ESTADO DEL ARTE DE LA SEGURIDAD EN SISTEMAS BIOMETRICOS

ANDREA GIRALDO GIRALO
DIANA PATRICIA GOMEZ RAMIREZ

UNIVERSIDAD ABIERTA Y A DISTANCIA -UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2017

ESTADO DEL ARTE DE LA SEGURIDAD EN SISTEMAS BIOMETRICOS

ANDREA GIRALDO GIRALDO
DIANA PATRICIA GOMEZ RAMIREZ

Proyecto de Grado Monografía para Optar por el Título de Especialista en Seguridad Informática

Director
Luis Fernando Zambrano Hernández
Esp. en seguridad informática

UNIVERSIDAD ABIERTA Y A DISTANCIA -UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2017

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá 13 de diciembre de 2017

DEDICATORIA

Este proyecto de grado se lo dedico a mi familia: mi esposo Hernán Cortes, quien con su apoyo y motivación ha sido fuerza día a día para poder seguir la constante marcha, a mi hijo Nicolás Cortes, quien sacrificó el tiempo en familia para permitirme continuar, a mi papa, hermanas, que con sus constantes palabras de aliento motivaron en mi la disciplina suficiente para alcanzar este logro.

Andrea Giraldo Giraldo

Está tesis está dedicada primero a Dios, por permitirme lograr este objetivo y por darme las oportunidades y la fuerza para culminar esta tarea tan importante en mi crecimiento laboral, profesional y académico.

De igual forma, dedico está tesis a mi hija que es la fuerza que tengo cada día para lograr mis metas y sueños. Por su compañía y apoyo incondicional en mi proceso de formación y que este triunfo sea el ejemplo para que ella forje sus sueños y logre sus objetivos con un horizonte sin limitaciones.

A mis padres por enseñarme a luchar por mis sueños y a trabajar cada día en ellos hasta cumplirlos, por la formación que recibí en hábitos, valores que me permiten superar las dificultades y mantenerme firme en el logro de mis objetivos.

A mi compañera de tesis por su compañía, su fortaleza, su dedicación por alentarme en los momentos difíciles de este proceso y por formar un buen equipo de trabajo para cumplir este sueño.

A mi familia en general, porque siempre recibí su apoyo y su admiración durante todo el camino recorrido para lograr este objetivo.

Diana Patricia Gómez Ramírez

AGRADECIMIENTOS

A Dios por iluminar mi camino en esta dirección, la cual ha traído a mi vida retos y metas superadas gracias a las oportunidades que se han generado crecimiento profesional y personal y que me ha permitido plantear nuevos horizontes. A mi amigos y compañeros que con su constante guía y apoyo.

Andrea Giraldo Giraldo

En primer lugar, agradezco a Dios por haberme permitido mantenerme en este proceso de formación hasta lograr el objetivo de forma satisfactoria superando obstáculos y dificultades.

Agradezco a toda mi familia por la confianza y el apoyo que me brindaron, por su comprensión y entendimiento durante toda la carrera.

Diana Patricia Gómez Ramírez

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

La búsqueda de un medio de autenticación seguro y que no genera ambigüedad es una necesidad que surge desde tiempo atrás, como consecuencia de esta problemática surgen los Sistemas Biométricos dando gran importancia y gran valor a la confidencialidad, integridad y disponibilidad de la información.

Los sistemas biométricos se definen como técnicas automáticas de reconocimiento y autenticación que utilizan el análisis de patrones y/o características físicas y de comportamiento exclusivas de cada persona. El proceso de verificación de la identidad de las personas se realiza comparando los registros de sus datos biométricos con datos que previamente han sido almacenados en la base de datos, el resultado de esta comparación determina la identidad de la persona.

La era tecnológica trajo consigo la automatización de procesos por medio del uso de herramientas y aplicaciones informáticas que deben garantizar la privacidad, seguridad entre otras características de la información.

La clasificación de los sistemas biométricos se da en función de las características usadas por tipo biométrico, y se definen dos tipos los cuales se describen a continuación:

- Sistemas biométricos estáticos: Se enfocan en el estudio de las características físicas de la persona.
- Sistemas biométricos dinámicos: Se enfocan en el estudio de las características conductuales de la persona.

A su vez de los tipos de biometría se pueden extraer ciertos patrones o rasgos característicos de los seres humanos, que, de acuerdo al nivel de madurez alcanzado, en la actualidad existe un gran número de características.

El enfoque de este proyecto son los sistemas biométricos de Reconocimiento y de Autenticación, los cuales se describen más detalladamente en el numeral Clasificación de los sistemas biométricos.

1. TITULO

ESTADO DEL ARTE DE LA SEGURIDAD EN SISTEMAS BIOMETRICOS.

2. DEFINICION DEL PROBLEMA

La biometría es una necesidad que surge desde siglos pasados, la cual ha venido evolucionando en el tiempo debido a la necesidad de las personas de encontrar mecanismos de identificación y reconocimiento de las características de las personas y en la medida que los avances tecnológicos han permitido soportar la evolución a sistemas biométricos estables.

Actualmente, el campo de la biometría está orientado a diferentes áreas como la salud, la ciencia, la tecnología, el Internet de las cosas (IOT) y la autenticación por medio de dispositivos móviles, los cuales se encuentra en constante evolución, de allí toma gran importancia realizar el levantamiento de información que nos permita el análisis de los antecedentes y tendencias de los sistemas biométricos de reconocimiento y autenticación, para el control de acceso e identificación en las organizaciones.

Los sistemas biométricos control de acceso e identificación que actualmente se encuentran más estables, los cuales serán tratados en el presente proyecto son: los sistemas de reconocimiento e identificación de: huella dactilar, facial, retina, iris y firma, los sistemas de geometría de dedos y mano y sistemas de autenticación por voz. A través del análisis de las técnicas como son: los sensores, el procesamiento de la información, la captura de datos, la transmisión de datos biométricos, el procesamiento de señal, los algoritmos de decisión y plantillas de almacenamiento de los sistemas biométricos, se realizará un análisis comparativo de especificaciones de aspectos de funcionalidad, Estabilidad, aceptabilidad, facilidad de uso y estándares actuales de control de acceso e identificación.

Adicionalmente por medio del *benchmarking* se evaluará comparativamente *hardware* y *software* que nos permitirá evidenciar mejores prácticas de usabilidad y prevención de ataques de seguridad en los sistemas biométricos de control de acceso e identificación.

¿Cuáles son las técnicas y especificaciones de seguridad que utilizan los sistemas biométricos de reconocimiento y autenticación, para el control de acceso e identificación, que accedan a buenas prácticas de seguridad, funcionalidad y usabilidad, por medio de las características de una persona?

3. JUSTIFICACION

La necesidad de las organizaciones en la búsqueda de la evolución en el uso de tecnologías, la conexión a través de internet, el intercambio de información, el manejo de grandes volúmenes de datos ha generado al mismo tiempo la automatización de tareas para reducción de costos, errores y tiempo en ejecución de tareas. Así mismo los sistemas de identificación personal que estaban ligados a posesiones de objetos como llaves, tarjetas, números secretos o palabras claves han evolucionado, dando lugar a la necesidad de automatizar mecanismos de control de acceso a los recursos e identificación de las personas por medio de los sistemas biométricos.

Dada la importancia que han cobrado los sistemas biométricos para el control de acceso e identificación y la falta de información consolidada se realiza la recopilación de técnicas, herramientas biométricas, basado en publicaciones recientes, tesis doctorales, documentos de investigación e información relevante que nos permita transferir conocimiento y mejores prácticas de usabilidad y prevención de ataques de seguridad en los sistemas biométricos de control de acceso e identificación.

Esta investigación generará referencia a otros investigadores y organizaciones que requieran evaluar la viabilidad de implementar sistemas biométricos de control de acceso e identificación y servirá como base para alimentar la generación de conclusiones y diferencia de las características de los sistemas biométricos de reconocimiento y autenticación.

4. OBJETIVOS

4.1 GENERAL

Elaborar el estado del arte de la seguridad en los Sistemas Biométricos para control de acceso e identificación.

4.2 ESPECIFICOS

- Realizar el levantamiento de la información conceptual, antecedentes, tendencias, estado de arte de la seguridad en los sistemas biométricos.

- Identificar las técnicas de reconocimiento de patrones, herramientas biométricas, control de acceso e identificación.

- Determinar la usabilidad y la seguridad de los Sistemas Biométricos.

- Diseñar guía comparativa de soluciones y técnicas de sistemas de seguridad en biométricos, para el control de acceso e identificación.

