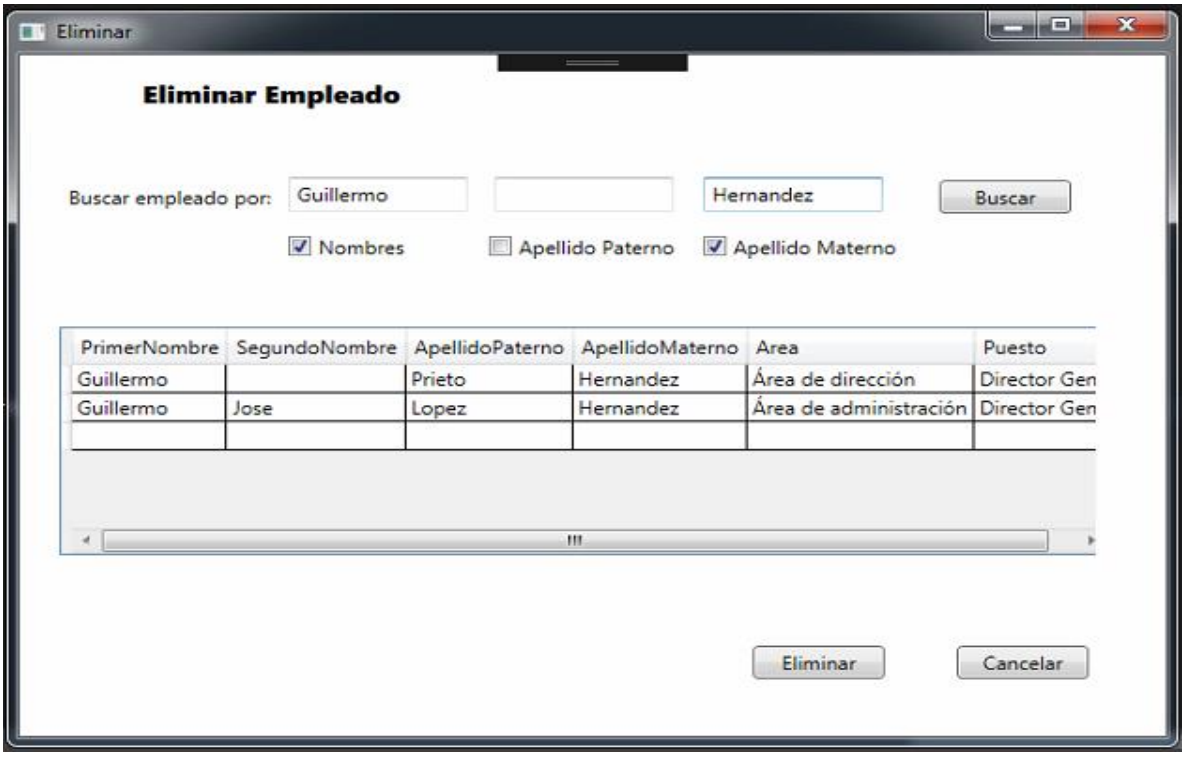


Figura 52. Interfaz de eliminar empleado con la combinación de dos filtros de nombre y apellido materno.

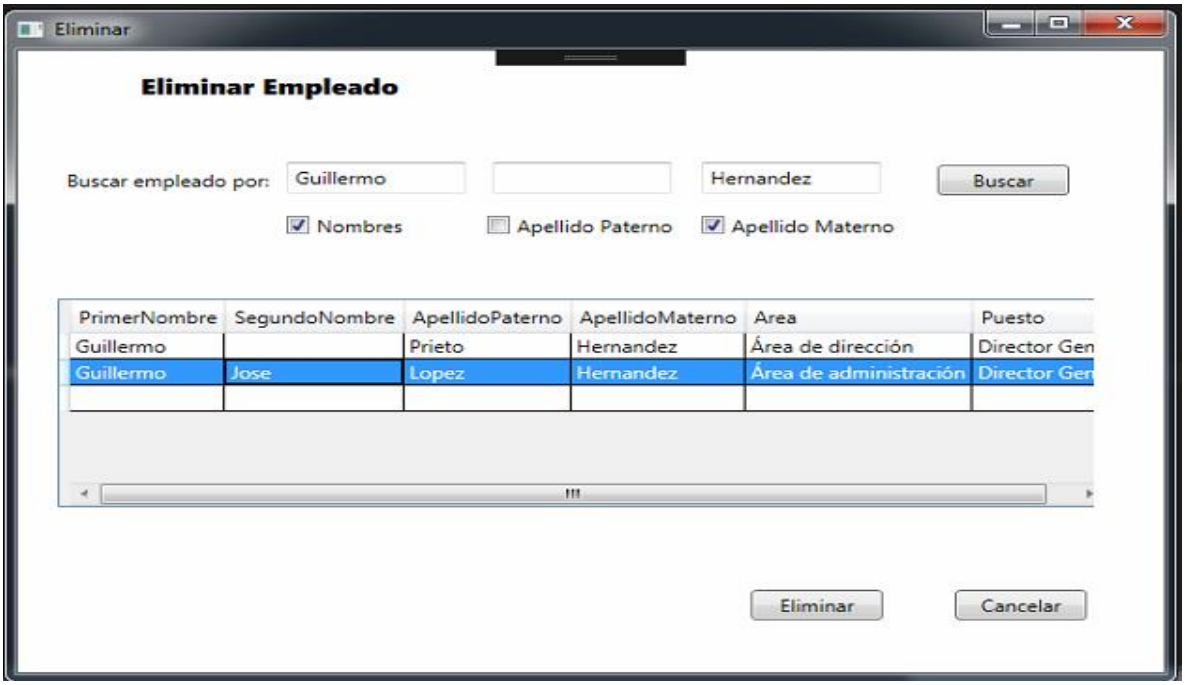


Figura 53. Interfaz selección de empleado para eliminar.

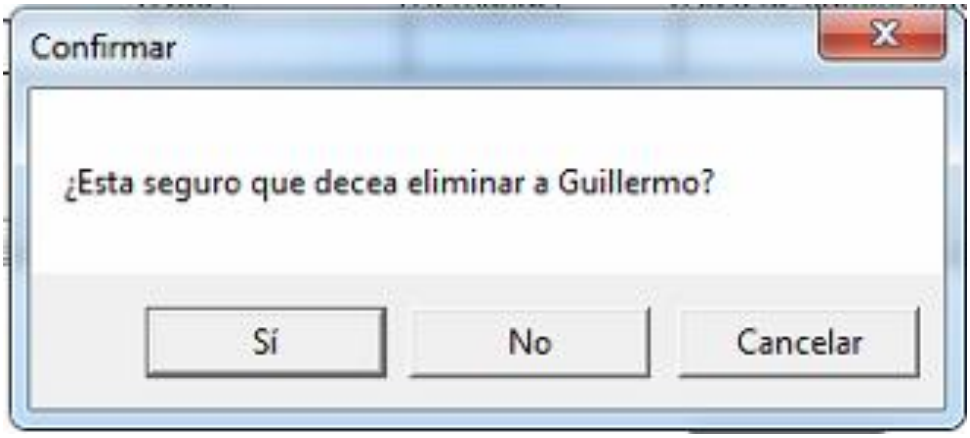


Figura 54. Mensaje de confirmación para eliminar empleado Guillermo.

Modificar empleado

Dentro de la aplicación ABHI se tiene la opción de modificar el empleado por cierta razón no se guardó correctamente o se cambió de puesto se puede hacer su respectiva modificación, para esto se necesita hacer la búsqueda del empleado a modificar (ver figura 55). Se puede realizar con su respectivos filtros ya sea nombre (ver figura 56), por apellido paterno (ver figura 57), o ya sea por si apellido materno (ver figura 58), o combinación de estos (ver figura 59). Los filtros se utilizan puesto hay veces el administrador puede que no le proporcionaron el dato completo sobre su nombre a modificar por eso se utilizan los filtros ya que también puede haber un número indefinido de empelados registrados en la empresa llámese empresa grande.

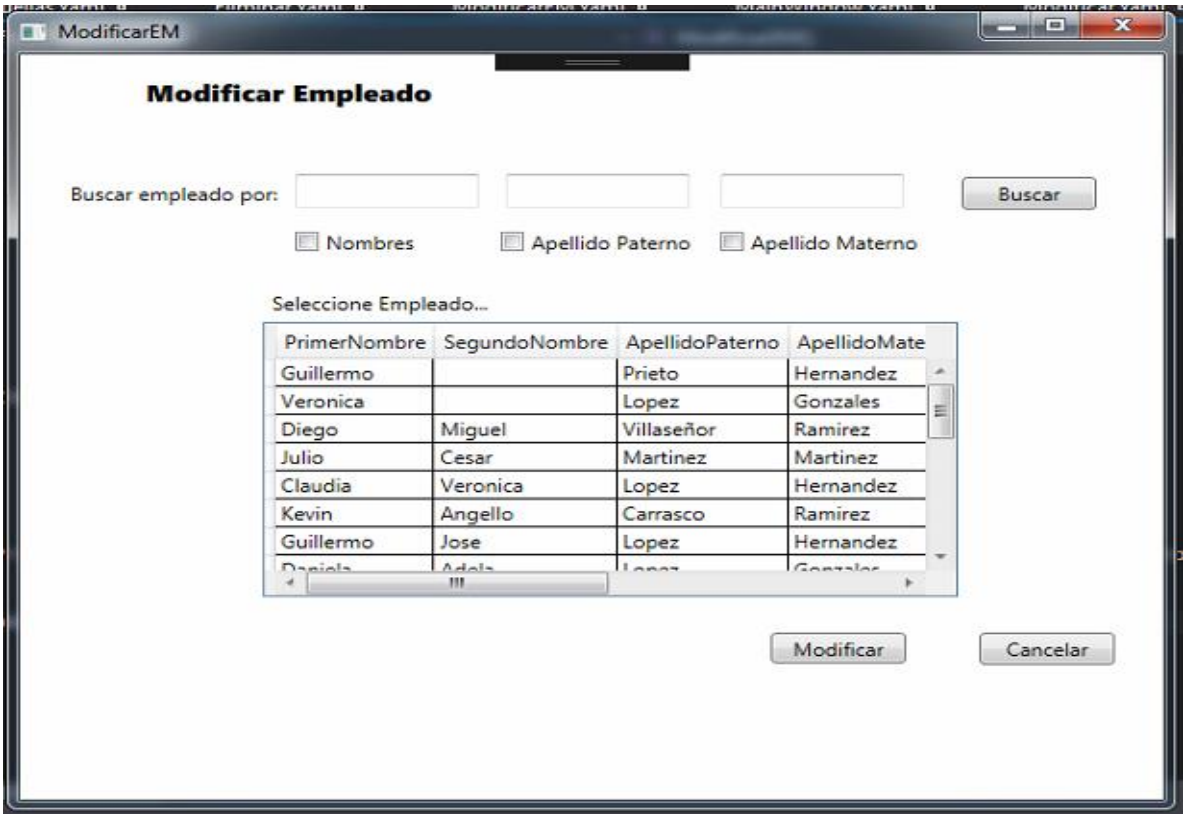


Figura 55. Interfaz de modificación de empleado.

Figura 56. Interfaz de modificación de empleado con el filtro nombres.

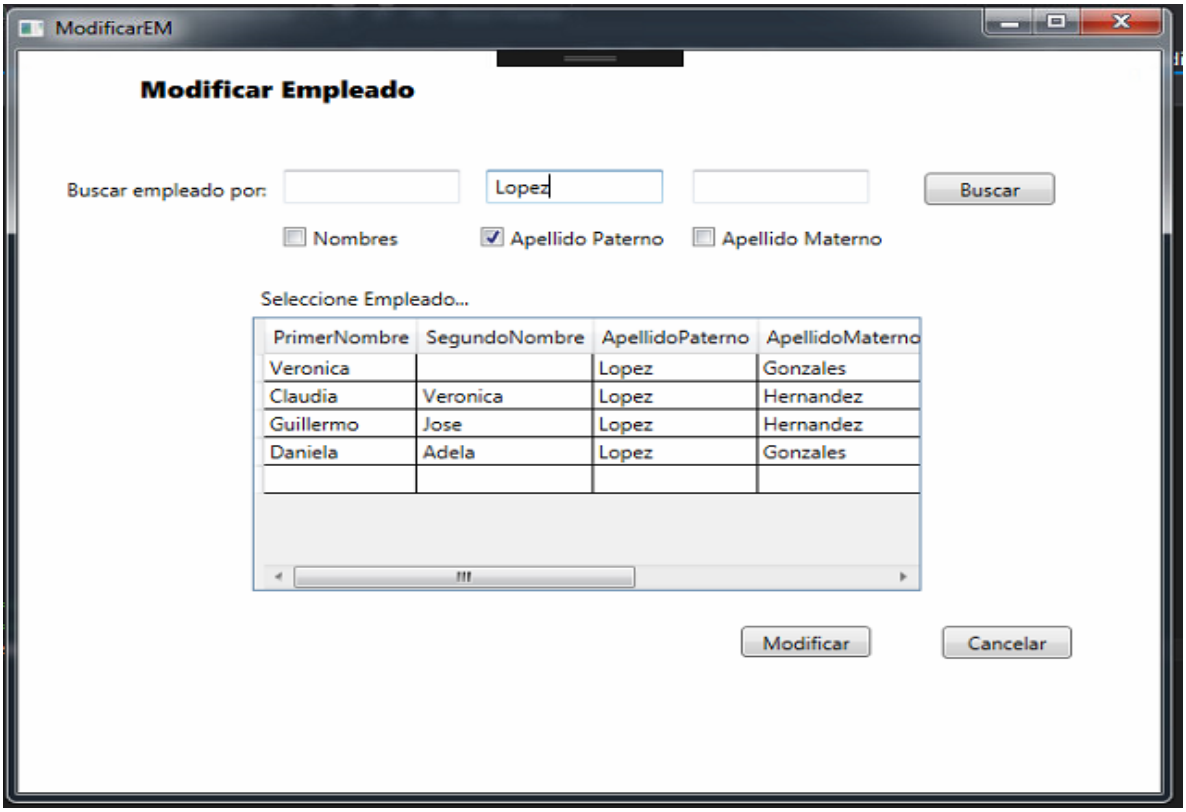


Figura 57. Interfaz de modificación de empleado con el filtro apellido paterno.

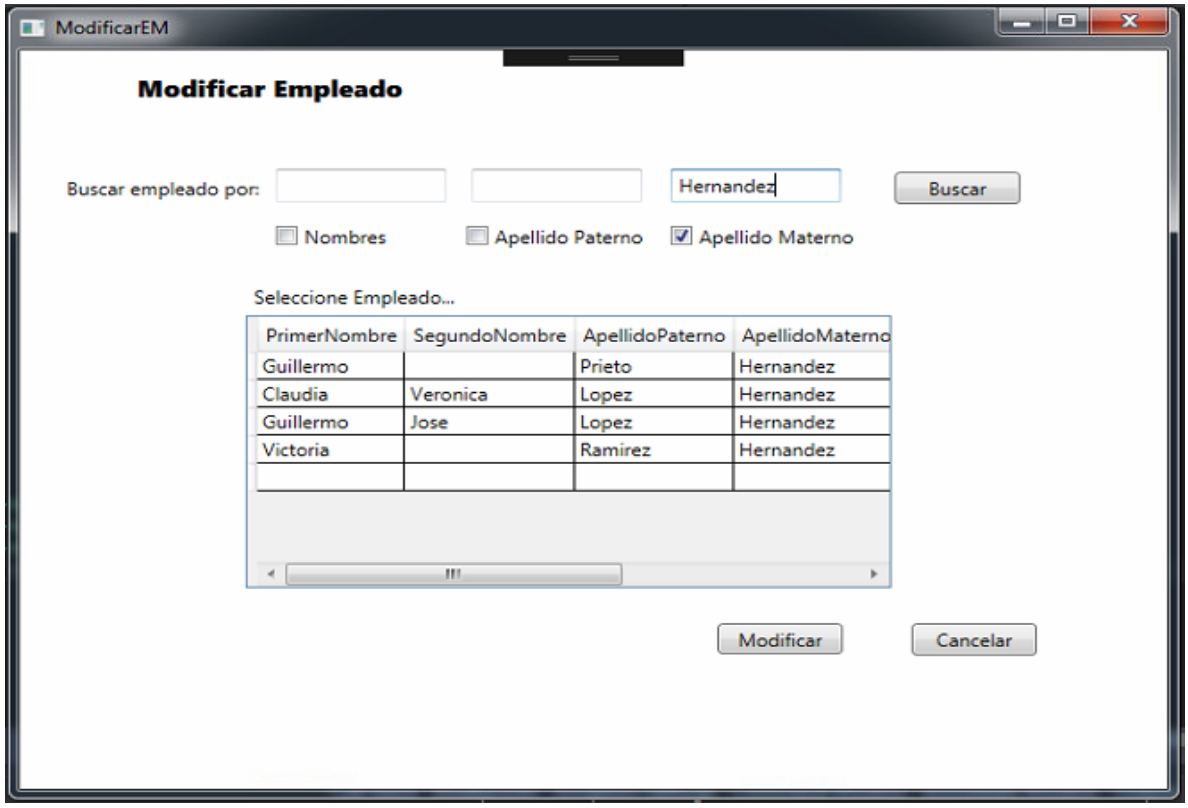


Figura 58. Interfaz de modificación de empleado con el filtro apellido materno.