5. MARCO REFERENCIAL

5.1 MARCO TEÓRICO

El término "biometría" se deriva de las palabras griegas "*bio*" (vida) y "*métrica*" (medir), se basa en ideas que fueron concebidas originalmente cientos e incluso miles de años atrás, por lo que se deduce que por medio de la biometría es posible medir e identificar las características de los individuos. Las primeras civilizaciones en la necesidad de reconocer individuos implementaron medios no formales de identificación, tales como, los registros de las transacciones comerciales en Babilonia y China que incluían huellas dactilares, también se tiene antecedentes en la historia egipcia, donde los comerciantes realizaban la descripción física de los comerciantes para recordar su reputación y confianza, pero con el rápido crecimiento de la población se dificultó la identificación de las personas con métodos no formales.

5.1.1 Antecedentes. A mitad del año 1800 cuando llegó la revolución industrial, la incursión de la agricultura y las poblaciones móviles y numerosas, crece la necesidad de crear sistemas formales de identificación y rasgos de identidad de las personas especialmente aplicados en los sistemas de justicia.

Los hitos que marcan la evolución de la biometría como solución para la identificación de las personas, tiene sus orígenes desde hace millones de años, pero los avances automatizados sobre biometría se describen como se puede apreciar en la tabla 1:

Tabla 1. Hitos de Evolución de la Biometría

Biometría	
Año	**Descripción**
1870	Bertillon desarrolla la antropometría para identificar individuos
1998	FBI lanza CODIS base de datos de ADN forense
1999	IAFIS mejora los componentes operacionales del FBI
2000	Se inicia la investigación de uso de patrones vasculares
2002	Se estableció el subcomité 37 encargado de realizar el apoyo para el estándar de tecnologías biométricas de manera genérica.
2003	Se establece el Foro Europeo de Biométricos (*European Biometrics Forum*)
Biometría de la Mano	
Año	**Descripción**
1858	La captura sistemática de imágenes de la mano para fines de registros de identificación.

Tabla 1. (Continuación)

Biometría de la Mano	
Año	**Descripción**
1974	Surgen los primeros sistemas de geometría de la mano
1985	Se concede el Patente de identificación de la mano
1994	Reconocimiento al sistema de palma de mano INSPASS es implementado
1996	Se implementa la geometría de la mano para los juegos olímpicos
2002	Se evalúa el papel de impresión de la palma de la mano
2004	Despliegue de base de datos automatizada de impresión de la palma de la mano en EE. UU
Biometría de la Huella Dactilar	
Año	**Descripción**
1892	Galton desarrolla un sistema de clasificación para huellas dactilares
1896	Henry desarrolla un sistema de clasificación de huellas dactilares
1903	*New York* implementa el reconocimiento de huellas dactilares en las cárceles del Estado Bertillon se derrumba el sistema de antropometría
1963	Hughes publica su investigación de la automatización de huellas digitales
1969	El FBI reconoce el sistema automatizado de reconocimiento de huellas dactilares
1975	El FBI desarrolla los sensores y la tecnología para la extracción de minucias
1986	Se publica el estándar de intercambio de datos de minucias de huellas dactilares
1992	Biométrica incursiona dentro del Gobierno de EE. UU
1999	Lanza estudio sobre la compatibilidad de biometría por máquina de documentos de viaje
2000	Se crea el programa de grado en biometría en *West Virginia*
2002	Se establece la norma ISO/IEC de biometría Se conforma el primer comité técnico de biometría
2003	El gobierno de EE. UU comienza la coordinación de actividades con biométricos OACI adopta plan integral de datos biométricos en los documentos de viaje, se establece el foro europeo de biometría
2004	Se lanza el programa US-VISIT DOD implementa ABIS Obligatoriedad de uso de tarjeta de identificación a los empleados del gobierno
Biometría del Iris	
Año	**Descripción**
1936	Se propone el uso del concepto de patrón de iris para la identificación de individuos
1985	Se expone el concepto de que no existen 2 iris iguales
1987	Se concede la patente que aprueba el uso del iris como identificación
1993	Se desarrolla prototipo de reconocimiento de iris
1994	AFIS crea el sistema de identificación automatizado integrado de huellas dactilares
1995	Prototipo comercial de reconocimiento de iris
2005	Expira la patente de EE. UU sobre el reconocimiento del iris Primera conferencia del Iris
Biometría de la Cara	
Año	**Descripción**
1960	Se desarrolla el sistema semi-automático de reconocimiento facial
1970	El avance de reconocimiento automatizado de rostro
1988	Se da el despliegue al sistema de reconocimiento facial semi-automatizado *Eigenface* desarrolla la técnica de reconocimiento facial

Tabla 1. (Continuación)

Biometría de la Mano	
Año	**Descripción**
1991	Se realiza la detección de rostros en tiempo real
1993	La tecnología FERET inicia el programa de reconocimiento facial
2000	Primera prueba de reconocimiento de rostro (FRVT 2000)
2001	Se usa el reconocimiento facial en el *Super Bowl* en *Tampa Florida*
2004	*Grand Challenger* comienza el reconocimiento de la casa
Biometría de la Voz	
Año	**Descripción**
1960	Se crea el modelo de producción de habla acústica
1970	Se modelan los componentes conductuales del habla
1976	Se desarrolla el prototipo del sistema de voz
1980	NIST crea el grupo de reconocimiento de voz
1994	Se patenta el algoritmo de reconocimiento de voz
1997	NIST inicia el proceso de evaluación anual de reconocimiento de voz
Biometría de Firma	
Año	**Descripción**
1965	Se inicia la investigación de reconocimiento automatizado de firma
1977	Se concede la patente para la adquisición de la información dinámica de la firma

Fuente: Adaptado de NSTC, *Committee on Homeland and National Security, Subcommittee on Biometrics*. Enero, 2001. p. 1-10.

Los sistemas biométricos se han investigado y probado por algunas décadas, pero han entrado recientemente en auge debido a los grandes avances de procesamiento de los computadores, la ampliación de la comunicación y el poder adquisitivo de los recursos que lo soportan. Además, obligados a cumplir al mismo tiempo la creciente demanda de seguridad, que surge en la medida que la tecnología avanza, y de esta manera reducir la suplantación de las personas, la protección de datos personales, los controles de acceso surgen de los entornos tecnológicos modernos.

“Reconocimiento es un término genérico y no necesariamente implica verificación o identificación. Todos los sistemas biométricos realizan un “reconocimiento” para “volver a conocer” a una persona que ya ha sido enrolada previamente.”[1]. "Biometría" es un término general utilizado para describir una característica o un proceso, por lo tanto, existen características de los sistemas de reconocimiento biométrico al momento de realizar la selección del patrón biométrico que deben ser contemplados como: la universalidad, la distinción, la permanencia y la registración. También las características biológicas que se encuentran vinculadas a órganos y sistemas (anatómica y fisiológica) y características del comportamiento medibles o funcionales, que se puede utilizar para el reconocimiento automatizado de reconocimiento de un individuo. Adicionalmente debe tener en cuenta las siguientes

[1] WOODWARD, Jhon D.; ORLANS, Nicholas M. y HIGGINS, Peter T. Biometrics. New York.: McGraw-Hill, 2003.

propiedades: Unicidad, la cual refiere a que no debe existir dos personas con la misma característica, Fiabilidad es el rendimiento o nivel de precisión de reconocimiento, Facilidad de Uso que los usuarios puedan percibir, la Resistencia ataques que está orientada a la resistencia del biométrico de ser burlado, Aceptabilidad de las personas en sus bases culturales, Costo aceptable, No intrusiva cuando se realiza el contacto físico con el sensor, Tamaño del lector de los dispositivos que capturan ya que cuentan con particularidades según la necesidad.[2]

Un sistema biométrico típico se compone de cinco componentes integrados: según NSTC[3] se utiliza un sensor para recopilar los datos y convertir la información a un formato digital, algoritmos de procesamiento de señales que realizan actividades de control de calidad y el desarrollo de una plantilla biométrica, un componente de almacenamiento de datos que mantiene la información de las nuevas plantillas biométricas, que son comparadas con un algoritmo de coincidencia cuyo fin es comprar la nueva plantilla biométrica almacenada. Finalmente, se realiza un proceso de decisión (ya sea automatizado o manual) que utiliza los resultados correspondientes para tomar una decisión a nivel de sistema.