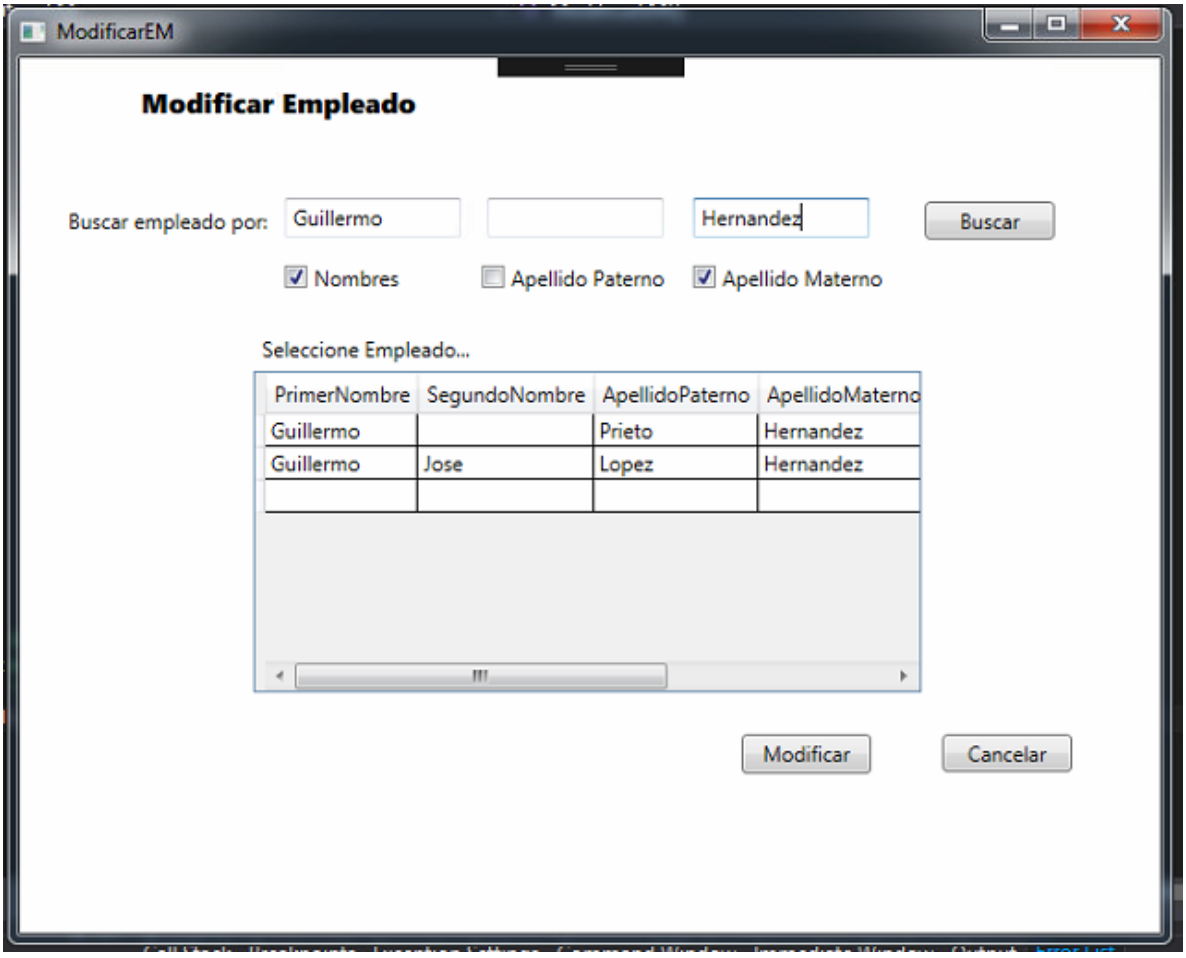


Figura 59. Interfaz de modificación de empleado con combinación de filtros nombre y apellido materno.

Al seleccionar el empleado a modificar se mostrará otra pantalla con los datos del empleado guardados en la base de datos. Para modificar solo se tiene que cambiar en el campo que se desea modificar, todos los campos del empleado están sujetos a cambio incluso con la huella dactilar o el iris. El único campo que puede estar vacío es solo segundo nombre. Para guardar las modificaciones se da un click en el botón modificar, se muestra un mensaje de confirmación para guardar los cambión si selecciona si se guardara la modificación del empelado en el caso de no, o cancelar se sigue conservando los datos del empleado (ver figura 60).

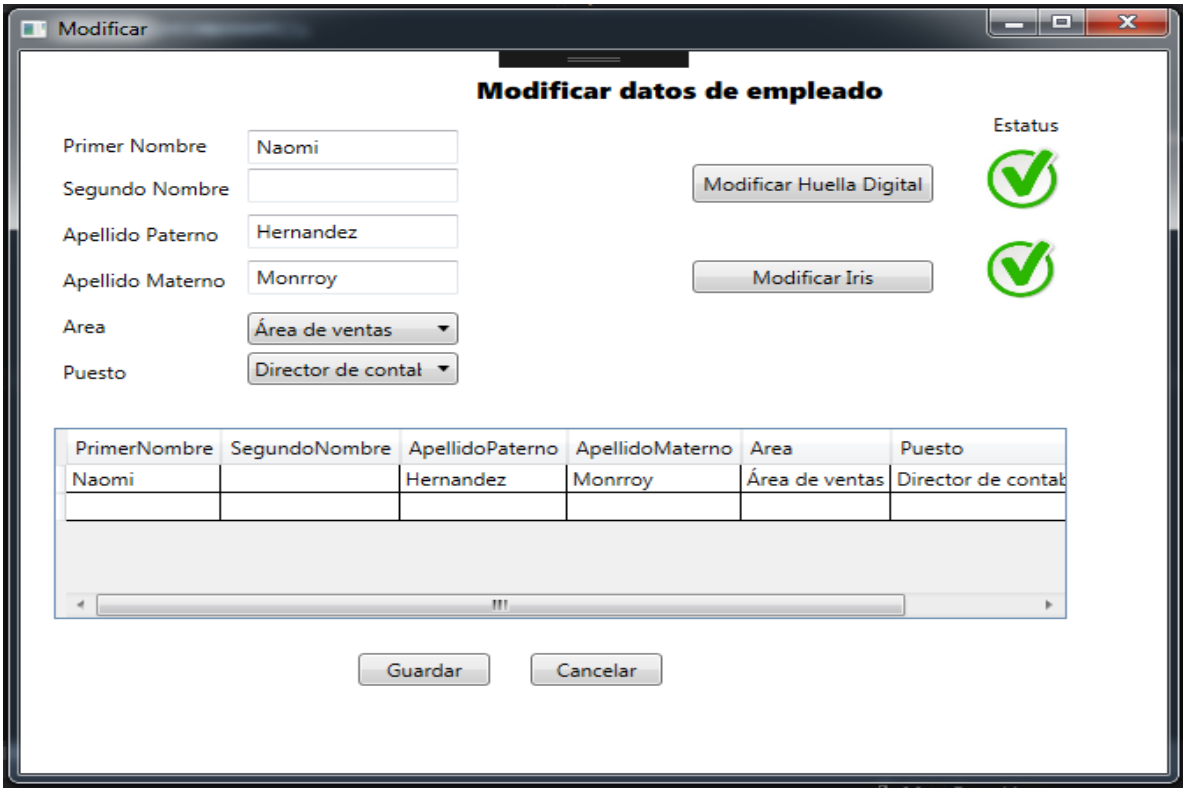


Figura 60. Interfaz de modificación de empleado con sus datos actuales.

En este caso se modificara el empleado Naomi se agregara su segundo nombre ya que por alguna situación no se agregó y modificara el puesto ya que por ejemplo subió de puesto (ver figura 61). Al modificar los campos y seleccionar el botón guardar nos indicara en un mensaje si estamos seguros de modificar el empleado en este caso Naomi (ver figura 62), tenemos tres opciones el SI guardara todos los cambios el no o cancelar no guardar los cambios que se realizaron al empleado (ver figura 63).

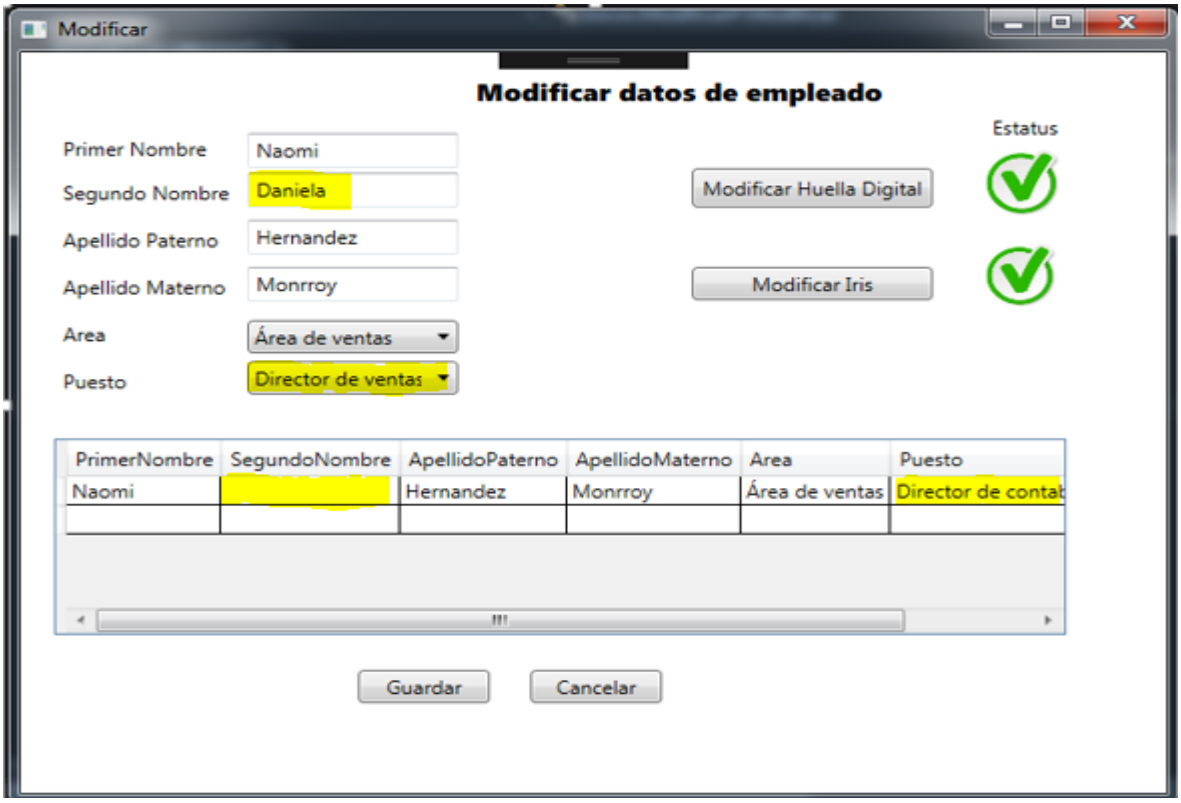


Figura 61. Interfaz de modificación de empleado haciendo las modificaciones.