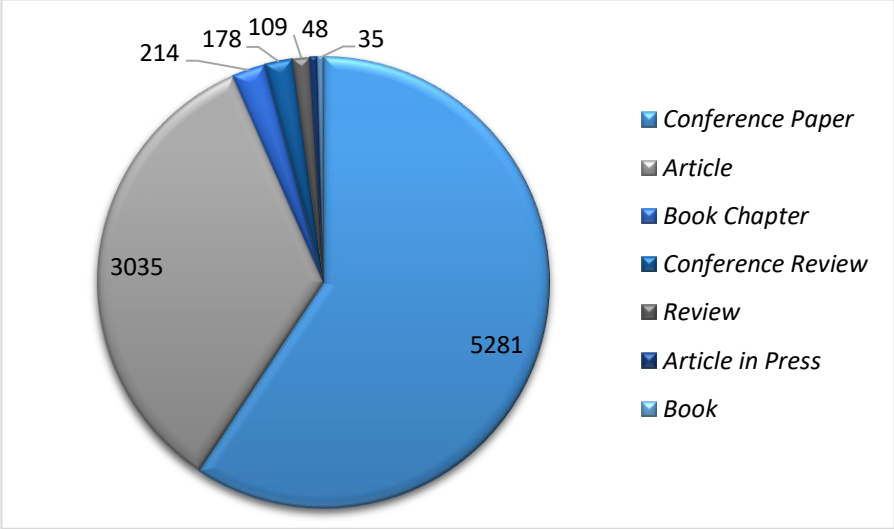
5.2 ESTADO DEL ARTE

5.2.1 Literatura. Para saber que tanto se ha investigado sobre Biometría se tomó como marco de referencia la información registrada en la base de datos Scopus, la cual incluye diferentes tipos documentales tales como: Conferencias, artículos, capítulos de libros, revistas, libros, editoriales, notas, y cartas, el cual nos arrojó un resultado de 19.482 documentos relacionados, desde el año 2010 a la actualidad.

La temática se enfocó en la investigación sobre seguridad en biometría se encontraron 8.932 documentos, los cuales se encuentran distribuidos como se observa en la Figura 1.

[2] WOODWARD, Jhon D.; ORLANS, Nicholas M. y HIGGINS, Peter T. Biometrics [online]. New York.: McGraw-Hill, 2003.
[3] NATIONAL SCIENCE AND TECHNOLOGY COUNCIL. Biometrics Overview

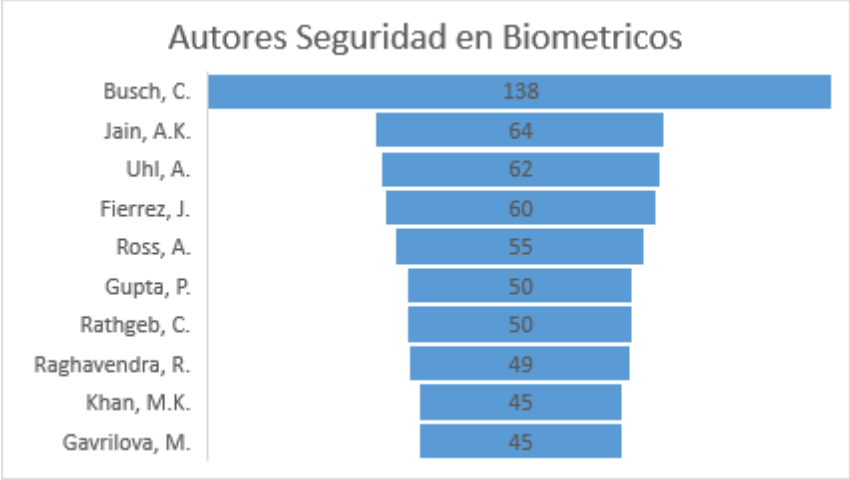
Figura 1. Tipos de Documentos sobre Biometría



Fuente: Adaptado de Base de Datos Scopus https://bibliotecavirtual.unad.edu.co:2098/home.uri

Dentro de los autores que han escrito sobre seguridad en biométricos se encontraron 15 autores representativos, encabezando la lista los tres primeros corresponden a: *Busch, Christoph H.*, de Alemania seguido de *Jain, Anil K*. de Estados Unidos y *Uhl, Andreas* de Austria, que están enfocados en el área de ingeniería y ciencias de la computación como se puede observar en la Figura 2.

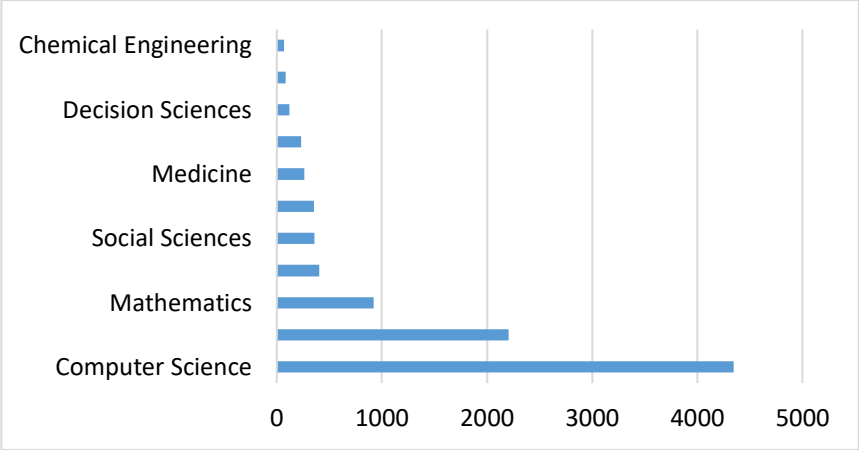
Figura 2. Autores representativos de documentos de Biometría



Fuente: Adaptado de Base de Datos Scopus https://bibliotecavirtual.unad.edu.co:2098/home.uri

La literatura existente sobre seguridad en sistemas biométricos cuenta con alrededor de 5.697 documentos, con un gran aporte de conferencias y artículos, los cuales son en su mayor parte de la India, Estados Unidos y china, los cuales están orientados a las áreas de ciencias de la computación, la ingeniería, matemática, bioquímica y genética molecular, tal como se observa en la Figura 3.

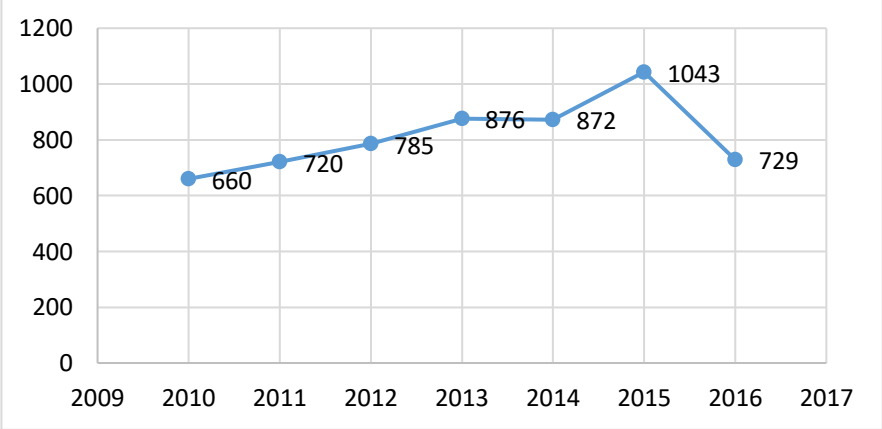
Figura 3. Áreas de aplicación en documentos de Biometría



Fuente: Adaptado de Base de Datos Scopus https://bibliotecavirtual.unad.edu.co:2098/home.uri

La literatura a partir del año 2010, ha tenido un ritmo constante, pero tuvo una fuerte influencia en el año 2015, donde los autores más representativos son: *Busch, Christoph H.*, y *Jain, Anil K*. En la Figura 4 a continuación se puede ver la tendencia de las publicaciones sobre seguridad en sistemas biométricos.

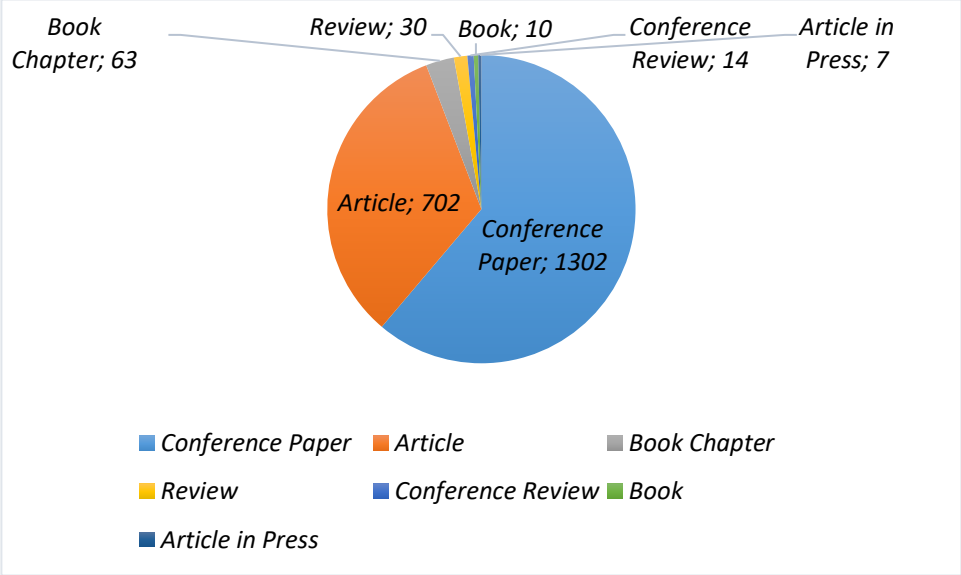
Figura 4. Publicaciones por años de documentos de Biometría



Fuente: Adaptado de Base de Datos Scopus https://bibliotecavirtual.unad.edu.co:2098/home.uri

En la actualidad existe poca literatura orientada a la seguridad en sistemas biométricos de reconocimiento e identificación, y se cuenta con la publicación de 2.128 documentos, ver Figura 5, los que continúan con la tendencia marcada en publicaciones en el año 2015, donde el autor *Busch, Christoph H* continua predominando en las publicaciones relacionadas con la temática e incursión la autor *Gavrilova, Marina L*. de Canadá, con un 61.2% de información relacionadas con conferencias, lo que nos indica que aún es una temática que se encuentra en investigación y desarrollo de nuevas tendencias.

Figura 5. Tipo de Publicaciones de documentos de Biometría

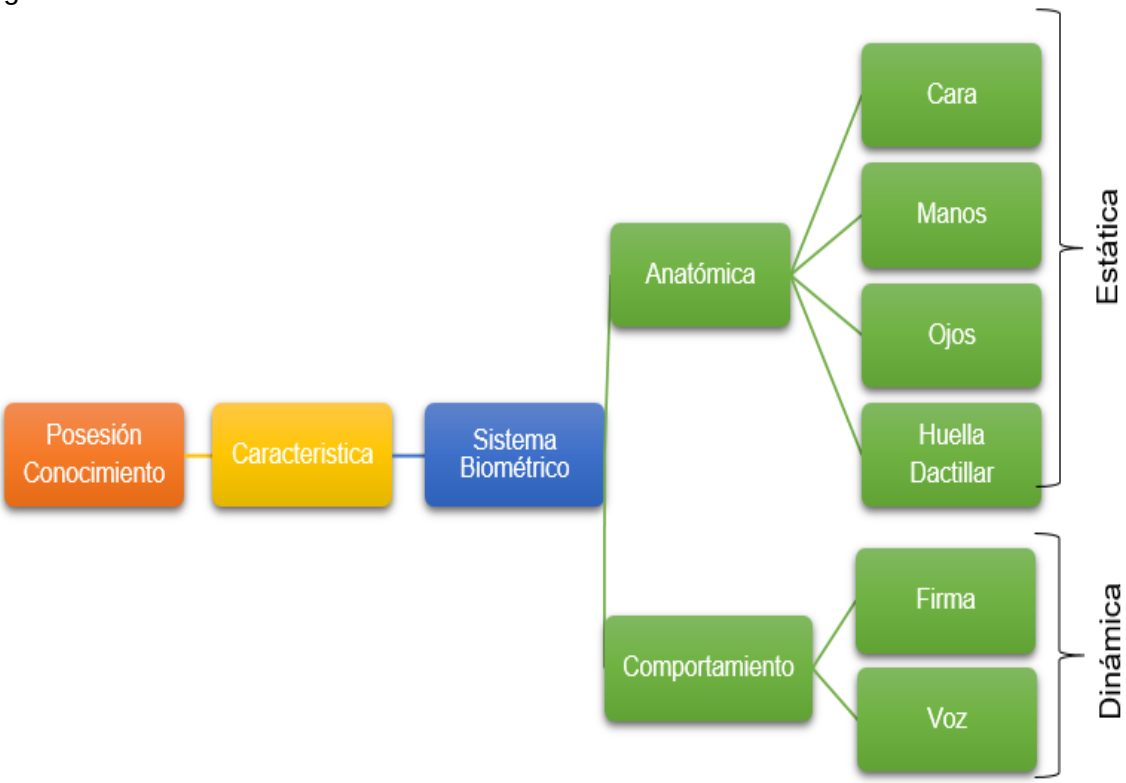


Fuente: Adaptado de Base de Datos Scopus https://bibliotecavirtual.unad.edu.co:2098/home.uri

5.2.2 Sistemas Biométricos. En la actualidad existen investigaciones en diferentes etapas de evaluación y desarrollo de las particularidades biométricas, aunque las técnicas biométricas usan una combinación de factores corporales y de comportamiento. Como se puede apreciar en la Figura 6., Cesar Borja[4] refiere que la medición de las características corporales de las personas se le conoce como biometría estática, está basada en la medición de huellas digitales, la geometría de la mano, el diagrama del iris, la forma de la cara, retina y venas del dorso de la mano. La medición de las características del comportamiento de las personas es conocida como biometría dinámica se basa en patrones de reconocimiento de voz y reconocimiento de firma manuscrita.

[4] BORJA, Cesar. Sistemas Biométricos

Figura 6. Clasificación de los Sistemas Biométricos



Fuente: Sistemas Biométricos. Disponible en: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

Moreno Ana[5] indica que: Los sistemas biométricos pueden ser de verificación o de reconocimiento: En los sistemas de verificación (o autenticación de la identidad) la persona se presenta reportado una identidad, el sistema captura las características biométricas y el sistema realiza la comparación con las características almacenadas, posteriormente genera un resultado de aceptación o rechazo de la identidad de la persona o algún grado de aproximación. En los sistemas de reconocimiento, la persona se presenta aportando las características biométricas y el sistema identifica a la persona, por medio de la comparación de las características de las personas almacenadas. En caso de que no la encuentre proporciona información de novedad de reconocimiento de la persona.

[5] MORENO DIAZ, Ana Belén. Reconocimiento Facial Automático mediante Técnicas de Visión Tridimensional Tesis Doctoral Reconocimiento Facial 2004.

5.2.3 Clasificación de los Sistemas Biométricos

5.2.3.1 Reconocimiento Huella Digital. Biometría[6] menciona que en la huella dactilar usualmente aparecen una serie de líneas oscuras que representan los relieves, tienen una superficie irregular de crestas (líneas oscuras) y valles (líneas claras) que forman un patrón único para cada individuo, entre estas crestas aparecen como espacio en blanco y están en bajo relieve, la porción subyacente de las crestas de fricción ver Figura 7. La identificación por medio del patrón de huella dactilar se obtiene a través de las minucias, la ubicación y dirección de la final cresta y una bifurcación (separaciones) de las crestas a lo largo su trayectoria.

Figura 7. El reconocimiento de la Huella Digital

Fuente: Métodos Biométricos de Reconocimiento de Huella

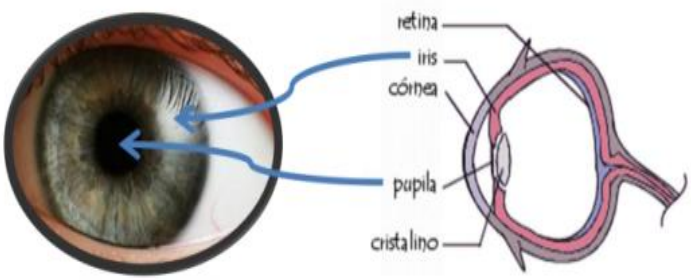
Las técnicas basadas en minucias y la huella dactilar son las más estudiadas y cuenta con mayor número de algoritmos para su análisis. Todos los sensores de huellas dactilares tratan de generar una imagen digital de la superficie del dedo, esta imagen tiene normalmente una resolución de píxel de 500 dpi. La generación de imagen puede ser diferente para cada tipo de sensor.

Actualmente, el reto de los sistemas biométricos de huella dactilar, consiste en el diseño de algoritmos con la capacidad de reconocimiento de manera eficiente, que permita obtener resultados con mayor precisión.

[6] BIOMETRIA. Métodos Biométricos de Reconocimiento de Huella Dactilar [online]. 2016. Disponible en: https://www.nist.gov/programs-projects/biometrics

5.2.3.2 Reconocimiento del Iris. El patrón biométrico del iris permanece a lo largo de la vida y corresponde a un patrón único de cada individuo, debido a que presenta mayor número de características como una especie de huella óptica. Danilo Zorita[7] describe: el ojo cuenta con un músculo que permite regular el tamaño de la pupila, controlando la cantidad de luz que entra en el ojo. Las condiciones de iluminación deben ser constantes ya que el tamaño del iris puede variar con la intensidad lumínica, así como *BHALCHANDRA*[8] describe el iris como la parte coloreada del ojo como se puede ver en la Figura 8, con el colorante basado en la cantidad de pigmento de la melatonina en el músculo.