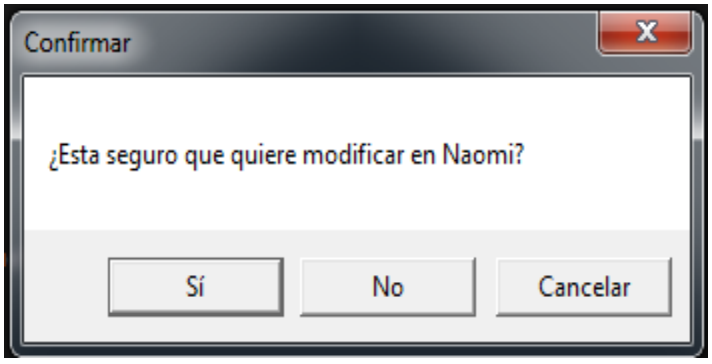


Figura 62. Mensaje de confirmación al modificar el empleado Naomi.

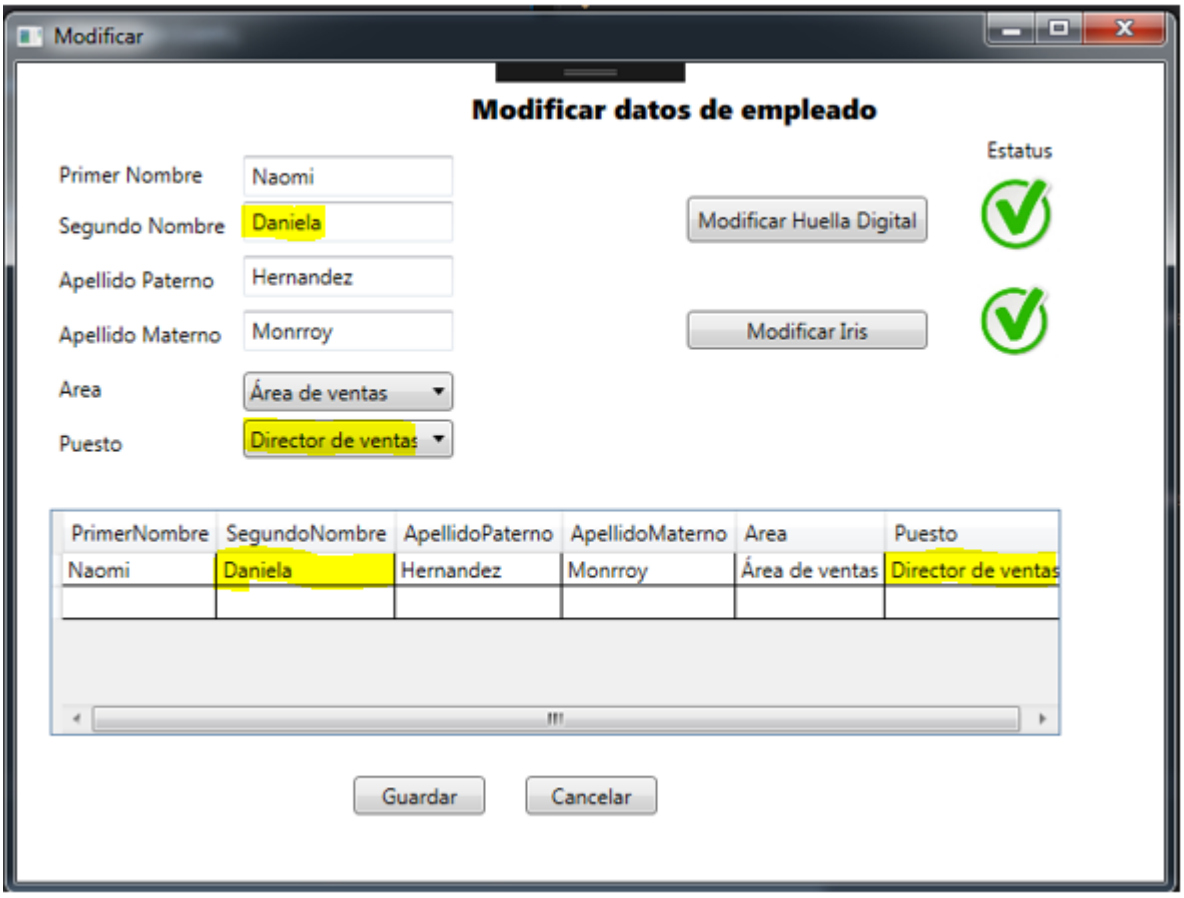


Figura 63. Interfaz de modificación de empleado ya con las nuevas modificaciones.

Reportes

El administrador dentro del menú principal tendrá la opción de realizar reportes estos pueden ser con varios filtros por persona, área, puesto y fecha, estos tres primeros se hace también el filtro por fecha para traer datos mas específicos. Los reportes generados se crean en formato Excel (ver figura 64).

Figura 64. Interfaz de menú para reportes.

Seleccionando generar reporte por persona se necesita hacer la búsqueda de la persona teniendo la opción de tres filtros nombres, apellido paterno y por ultimo apellido materno. Los filtros se utilizan puesto hay veces el administrador puede que no le proporcionaron el dato completo sobre su nombre a modificar por eso se utilizan los filtros ya que también puede haber un número indefinido de empelados registrados en la empresa llámese empresa grande (ver figura 65).

Al seleccionar algún filtro o varios filtros se da click en el botón buscar para que muestre los empleados que cumplen con esta características, dentro de la caja la tabla que aparecerán los empleados se debe seleccionar el empleado o los empleados para generar el reporte. Se debe seleccionar también la fecha inicial y fecha final y en ese momento se puede generar o para ser más específico se puede utilizar el filtro de fecha inicio y fecha fin (ver figura 66).

Figura 65. Interfaz de reportes por persona.

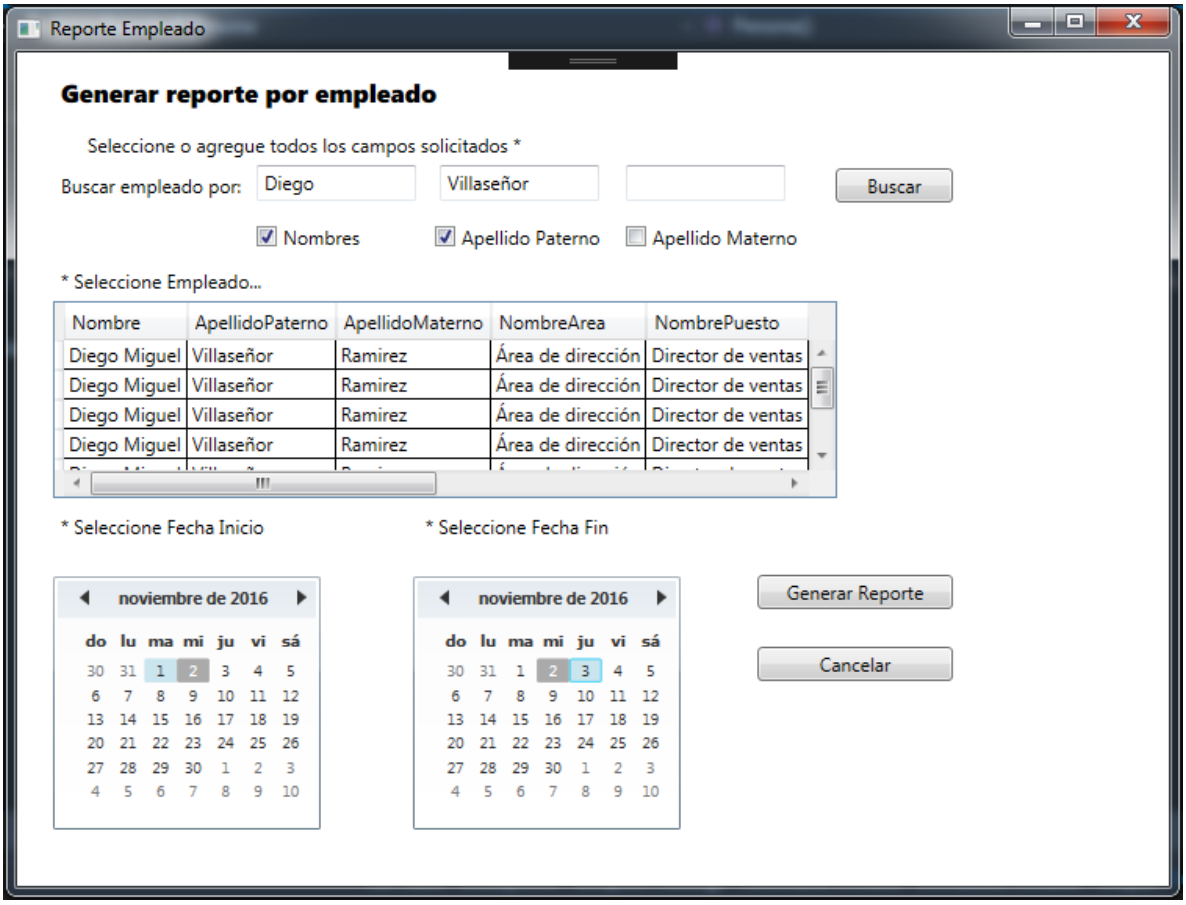


Figura 66. Interfaz de reportes por persona con el empleado Diego Villaseñor.