Figura 8. Diagrama del Iris



Fuente: Caracterización de Iris para posibles aplicaciones de identificación de personas. http://tesis.ipn.mx/bitstream/handle/123456789/14946/ic%20103%2012.pdf?sequence=1

El Autor Borja, indica que "cada iris concentra más de 400 características que pueden ser usadas para identificar a su propietario (criptas, surcos, anillos, fosos, pecas, corona en zig-zag…). Cuenta con un número de puntos distintivos 6 veces superior al de una huella dactilar"[9]

El procedimiento, usado en la actualidad es mucho más sencillo. Por medio de una cámara la cual captura los ojos por medio de una alineación específica en un campo de visión. A continuación, por medio de la captura de una imagen por medio de un algoritmo el cual es almacenado. Dicho algoritmo es conocido como los algoritmos de *Daugman* para obtener el *IrisCode* personal, un patrón único del iris que apenas ocupa 256 *bytes* de información. Este código generado que de manera precisa se encuentre su homólogo en una base de datos que cuenta con los patrones enrolados hasta identificar a su propietario. "Para la codificación del patrón del iris, usualmente se realiza una conversión de la imagen del iris de coordenadas

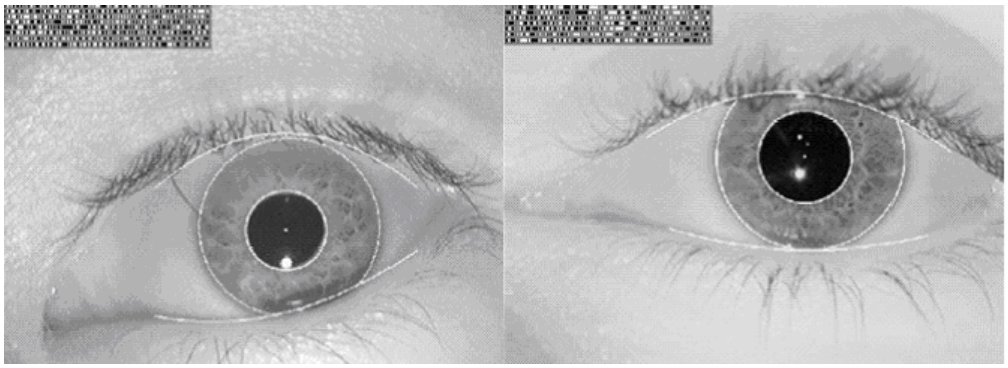
[7] Zorita, Danilo Simón y ORTEGA GARCIA, Javier. Reconocimiento automático medinate patrones biométricos de huella dactilar [online]. Tesis de Doctorado. Madrid: Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingenieros de Telecomunicación, 2003. 225 p

[8] BHALCHANDRA, A. S.; DESHPANDE, N. M. y PANTAWANE, N. G. Iris Recognition [online]. Diciembre, 2008. p. 1073-1078.

[9] BORJA, Cesar. Sistemas Biométricos

cartesianas a polares para facilitar la extracción de información, al pasar de una forma circular a una rectangular. A la nueva representación, se le aplican filtros multicanal, ya sean de *Gabor*, *Fourier* o *Wavelet,* para extraer los coeficientes que finalmente conformaran el código del iris". Ver Figura 10. [10]

Figura 9. Localización del Iris



Fuente: BHALCHANDRA, A. S.; DESHPANDE, N. M. y PANTAWANE, N. G. Iris Recognition véase en: http://connection.ebscohost.com/c/articles/65534673/efficient-speech-based-random-number-generators

El procedimiento del reconocimiento del iris, se realiza según las siguientes etapas:

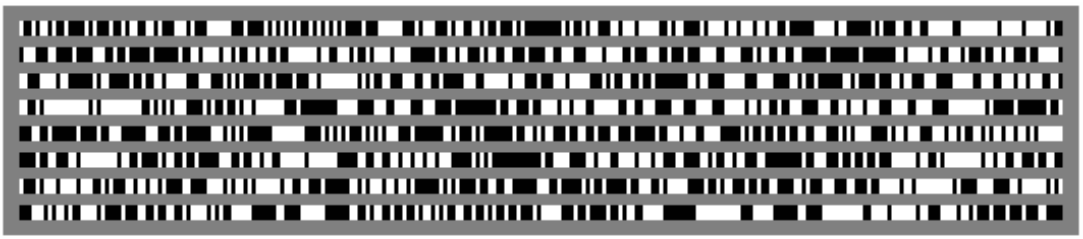
- Captura de Imagen del Ojo.
- Segmentación: se realiza la detección de la imagen capturando los círculos de la pupila y del iris, la segmentación de parpados y filtros consiste en aislar las pestañas y por medio de una matriz la cual obtiene el radio y las coordenadas del circulo que segmenta la pupila y el iris ver Figura 9. Como resultado se obtienen: las coordenadas (x, y) de ambos círculos y sus correspondientes radios, se genera además una matriz que identifica el ruido detectado en la imagen[11].
- Los esquemas blancos indican la localización del iris y los límites de los párpados.
- Normalización: se calcula el desplazamiento de la pupila del centro del iris, localizando la ubicación cartesiana el rededor del iris y los valores de interpolación. Posteriormente la imagen del iris se convierte a coordenadas. Según Valencia Murillo y otros." Se selecciona una cantidad determinada de puntos a lo largo de cada línea radial (resolución radial), y así mismo se define

[10] BHALCHANDRA, A. S.; DESHPANDE, N. M. y PANTAWANE, N. G. Iris Recognition [online]. Diciembre, 2008. p. 1073-1078

[11] UNIVERSIDAD CATOLICA. Extracción de características del Iris como mecanismo de identificación biométrica 2014. vol. 42, p. 1-15.

la cantidad de líneas radiales que van a través de la región del iris (resolución angular)" [12]

Figura 10. La representación pictórica



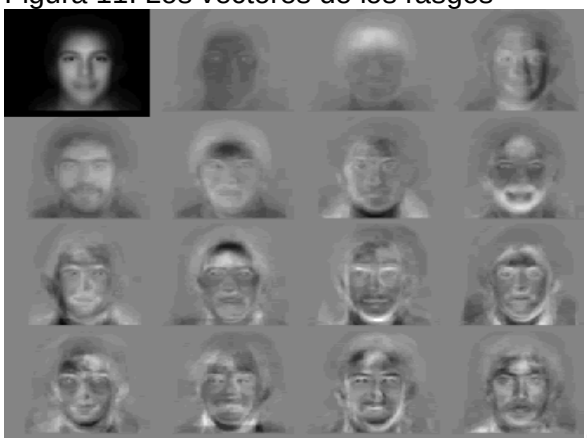
Fuente: BHALCHANDRA, A. S.; DESHPANDE, N. M. y PANTAWANE, N. G. Iris Recognition véase en: http://connection.ebscohost.com/c/articles/65534673/efficient-speech-based-random-number-generators

5.2.3.3 Reconocimiento Facial. Según *National Science and Technology Counci* describe: "El reconocimiento facial está basado en rasgos (geométrico) y lo visual (fotométrico), en el desarrollo de los avances del reconocimiento facial los investigadores desarrollaron algoritmos para obtener precisión según los más estudiados son: Análisis de componentes principales (*Principal Components Analysis, PCA*), Análisis lineal discriminante (*Linear Discriminant Analysis, LDA*), y Correspondencia entre agrupaciones de grafos elásticos *Elastic Bunch Graph Matching, EBGM*)".[13]

PCA exige que las imágenes posean el mismo tamaño, para poder realizar la alineación de ojos y boca de la persona, posteriormente se realiza una compresión para generar una estructura de baja dimensión, retirando información que no sea necesaria y descompone en componentes octogonales la estructura facial. Posteriormente cada imagen se representa como se puede observar en la figura 11 como una suma ponderada o vector de rasgo que se almacenan como un conjunto.[14]

[12] UNIVERSIDAD CATOLICA. Extracción de características del Iris como mecanismo de identificación biométrica 2014. vol. 42, p. 1-15.
[13] NATIONAL SCIENCE AND TECHNOLOGY COUNCIL. Biometrics Overview [online]. Biometrics. Marzo, 2006. vol. 3, p. 1-10.
[14] NSTC, Op. cit

Figura 11. Los vectores de los rasgos



Fuente: Biometrics Overview Biometrics. Disponible en: https://www.nist.gov/programs-projects/biometrics

LDA es utilizada para dar clasificación facial desconocidas basada en ejemplos de entrenamiento con clases conocidas ver figura 12, con la finalidad de maximizar y minimizar la varianza entre bloques las clases de las personas, el cual presenta inconvenientes para realizar las comparaciones faciales de alta dimensión.

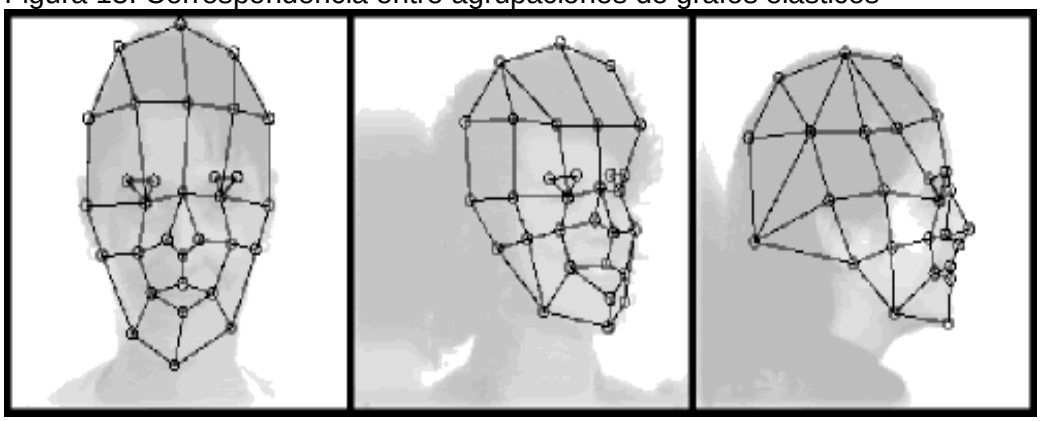
Figura 12. Ejemplo de seis clases usando LDA

Fuente: Biometrics Overview Biometrics. Disponible en: https://www.nist.gov/programs-projects/biometrics

EBGM utiliza imágenes faciales reales con un mayor número de características no lineales que tienen en cuenta características como la iluminación (interior, exterior, fluorescente), la postura de las imágenes, (frontal vs. inclinada) y expresión (sonrisa vs. ceño fruncido)[15]. En la figura 13 explica como por medio de un filtro de correspondencia de grafos elásticos se pueden extraer características y formas después de realizar el procesamiento de la imagen, el cual puede ser el resultado de combinar PCA y LDA.

[15] PEREZ, Pablo. Estudio sobre las Tecnologías Biométricas aplicadas a la Seguridad [online]. Instituto Nacional de Tecnología de la Comunicación. 2011. p. 100.

Figura 13. Correspondencia entre agrupaciones de grafos elásticos



Fuente: Biometrics Overview Biometrics. Disponible en: https://www.nist.gov/programs-projects/biometrics

5.2.3.4 Geometría de dedo y mano. En 1970 se propone un sistema de identificación de personas basado en las medidas de diversas partes del cuerpo, propuesto por el antropólogo francés *Alphonse Bertillon*. El sistema es denominado *Bertillon o Bertillonaje* y fue probado por la policía francesa, una de las primeras instituciones en usar este sistema biométrico fue la universidad de Georgia en 1974. En 1984 este sistema biométrico es usado por el ejército de los Estados Unidos en el sistema financiero. Este sistema biométrico fue patentado por *David Sidlauskas* en 1985, en paralelo fue creada la empresa *Recognition System Inc*. [16]

Este sistema biométrico utiliza la forma de la mano para confirmar la identidad de una persona, su aceptación en sistemas de seguridad es muy elevada, porque no requiere de información detallada de los usuarios. Este sistema biométrico es recomendó para la verificación de personas más no para la identificación de las mismas. [17]

5.2.3.5 Autenticación de la voz. Los acontecimientos más importantes del sistema biométrico de Autenticación de Voz, tuvieron una gran influencia de los años de 1960 a 1996, desde la reproducción de sonidos fónicos hasta, el reconocimiento como control biométrico por voz, representado en la línea del tiempo de la Tabla 2.

[16] PEREZ, Pablo. Estudio sobre las Tecnologías Biométricas aplicadas a la Seguridad [online]. Instituto Nacional de Tecnología de la Comunicación. 2011. p. 120.

[17] HERNANDEZ BRIONES, Avril. Propuesta de estándar para el uso seguro de Tecnologías Biométricas [online]. Trabajo de grado. México: Universidad Nacional Autónoma de México.

Tabla 2. Línea del Tiempo Sistemas Biométrico de Reconocimiento de Voz

Año	Científico	Avance
1960	Profesor, *Gunnar Fant*	Publica modelo que describe componentes psicológicos de producción del habla acústica, basado en el análisis de rayos x de individuos produciendo sonidos fónicos específicos
1970	*Doctor, Joseph Perkell*	Expandió el modelo de Fant utilizando rayos x en movimiento incorporando la lengua y la quijada.
1976	*Texas Instruments*	Esta compañía construye un sistema de prototipo que fue probado por la Fuerza Aérea de los USA y la corporación Mitre.
1980	NITS (Instituto Nacional de Estándares y Tecnología	Desarrolló el grupo de discurso NITS, cuyo principal objetivo fue estudiar y promover técnicas y procesamiento del método de discurso.
1996	NSA (Agencia Nacional de Seguridad)	Buscando avance en el sistema biométrico de reconocimiento de voz, el Instituto Nacional de Estándares y Tecnología lleva a cabo evaluaciones anuales al *Workshop* de Evaluación de Reconocimiento de Voz.

Fuente: El Autor

Los Principios de Funcionamiento del reconocimiento de voz se describen en la Figura 14. Se considera uno de los sistemas biométricos con mayor eficacia, debido a la espontaneidad del habla de las personas.[18]

Figura 14. Principios de funcionamiento de voz

Modo	Descripción
Entrenamiento	Es el proceso de recolección de patrones y valores de referencia de cada uno de los usuarios del sistema.
Funcionamiento o servicio	Es el proceso que pone en funcionamiento el sistema, a partir del reconocimiento de las señales de voz, el sistema evalúa y toma decisiones acerca de la identidad.
Actualización	Es el proceso de administración del sistema, que permite el ingreso, eliminación y actualización de la información almacenada en la base de dato

Fuente: El Autor

Este sistema funciona mediante la digitalización de palabras a partir de la conversión de la señal acústica en una serie de vectores que permiten identificar los patrones únicos de cada individuo como se puede observar en la Figura15, donde

[18] CORTES OSORIO, Jimy Alexander; MEDINA AGUIRRE, Francisco Alejandro y MURIEL ESCOBAR, José A. Sistemas de Seguridad Basados en Biometría [online]. Scientia et Technical. 2010. vol. 17, p. 98-102.

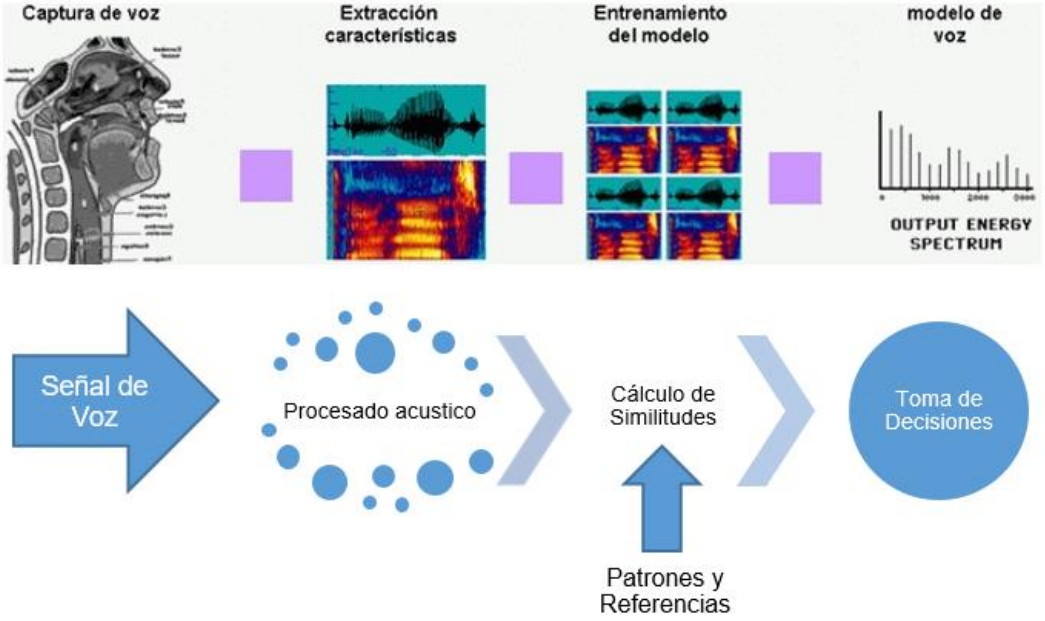
es posible obtener tres o cuatro tonos dominantes que se almacenan de forma digital en una plantilla de voz [19]

Este sistema biométrico tiene tres formas de reconocimiento:

- Dependencia: Siempre se repite el mismo texto
- Texto Aleatorio: El sistema de forma automática escoge un texto a repetir
- Independencia de texto: El usuario tiene la libertad de escoger lo que quiere decir [20]

En relación a factores ambientales “este sistema biométrico es sensible a factores externos como el ruido, el estado de ánimo, el envejecimiento y enfermedades de tipo respiratorio que alteren la voz”. [21]

Figura 15. Proceso de reconocimiento de voz

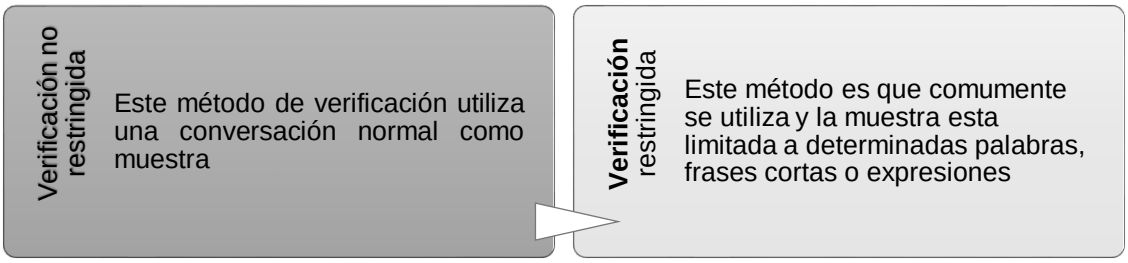


Fuente: Adaptada Propuesta de estándar para el uso seguro de Tecnologías Biométricas Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/biometria/index.html

[19] CORTES OSORIO, Jimy Alexander; MEDINA AGUIRRE, Francisco Alejandro y MURIEL ESCOBAR, José A. Sistemas de Seguridad Basados en Biometría [online]. Scientia et Technical. 2010. vol. 17, p. 98-102.
[20] MISFUD-K IDATZIA, Elvira. Sistemas Físicos y biométricos de seguridad [online]. Observatorio Tecnológico. 2012.
[21] MISFUD-K, Op. cit.,

Los Métodos de verificación del sistema biométrico de reconocimiento de voz se describen en la Figura 16.