Una vez dado click al botón Generar Reporte se crea un archivo Excel con el nombre del empelado con las fecha inicio y fecha final que se desea general (ver figura 67).

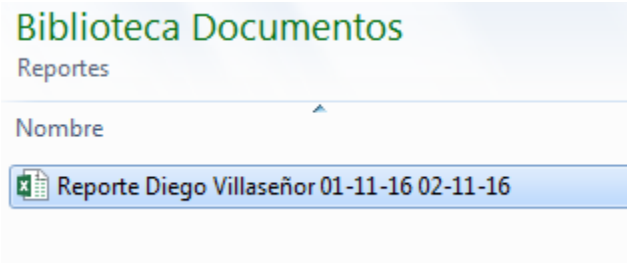
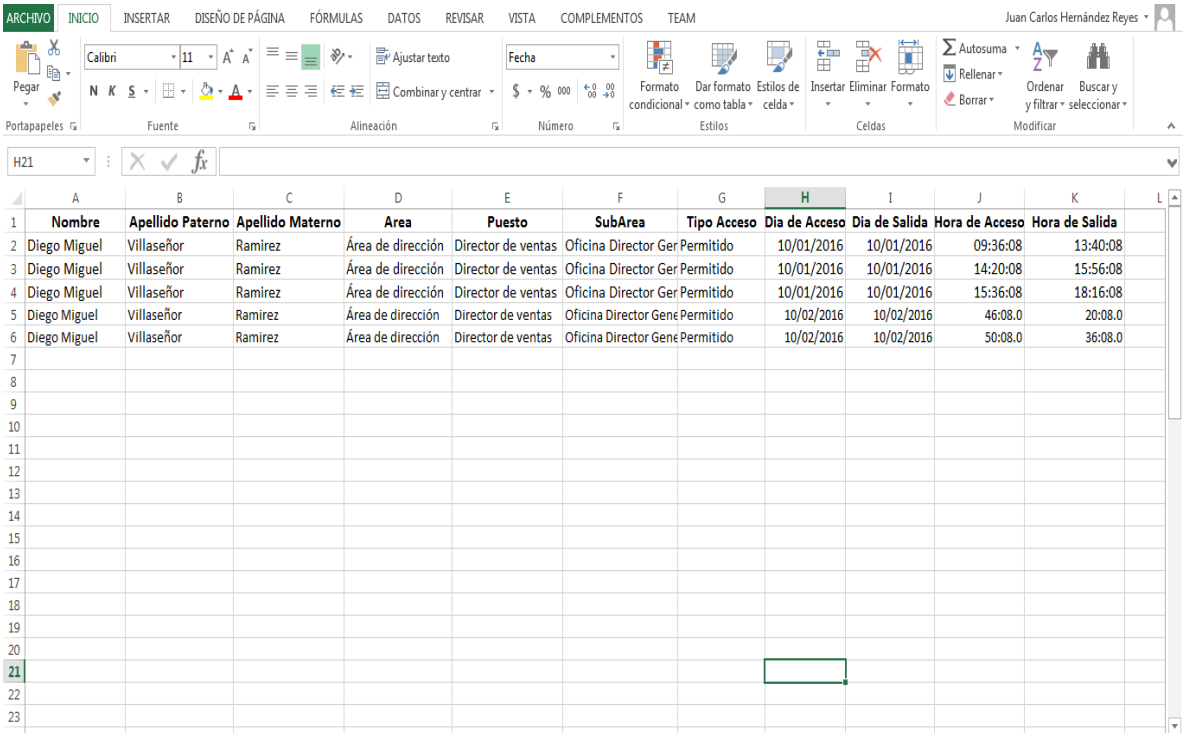


Figura 67. Creación de Excel con nombre y fecha incio fecha final del empleado.

Al abrir el reporte de Excel se muestra la consulta del empleado Diego Villaseñor entre las fechas 01-11-2016 y 02-11-2016 (ver figura 68).



	A	B	C	D	E	F	G	H	I	J	K
1	Nombre	Apellido Paterno	Apellido Materno	Area	Puesto	SubArea	Tipo Acceso	Dia de Acceso	Dia de Salida	Hora de Acceso	Hora de Salida
2	Diego Miguel	Villaseñor	Ramirez	Área de dirección	Director de ventas	Oficina Director Ger	Permitido	10/01/2016	10/01/2016	09:36:08	13:40:08
3	Diego Miguel	Villaseñor	Ramirez	Área de dirección	Director de ventas	Oficina Director Ger	Permitido	10/01/2016	10/01/2016	14:20:08	15:56:08
4	Diego Miguel	Villaseñor	Ramirez	Área de dirección	Director de ventas	Oficina Director Ger	Permitido	10/01/2016	10/01/2016	15:36:08	18:16:08
5	Diego Miguel	Villaseñor	Ramirez	Área de dirección	Director de ventas	Oficina Director Gene	Permitido	10/02/2016	10/02/2016	46:08.0	20:08.0
6	Diego Miguel	Villaseñor	Ramirez	Área de dirección	Director de ventas	Oficina Director Gene	Permitido	10/02/2016	10/02/2016	50:08.0	36:08.0

Figura 68. Reporte del Excel del empleado.

Dentro del menú de reportes también está la opción de obtener reportes por área y por ser más preciso las sub-áreas que se manejan dentro de la empresa. En este caso se manejan cinco áreas y entre ellas se encuentran cinco sub-áreas, recordando que entre estas áreas se encontrar el dispositivo para autenticarse en la entrada de la sub-área de la empresa (ver figura 69). Con su respectivo filtro de fechas para ser más preciso entre los datos que se quiere traer en los reportes puestos sino se selecciona ninguna fecha el sistema manada un mensaje indicando que falta seleccionar fechas (ver figura 71). Al seleccionar el botón generar se genera el archivo en formato Excel con el nombre del área sub área y las fechas seleccionadas o por default (ver figura 70). Al abrirlo se muestra los movimientos que se realizaron en esa fecha y áreas correspondientes (ver figura 72).

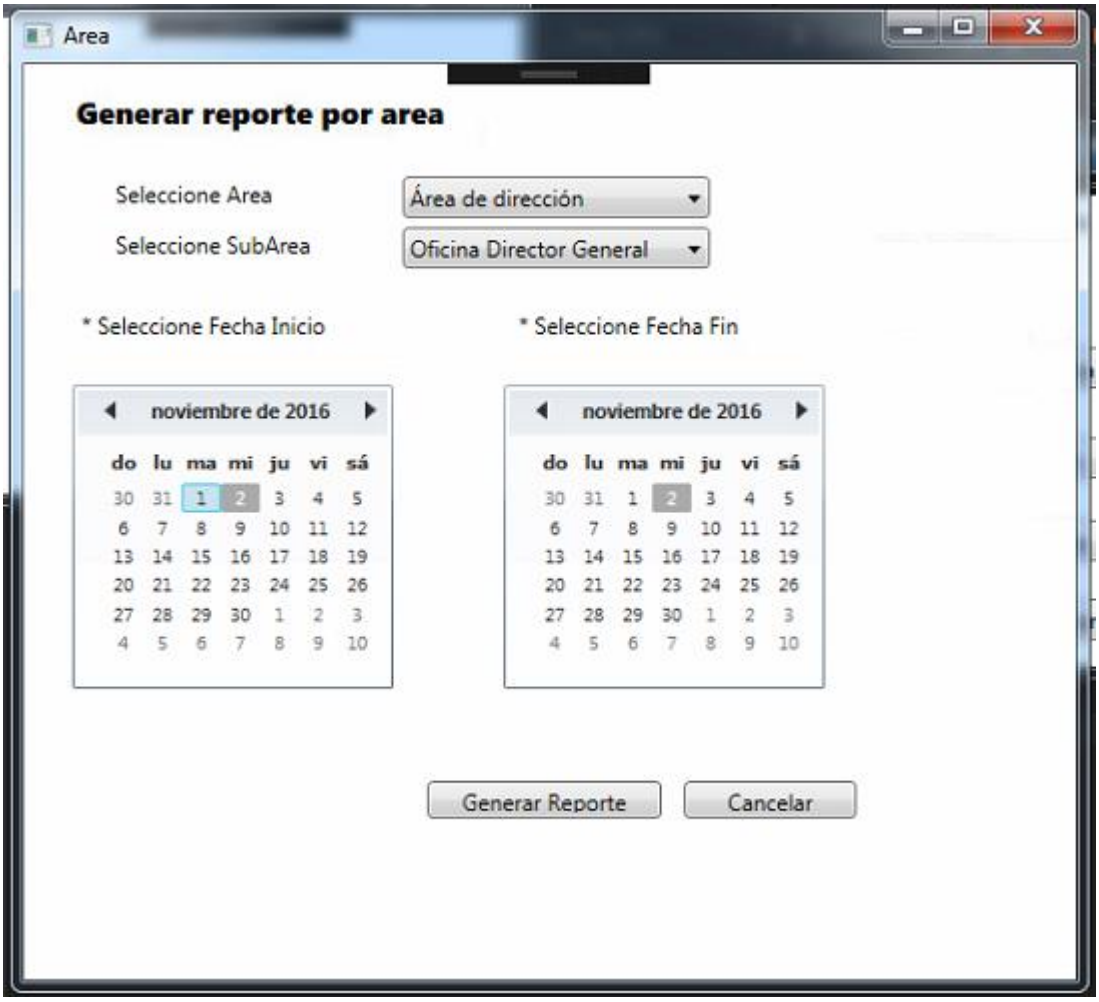


Figura 69. Interfaz de reportes por persona.