Figura 16. Métodos verificación Sistemas Biométricos Reconocimiento Voz



Fuente: Adaptada Propuesta de estándar para el uso seguro de Tecnologías Biométricas Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/biometria/index.html

5.2.3.6 Reconocimiento de la firma. Este sistema biométrico está tipificado como dinámico, el objetivo de este sistema es confirmar la identidad de una persona mediante el análisis de la firma manuscrita, aunque la firma sufre ligeras variaciones, la naturalidad del movimiento al firmar y el número de repeticiones hace que se pueda determinar y reconocer un patrón.

Cada tipo de biométrico puede satisfacer diferentes demandas de uso, algunas de estas son: Geometría de mano, dedo o facial son apropiadas para acceder a áreas restringidas, el reconocimiento de la firma, es apropiado para validar la emisión de mensajes, cheques, transacciones bancarias, el reconocimiento de huella dactilar es la que más implementaciones tiene, es un mecanismo de identificación más usado, pero es el más intrusivo, por lo cual genera más indisponibilidad a las personas, puesto que deberá contribuir para la captura de las huellas.

5.2.4 Seguridad en los Sistemas Biométricos

5.2.4.1 Seguridad en Hardware. En lo referente a la seguridad en *hardware* en los sistemas biométricos no existía una metodología estándar, inicialmente cada país (USA, Canadá y Europa) utilizaba sus propias tecnologías para evaluar esta característica en los productos de TI. En 1996 se fusionaron las tres metodologías para formar la CC (*Common Criteria for TI security evaluation*) reconocido como el único marco de evaluación para establecer e indicar el nivel de seguridad de los sistemas biométricos. La siguiente Figura 17, muestra la historia y los hitos de las evaluaciones de seguridad implementadas:

Figura 17. Evaluaciones de Seguridad Implementadas

País	Patrón Biométrico
USA	Por medio de él DOD 5200.28-SDT (*Departament of Defense Trusted Computer System Evaluation Criteria*" aplicó un conjunto de criterios técnicos de seguridad y metodologías para apoyar el procesamiento automático de datos.
Europa	Utilizó un criterio de evaluación de la seguridad de las tecnologías de la información (ITSEC), creado en 1991 por Francia. Alemania, Países Bajos y Reino Unido con el objetivo de homologar los criterios de seguridad existentes en estos países.
Canadá	En 1993 el centro canadiense de seguridad del sistema implemento los Criterios Canadienses de Evaluación de Productos Informáticos de Confianza (CTCPEC), con el fin de lograr una evolución y actualización de los criterios ya existentes, es considerado el primer preliminar condensada de los tres criterios.

Fuente: Adaptado Evaluation *Methodologies for Security Testing of Biometric Systems beyond Technological Evaluation*

Continuando con el objetivo de los países de crear un solo criterio de evaluación de seguridad para los sistemas biométricos, en 1992 se desarrolló el Criterio Federal para la seguridad de las Tecnologías de la Información (FC), sin obtener mayor avance en este proceso.

Con el apoyo de las organizaciones patrocinadoras (TCSEC, ITSEC, CTCPEC y FC) y la ISO, finalmente en 1993 surgió como metodología de evaluación de los productos de TI "*Common Criteria*" (CC) basado en todos los criterios de evaluación existentes.

"*Common Criteria*" es un marco internacional de evaluación que define la metodología de valoración de los requisitos de asegurabilidad y el conjunto de requisitos funcionales de los productos de TI.

Common Criteria define dos tipos de contramedidas de evaluación que son:

- Contramedidas de TI
- Contramedidas que no son de TI que son generadas por el entorno operativo

El objetivo de este marco es garantizar que el producto que se está evaluando no presenta vulnerabilidades, sin embargo, se debe tener en cuenta que esta evaluación se enfoca en el análisis de las contramedidas de TI y que asume que las contramedidas que no son TI fueron evaluadas por el entorno operativo del producto. El proceso de evaluación se inicia con el análisis del *Security Target* (ST) con el fin de evidenciar que el producto cumple con las declaraciones de seguridad que describe el *Target of Evaluation* (TOE) y el *Security Problem Definition* (SPD).

El CC verifica que las contramedidas sean implementadas por TOE mediante la comprobación que el TOE se comporta de acuerdo a las especificaciones dadas por el ST, garantizando el cumplimiento del *Security Functional Requirements* (SFR's) en el entorno de desarrollo y la documentación requerida. Además de la evaluar estos conceptos la CC también evalúa que los perfiles de protección (PP) sean completos y consistentes de acuerdo al tipo de TOE.

A los sistemas biométricos se les aplica una evaluación adicional de la funcionalidad TOE *Security Functionality* (TSF) que combina elementos de *software* y *hardware* involucrados en las funciones de inscripción, verificación e identificación de estos sistemas. Definimos el *hardware* como el dispositivo de captura biométrico, los medios de almacenamiento de la información y los circuitos requeridos sobre los que opera el *software*, y el *software* contempla la colección de programas que implementan los algoritmos para cumplir con las funciones del sistema biométrico. Con esto se logra que los sistemas biométricos sean evaluados con precisión y siguiendo un esquema de certificación internacional.

5.2.4.2 Seguridad en Software. En cuanto a la seguridad de *software* no existen ataques exitosos debido a la complejidad para burlar dichos sistemas, se pueden establecer dos posibles escenarios para este tipo de ataques.

- El primer escenario, aunque se detecta de forma rápida puede existir una amenaza en la modificación de las muestras biométricas.
- El segundo escenario, es la obtención o fabricación de una muestra
- Biométrica.

Todo sistema de información puede ser burlado, por lo tanto, para implementar un sistema biométrico es necesario aplicar otras medidas de seguridad teniendo en cuenta las amenazas y vulnerabilidades a las cuales está expuesta la información biométrica, las cuales se describen en la siguiente Figura 18.

Figura 18. Amenazas y vulnerabilidades de sistemas biométricos

Amenaza	Descripción
Pérdida o robo de la información biométrica	Los sistemas biométricos manejan información exclusiva y propia del individuo por lo tanto está amenaza es considerada un incidente de seguridad grave.
Suplantación de identidad	Es cuando el acceso a espacios o aplicaciones restringidas se da con el uso de información biométrica falsa o robada.
Sabotaje	Evitar el correcto funcionamiento de los sistemas biométricos realizando ataques consientes a los sensores.
Incumplimiento de la normatividad de protección de datos personales	No cumplir con la ley de protección de datos (Ley 1581 de 2012) o dar un trato inadecuado a los datos biométricos.
Idoneidad de la implantación	Es la necesidad de realizar un análisis entre costo y beneficio de la implantación de un sistema biométrico.
Calidad de la tecnología	El uso de tecnología de punta y adecuada, garantiza mayor seguridad en el uso de sistemas biométricos, se requiere incluir en este punto todos los elementos de un sistema biométrico, para garantizar la calidad de los sensores, el desempeño eficiente del algoritmo de comparación, los controles criptográficos de la base de datos y la integración con otros sistemas.
Incidencias con el sistema	Tener en cuenta un plan de contingencia que supla fallos eléctricos y de comunicación.

Fuente: Adaptada Tecnologías biométricas aplicadas a la ciberseguridad –Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

5.2.5 Tendencias

5.2.5.1 Sistemas de vigilancia electrónica. También reconocida como imperios de vigilancia con insectos voladores robotizados, según Ignacio Ramonet[22] menciona que la tecnología actual permite un tipo de vigilancia omnipresente que antes era solo terreno acotado solo de los escritores de ciencia ficción, tras el 11-S el gobierno norteamericano ha creado culto a la seguridad Estadounidense, pero también para otros gobiernos de países como Francia y España en la lucha contra el terrorismo se ha visto obligado a obtener información con tecnología de punta,

[22] RAMONET, Ignacio. El Imperio de la Vigilancia. C . Intelectual, 2016. p. 168.

reforzando técnicas militares de rastreo y selección de objetivos en los espacios de la vida cotidiana.