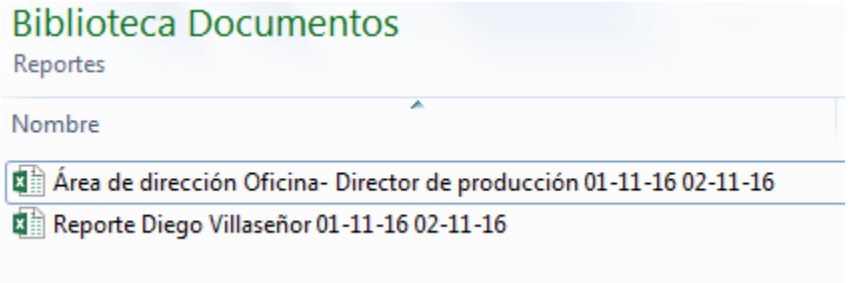


Figura 70. Interfaz de reportes por persona.

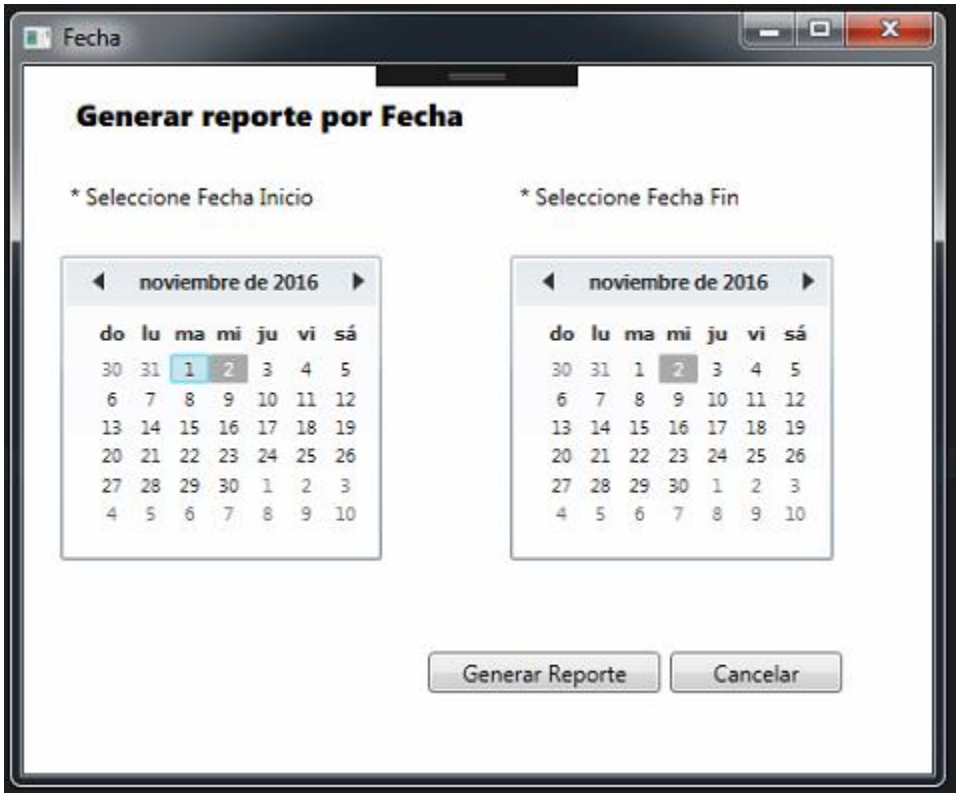
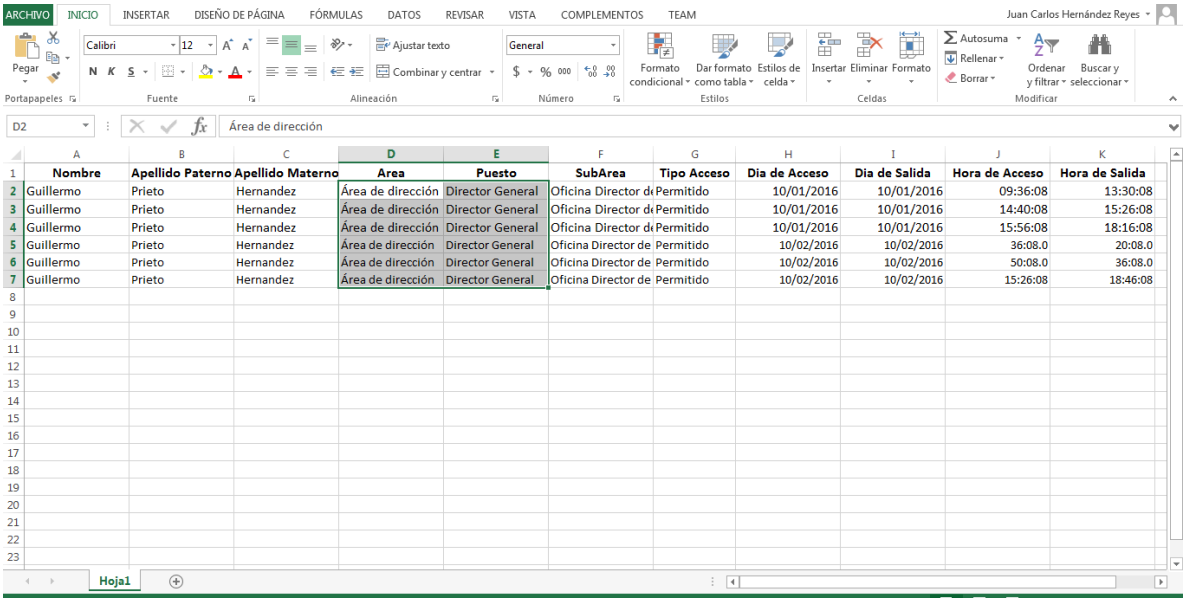
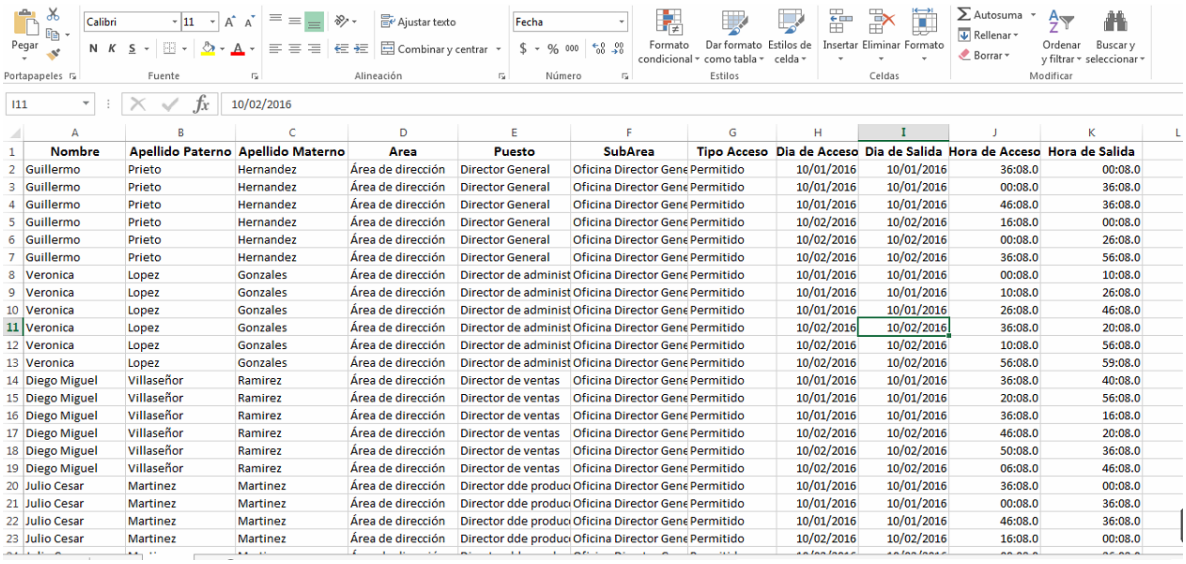


Figura 71. Interfaz de reportes por persona.



	A	B	C	D	E	F	G	H	I	J	K
1	Nombre	Apellido Paterno	Apellido Materno	Area	Puesto	SubArea	Tipo Acceso	Dia de Acceso	Dia de Salida	Hora de Acceso	Hora de Salida
2	Guillermo	Prieto	Hernandez	Área de dirección	Director General	Oficina Director de	Permitido	10/01/2016	10/01/2016	09:36:08	13:30:08
3	Guillermo	Prieto	Hernandez	Área de dirección	Director General	Oficina Director de	Permitido	10/01/2016	10/01/2016	14:40:08	15:26:08
4	Guillermo	Prieto	Hernandez	Área de dirección	Director General	Oficina Director de	Permitido	10/01/2016	10/01/2016	15:56:08	18:16:08
5	Guillermo	Prieto	Hernandez	Área de dirección	Director General	Oficina Director de	Permitido	10/02/2016	10/02/2016	36:08.0	20:08.0
6	Guillermo	Prieto	Hernandez	Área de dirección	Director General	Oficina Director de	Permitido	10/02/2016	10/02/2016	50:08.0	36:08.0
7	Guillermo	Prieto	Hernandez	Área de dirección	Director General	Oficina Director de	Permitido	10/02/2016	10/02/2016	15:26:08	18:46:08

Figura 72. Interfaz de reportes por persona.



	Nombre	Apellido Paterno	Apellido Materno	Area	Puesto	SubArea	Tipo Acceso	Dia de Acceso	Dia de Salida	Hora de Acceso	Hora de Salida
2	Guillermo	Prieto	Hernandez	Área de dirección	Director General	Oficina Director Gene	Permitido	10/01/2016	10/01/2016	36:08.0	00:08.0
3	Guillermo	Prieto	Hernandez	Área de dirección	Director General	Oficina Director Gene	Permitido	10/01/2016	10/01/2016	00:08.0	36:08.0
4	Guillermo	Prieto	Hernandez	Área de dirección	Director General	Oficina Director Gene	Permitido	10/01/2016	10/01/2016	46:08.0	36:08.0
5	Guillermo	Prieto	Hernandez	Área de dirección	Director General	Oficina Director Gene	Permitido	10/02/2016	10/02/2016	16:08.0	00:08.0
6	Guillermo	Prieto	Hernandez	Área de dirección	Director General	Oficina Director Gene	Permitido	10/02/2016	10/02/2016	00:08.0	26:08.0
7	Guillermo	Prieto	Hernandez	Área de dirección	Director General	Oficina Director Gene	Permitido	10/02/2016	10/02/2016	36:08.0	56:08.0
8	Veronica	Lopez	Gonzales	Área de dirección	Director de administ	Oficina Director Gene	Permitido	10/01/2016	10/01/2016	00:08.0	10:08.0
9	Veronica	Lopez	Gonzales	Área de dirección	Director de administ	Oficina Director Gene	Permitido	10/01/2016	10/01/2016	10:08.0	26:08.0
10	Veronica	Lopez	Gonzales	Área de dirección	Director de administ	Oficina Director Gene	Permitido	10/01/2016	10/01/2016	26:08.0	46:08.0
11	Veronica	Lopez	Gonzales	Área de dirección	Director de administ	Oficina Director Gene	Permitido	10/02/2016	10/02/2016	36:08.0	20:08.0
12	Veronica	Lopez	Gonzales	Área de dirección	Director de administ	Oficina Director Gene	Permitido	10/02/2016	10/02/2016	10:08.0	56:08.0
13	Veronica	Lopez	Gonzales	Área de dirección	Director de administ	Oficina Director Gene	Permitido	10/02/2016	10/02/2016	56:08.0	59:08.0
14	Diego Miguel	Villaseñor	Ramirez	Área de dirección	Director de ventas	Oficina Director Gene	Permitido	10/01/2016	10/01/2016	36:08.0	40:08.0
15	Diego Miguel	Villaseñor	Ramirez	Área de dirección	Director de ventas	Oficina Director Gene	Permitido	10/01/2016	10/01/2016	20:08.0	56:08.0
16	Diego Miguel	Villaseñor	Ramirez	Área de dirección	Director de ventas	Oficina Director Gene	Permitido	10/01/2016	10/01/2016	36:08.0	16:08.0
17	Diego Miguel	Villaseñor	Ramirez	Área de dirección	Director de ventas	Oficina Director Gene	Permitido	10/02/2016	10/02/2016	46:08.0	20:08.0
18	Diego Miguel	Villaseñor	Ramirez	Área de dirección	Director de ventas	Oficina Director Gene	Permitido	10/02/2016	10/02/2016	50:08.0	36:08.0
19	Diego Miguel	Villaseñor	Ramirez	Área de dirección	Director de ventas	Oficina Director Gene	Permitido	10/02/2016	10/02/2016	06:08.0	46:08.0
20	Julio Cesar	Martinez	Martinez	Área de dirección	Director dde produc	Oficina Director Gene	Permitido	10/01/2016	10/01/2016	36:08.0	00:08.0
21	Julio Cesar	Martinez	Martinez	Área de dirección	Director dde produc	Oficina Director Gene	Permitido	10/01/2016	10/01/2016	00:08.0	36:08.0
22	Julio Cesar	Martinez	Martinez	Área de dirección	Director dde produc	Oficina Director Gene	Permitido	10/01/2016	10/01/2016	46:08.0	36:08.0
23	Julio Cesar	Martinez	Martinez	Área de dirección	Director dde produc	Oficina Director Gene	Permitido	10/02/2016	10/02/2016	16:08.0	00:08.0

Figura 73. Pantalla de reporte Excel.

El sistema que se propone es un sistema realizado para que el exista un administrador que pueda controlar todo y visualizar todo lo que contenga el sistema, así como también que puede crear a otros administrador con ciertos privilegios para que puedan dar de alta, baja o cambio a los empleados del sistema. Los reportes de control que se pueden visualizar se realizan en formato Excel (ver figura 73).

5.6 Importancia de validar la identificación de una persona

Hoy en día existes muchos documentos de identificaron de una persona, la credencial para votar INE(Instituto Nacional Electoral) es el principal documento de identificación de una persona pero también existe por ejemplo: Cartilla de servicio militar (caso de hombre), pasaporte, cedula profesional, licencia de manejo entre otras que en la mayoría son válidos para identificación para los institutos de gobierno y algunas privadas.

En otros caso algunas empresa hacen o entregan alguna contraseña, nip o credencial de la empresa entre otras para tener acceso ya sea a zonas de trabajo o información restringida. Pero estos documentos ya pueden ser falsificando, robados o clonados, como puede ser una credencial de una empresa o incluso la credencial para votar, también las contraseñas pueden ser robadas. Para esto se necesita un mecanismo que nos identifique como la persona que decimos ser, y que sea lo más eficaz posible.

La autenticación biométrica hace posible que una persona pueda ser identificada no por un documento o contraseña sino en lugar de esto puede hacerlo con alguna parte del cuerpo, ya sea palma de la mano, dedo dactilar, iris entre otras.

Es muy importante validar que la persona sea quien dice ser, en algunas empresas y ciertos departamentos de gobierno se toman muy enserio la identificación de su personal pues pueden tener acceso a información o zonas de trabajo que son restringidas para los demás. Un claro ejemplo seria de parte del gobierno en el departamento de seguridad necesita alta seguridad en cuestión de armamento (más específico bombas) pues solo ciertas personas tendrán el acceso para activar o desactivar. La persona no solo entra con una credencial o algún nip sino hoy en día se necesita de la autenticación biométrica ya sea por autenticación por huella dactilar, rostro o iris.

V. CONCLUSIONES Y SUGERENCIAS

La necesidad de tener un sistema de seguridad ya sea para control de acceso o autenticación de individuo ha llevado estar buscando nuevas alternativas de sistemas. Los sistemas biométricos para el control de seguridad es más cada día más empleado y seguro, ya que maneja grandes ventajas de identificar quien es no que trae, como es las características únicas de cada individuo que lo hace ser único. Estos sistemas no recurren al uso de claves personalizadas, tarjetas, llaves, entre otras los cuales son fácilmente de robar o clonar. Sino al proceso de autenticar biométricamente con iris y huella dactilar, esto da una mayor confiabilidad en la seguridad puesto si solo la huella dactilar es un sistema con mayor confiabilidad ahora creando un sistema con dos biométrico, esto duplicará el porcentaje de seguridad, ya que anteriormente para la huella dactilar existían mecanismos para clonar o duplicar una huella dactilar, (aunque estos mecanismos son costoso), en el caso que llegará a pasar el sistema puede reconocer a la persona por la huella dactilar, pero el sistema también requiere el iris de la persona o no podrá tener acceso.

El primer paso a efectuar es adquirir las imágenes biométricas, para así poder continuar con el análisis y poder extraer las características necesarias para realizar el control adecuado. Para el caso de este trabajo, se creó una base de datos para así poder minimizar los costos del proyecto. Cuando se procede a la obtención de la imagen esta puede presentar varios problemas de ambiente, como por ejemplo en cuanto a su contraste, brillo o puede estar movida por lo que el sistema detectara si algún dato aún no está bien registrado o no presenta las características básicas que se requiere en el procesamiento de la imagen (huella dactilar o iris).

Se puede hacer un sistema el cual puede almacenar y administra con mayor facilidad grandes cantidades de información de manera sencilla, eficiente y en este caso con una confiabilidad, hablando de seguridad. Los principales beneficios al implementar este mecanismos son el ahorro de recursos económicos, ahorro de

almacenamiento pues todo se alojará en una base de datos y no en un lugar físico (bodega). Además, que es un sistema amigable pues solo se necesita la mano y el ojo del individuo, no tendrá que preocuparse por recordar la contraseña o preocuparse al perder la tarjeta, llave entre otras cosas. También beneficio para la empresa, pues así no podrá ser manipulado el acceso de las personas en ciertas áreas como también el registro del día y hora de ingreso a las áreas.

Puede que los empleado en un principio se opongan al sistema de autenticación biométrica por iris y huella dactilar pues puede ser algo nuevo para ellos, pero es sistema amigable y se pueden acostumbrar de una manera más fácil así como después pueden conocer entre varios beneficios que obtiene ellos como es seguridad para los empleado como la facilidad de acceso a las áreas. Cuando se habla de facilidad de acceso a las áreas es porque no requieren de un objeto que les permita el acceso llámese tarjeta, gafetes, llaves, nip, contraseñas entre otras. Así el empleado es responsable a donde ingresa y claro donde tiene permiso de accesar y no tener el pretexto que su tarjeta fue utilizada de mala manera por otro empleado.

El objetivo principal de esta investigación se cumplió, a través de la propuesta del sistema de autenticación biométrica a través de huella dactilar e iris de los cuales los elementos principales son el lector de huella dactilar y el lector de iris así como también la base de datos que va a guardar toda la información de los empleados. El sistema puede ser ocupado no solo en el ámbito industrial también en sector público y privado como puede ser una escuela privada para el acceso de sus alumnos como también hospitales de control de sus doctores. El así también el objetivo como estudiante de ingeniería en computación se concreta en otros más específicos relacionados con la formación teórica y la practica adquirida al realizar la propuesta de sistema de autenticación biométrica.

VI. REFERENCIAS DE CONSULTA

A., J. M. (s.f.). Feasibility Studies of Personal IdentificationA.

Alexei, C. M. (2011). sistema de Huella digital para el registro de asitencia de la D.C.B Ingeniero en Computacion. UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

Angela, J. (s.f.). Facial Recognition Systems. Obtenido de Forensic: http://www.forensicevidence

Ávila, C. S. (s.f.). Recuperado el 22 de Septiembre de 2014, de http://www.criptored.upm.es/descarga/TASSI2012_CarmenSanchez.pdf

Ballester, J. (s.f.). Universidad de Murcia. Obtenido de DACTILOSCOPIA: http://www.criminologia.org.es/aportaciones/segundo/nuevodacti.pdf

Biometría Aplicada México. (2012). Soluciones biometricas de huellas digitales. Recuperado el 22 de 11 de 2014, de http://www.biometriaaplicada.com/huella.html

Biometric Computer Technology in Healthcare Forensics. (s.f.). Obtenido de https://sites.google.com/a/g.clemson.edu/efinney140/biometrics

Biometrics. (7 de 09 de 2006). DynamicSig. Obtenido de http://www.biometrics.gov/Documents/DynamicSig.pdf

Biometrics. (7 de Agosto de 2006). Hand Geometry. Recuperado el 23 de 09 de 2016, de http://www.biometrics.gov/Documents/HandGeometry.pdf

BIOMETRICS, D. F. (2013). Obtenido de THE DEFENSE FORENSICS & BIOMETRICS AGE: http://www.biometrics.dod.mil/default.aspx

Blackburn, D. (2006). Biometrics History. Virginia.

Carpenter, M. E. (s.f.). ¿Qué son los sistemas biométricos de huellas dactilares? Recuperado el 16 de Septiembre de 2014, de

http://www.ehowenespanol.com/son-sistemas-biometricos-huellas-dactilares-info_224048/

Courts, N. C. (2005). Individual Biometrics: Iris Scan.

Courts, N. C. (06 de Julio de 2006). Individual Biometrics: Iris Scan". Obtenido de http://ctl.ncsc.dni.us/biomet%20web/BMIris.html

Flores, V. S. (Noviembre de 2014). Revistas Bolivianas Revista del Postgrado en Informática. Obtenido de Algoritmo de Clasificación de Huellas Dactilares Basado en Redes Neuronales Función Base Radial: http://www.revistasbolivianas.org.bo/scielo.php?pid=S3333-77772014000100021&script=sci_arttext

García, L. J. (s.f.). Departament d'Enginyeria Electrònica. Obtenido de Algoritmo para la identificación de personas basado en huellas dactilares: http://upcommons.upc.edu/bitstream/handle/2099.1/8082/proyecto%20final%20de%20carrera.pdf?sequence=1

Goldestein, Harmon, & Lesk. (1971). Identification of Human Faces,. Proc. IEEE, Vol. 59, No. 5.

Group, M. M. (25 de Julio de 2002). "Photobook/Eigenfaces Demo" . Obtenido de http://vismod.media.mit.edu/vismod/demos/facerec/basic.html

Group, N. S. (25 de Abril de 2005). NIST Speaker Recognition Evaluations". Obtenido de http://www.nist.gov/speech/tests/spk/index.htm

Hernández, A. (2009). Tesis: Propuesta de estándar para el uso seguro de. Universidad Nacional Autónoma de México.

Hernández, B. A. (2009). Tesis: Propuesta de estándar para el uso seguro de tecnologías biométricas. Universidad Nacional Autónoma de México.

Huella digital. (2014). Recuperado el 25 de 09 de 2014, de http://www.integracion-de-sistemas.com/Huella_digital/

Instituto de Ciencias Forenses. (2010). Obtenido de Dactiloscopía: http://www.semefo.gob.mx/es/INCIFO/Dactiloscopia

Internacional, (. O. (2003). Biometrics - ICAO Recommendation. Obtenido de http://www.icao.int/mrtd/biometrics/recommendation.cfm

Introducción a la Seguridad Biométrica. (27 de Octubre de 2015). Obtenido de Newzzniper: https://newzzniper.com/index.php/2015/10/27/introduccion-a-la-seguridad-biometrica/

J., J. A. (2008). Handbook of Biometrics. USA.

Java. (2014). Java. Recuperado el 22 de 11 de 2014, de https://www.java.com/es/about/

Jhon, D. W., Nicholas, M. O., & Peter, T. H. (2003). Biometrics. New York: McGraw Hill Osborne.

K., L., & F., R. (s.f.). Development of Integrated Criminal Justice Expert System Applications. Obtenido de http://ai.eller.arizona.edu/COPLINK/publications/develop/developm.html

kimaldi. (21 de 09 de 2016). kimaldi. Obtenido de ¿Qué es la biometría?: http://www.kimaldi.com/area_de_conocimiento/biometria/que_es_la_biometria

Kimaldi Electronics. (s.f.). Obtenido de Terminal de reconocimiento de iris Anviz UltraMatch: http://www.kimaldi.com/productos/sistemas_biometricos/biometricos_por_fabricante/anviz/terminal_de_reconocimiento_de_iris_anviz_ultramatch

Komarinski, P. (2004). Automated Fingerprint Identification.

Lu, J. (2002). "Boosting Linear Discriminant Analysis for Facial Recognition". Obtenido de http://www.dsp.toronto.edu/juwei/Publication/JuweiICIP03.pdf

Netbeans. (2013). Recuperado el 22 de 11 de 2014, de https://netbeans.org/index_es.html

Newzzniper. (27 de Octubre de 2015). Introducción a la Seguridad Biométrica. Obtenido de https://www.newzzniper.com/index.php/2015/10/27/introduccion-a-la-seguridad-biometrica/

NSTC Subcommittee on Biometrics. (2005). Palm Recognition Foundation Document.

Pachay, J. (5 de Agosto de 2011). ¿Que es un Lector Biometrico de retina? Recuperado el 16 de Septiembre de 2014, de http://lectorbiometricoretina.blogspot.mx/2011/08/que-es-un-lector-biometrico-de-retina.html

Perez, E. (s.f.). Reconocimiento dela geometria de la mano. Obtenido de SISTEMAS BIOMETRICOS: https://sites.google.com/site/sistemasbiometricoseliseoperez/home/reconocimiento-dela-geometria-de-la-mano

Phillips, Moon, Rizvi, & Rauss. (2000). The FERET Evaluation Methodology for Face-Recognition Algorithms. IEEE Transactions on PAMI, Vol. 22, No. 10. Obtenido de http://www.frvt.org/FERET/default.htm

Publishing Evaluseek. (2005). Downzoom. Recuperado el 16 de 09 de 2014, de Historia Biometría - En cuanto a las tecnologías biométricas del pasado al presente: http://downzoom.com/historia-biometr%C3%ADa---en-cuanto-a-las-tecnolog%C3%ADas-biom%C3%A9tricas-del-pasado-al-presente_573b3.html

Recognition, N.-S. (7 de Agosto de 2006). Speaker Recognition. Obtenido de http://www.biometrics.gov/Documents/SpeakerRec.pdf

RECONOCIMIENTO FACIAL. (Agosto de 2006). Obtenido de Consejo Nacional de Ciencia y Tecnología (NSTC): http://www.biometria.gov.ar/metodos-biometricos/facial.aspx

REILLO, A. S. (2000). MECANISMOS DE AUTENTICACIÓN BIOMÉTRICA MEDIANTE TARJETA . Recuperado el 16 de Septiembre de 2014, de http://oa.upm.es/844/1/09200001.pdf

relojchecador de México. (2009-2010). Maersa. Recuperado el 16 de Septiembre de 2014, de Historia de la Biometría y la Huella Digital: http://www.maersa.com.mx/historia.html

Sánchez, R. A. (2000). MECANISMOS DE AUTENTICACIÓN BIOMÉTRICA MEDIANTE TARJETA. Recuperado el 16 de Septiembre de 2014, de http://oa.upm.es/844/1/09200001.pdf

seguridad online. (22 de Septiembre de 2014). Obtenido de http://www.seguridad-online.com.ar/index.php?mod=Home&ac=verNota&id_nota=302&id_seccion=96

Tango, D. (05 de Noviembre de 2015). Retina. Obtenido de Medlineplus: https://medlineplus.gov/spanish/ency/article/002291.htm

Trade, J. (13 de Agosto de 2014). TECNOLOGÍA DE IDENTIDAD Y SEGURIDAD, TARJETAS INTELIGENTES E IDENTIFICACIÓ. Recuperado el 16 de Septiembre de 2014, de IDNoticias: http://www.idnoticias.com/2014/08/13/biometria-de-iris-vs-retina-si-en-realidad-son-diferentes

UNAM. (s.f.). Clasificación de los Sistemas Biométricos. Recuperado el 16 de Septiembre de 2014, de UNAM - Facultad de Ingeniería : http://redyseguridad.fi-p.unam.mx/proyectos/biometria/clasificacionsistemas/preprocesadoiris.html

Valdespino, J. L. (22 de Julio de 2008). Slidershare. Recuperado el 22 de septiembre de 2014, de http://es.slideshare.net/contactofaum/metodologa-524067