Adicional Ignacio Ramonet expone en su reciente publicación “Nuevas estrategias de vigilancia y control implementadas por las autoridades están orientadas a herramientas de espionaje a distancia por medio de tecnologías de seguimiento disponibles como: video, escáner biométrico, satélites, drones, cámaras infrarrojas y técnicas de captación de datos” [23]

5.2.5.2 Internet de las cosas IOT. El internet de las cosas (IOT) es un término propuesto por *Kevin Ashton* en 1999. “Durante una presentación en la que argumentó que mediante la asociación de los objetos físicos con etiquetas RFID, se podría dar identidad a cada objeto para generar datos sobre tales cosas.” [24]

IOT, es el uso de Internet para el intercambio de datos y comunicar información con entidades físicas por los protocolos predefinidos mediante diferentes tecnologías, los objetos de IoT se extendieron a todos los dispositivos inteligentes para procesar y comunicar información a las entidades no inteligentes. Las técnicas relacionadas de su implementación técnica incluyen RFID, redes de sensores inalámbricos (WSN), y la Red de Próxima Generación (NGN) internet inalámbrico móvil. [25]

Según Fabián Cuzme: “La expansión de la Internet de los objetos, al desarrollo de la tecnología de comunicaciones basada en la red se ha convertido en una necesidad para el desarrollo de una tecnología de autenticación de usuario”.[26] Un creciente interés en la información del usuario personal o certificación de clave, la tecnología biométrica ha asegurado que influyen en la competitividad de los fabricantes de *hardware* y *software* móviles para autenticación de usuarios con alta seguridad y comodidad del usuario, métodos de sensor de huellas digitales y no ópticas se dividen principalmente en dos por métodos ópticos, control de acceso permitido, tiempo y asistencia, cerradura de la puerta, como los hogares y zona de seguridad física es principalmente utiliza los métodos de reconocimiento óptico de

[23] RAMONET, Ignacio. El Imperio de la Vigilancia. C . Intelectual, 2016. p. 168.
[24] VARGAS, Georgina A. T. y ARIAS DURA, Raquel. El cómputo ubicuo y su importancia para la construcción del internet de las cosas y el big data [online]. Revista General de Información y Documentación. 2014. vol. 24, no. 2, p. 217-232.
[25] JURADO PEREZ, Luis Alberto; VELASQUEZ VARGAS, Washington Adrián y VINUEZA ESCOBAR, Nelson Fernando. Estado del Arte de las Arquitecturas Internet de las Cosas (IoT)
[26] CUZME RODRIGUEZ, Fabián Geovanny. El internet de las cosas y las consideraciones de seguridad [online]. Tesis de Maestría en Redes de Comunicaciones. Ecuador: Pontificia Universidad Católica del Ecuador. Facultad de Ingeniería, 2015. 179 p

huellas dactilares teléfonos inteligentes incluyendo en los dispositivos móviles está disponible sensor capacitivo de huellas digitales basado en semiconductores.

El Internet de las cosas, conocida como la tercera ola de la industria de la información del mundo, ha sido generalizado en nuestra sociedad. Muchos países consideran la IO como una tecnología nacional de nivel estratégico. En la era de la IO, cómo desarrollar evolución de la tecnología biométrica es una cuestión de preocupación.

El objetivo del control de acceso biométrico para aplicaciones de comercio electrónico en red y Banca, proyecto es desarrollar e implementar un sistema de seguridad con detección mejorada, esquemas de autenticación y control de acceso a las aplicaciones a través de Internet y el teletrabajo *webbanking* servicios.

5.3 MARCO CONCEPTUAL

- Característica Biométrica: identificación automática de una persona basada en características anatómicas o trazos personales:[27]:

    - Universalidad: Está presente en todas las personas
    - Unicidad: Debe ser diferente para todas las personas
    - Permanencia: No varía en corto tiempo
    - Inmutabilidad: No varía en el lapso de vida del individuo.
    - Colectabilidad: No puede causar ningún daño durante el proceso de adquisición y procesamiento.
    - Mensurabilidad: Es cuantificable.
    - Rendimiento: El proceso de reconocimiento debe ser rápido, sólido y preciso.
    - Aceptabilidad: El uso es aceptado por toda la población.
    - Invulnerabilidad: Difícil de imitar por su robustez.

- Control de Acceso: es una medida de seguridad activa que previene de peligros que en último extremo podrían afectar el núcleo de cualquier sistema de información.[28]

[27] LUIS JOYANES. Big Data, análisis de grandes volúmenes de datos en organizaciones. 2016 [online]

28 PURIFICACIÓN AGUILAR. Control de acceso en el entorno físico (seguridad informática). 2011, p.54. [online]

- Fisiología: estudia las funciones de los seres vivos y el cómo un organismo lleva a cabo las diversas actividades vitales: cómo siente, cómo se mueve, cómo se adapta a unas circunstancias cambiantes, y cómo da lugar a nuevas generaciones.[29]

- Modalidad Conductual: Evalúa los rasgos biométricos que implican la ejecución de una acción de comportamiento propia del individuo y que se adquiere a través del tiempo.

- Modalidad Física: Está modalidad se encarga de evaluar los patrones biométricos anatómicos o físicos de las personas y no es necesario que los usuarios realicen acciones específicas.

- Reconocimiento de Patrones: es la ciencia que se ocupa de los procesos sobre ingeniería, computación y matemáticas relacionados con objetos físicos o abstractos, con el propósito de extraer información que permita establecer propiedades de entre conjuntos de dichos objetos.[30]

- Sensor: dispositivo que capta magnitudes físicas (variaciones de luz, temperatura, sonido, etc.) u otras alteraciones de su entorno.[31]

- Sistema Biométrico: un sistema automatizado que realiza labores de biometría. Es decir, un sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada.32

[29] UNAM. Biometría Informática. [online]
[30] NATIONAL SCIENCE AND TECHNOLOGY COUNCIL. Face Recognition [online]. NSTC, Committee on Homeland and National Security, Subcommittee on Biometrics. Enero, 2001. p. 1-10. Disponible en: https://www.dhs.gov/biometrics
[31] NSTC, Op. Cit., p 1-110
[32] NSTC, Op. Cit., p 1-110

5.4 MARCO LEGAL

Los sistemas biométricos de autenticación, cuentan con un aspecto relevante que se podrían definir sus normas o estándares los cuales deben ser universalmente aceptados y con la finalidad de asegurar que su efectividad y precisión frente los requerimientos definidos por los usuarios, con el fin de permitir la compatibilidad desde diferentes lugares, permitiendo de esta manera la reducción de las diferencias entre los diferentes sistemas biométricos y generar un ambiente estable, maduro y que garantice la calidad, además, dichas normas o estándares contribuyen en la detección de vulnerabilidades y facilitan la investigación sobre los controles a implementar para la prevención de la violación de vulnerabilidades en los sistemas biométricos de reconocimiento e identificación.

La normalización entorno a la biometría inició alrededor de los años ochenta surgieron los estándares que permitieron realizar el intercambio de datos, donde se encuentran varios organismos internacionales de normalización como la comisión electrónica internacional (IEC) y el sector de telecomunicaciones (UIT-T). A mediados de los años noventa se genera la necesidad de la creación de interfaces comunes en donde se involucra el sector privado y sectorial, lo que logra que en el año de 2002 se realice la conformación del subcomité de identificación biométrica debido al creciente interés de diferentes autoridades.

De acuerdo a los anteriores antecedentes se reconoce como principal organismo que coordina las actividades de estandarización biométrica el Sub Comité 17 (SC17) del *Join Thechnical Committee on Information Technology* (ISO/IEC JTC1) se publica una lista de estándares biométricos y sus áreas de aplicación, el cual estableció algunas categorías: colección de datos biométricos, almacenamiento y registro de intercambio, perfiles de transmisión de datos biométricos, perfiles biométricos de credenciales de identidad, normas técnicas de interfaz, métodos de prueba para los estándares de metodología de prueba de rendimiento de los sistemas biométricos.[33]

[33] BOUIHROUZAN BELHAJ, Omar. Seguridad e inseguridad en los sistemas biométricos: seguridad vs privacidad [online]. Proyecto Fin de Carrera / Trabajo Fin de Grado, E.T.S.I. y Sistemas de Telecomunicación (UPM) [online]. Madrid 2016.

5.4.1 UIT-T X. El UIT-T X[34] Organismo del Sector de las Telecomunicaciones, inició los trabajos sobre biometría alrededor del año 2001 con la responsabilidad del estudio de la identidad y las metodologías técnicas adecuadas paras identificar los individuos y la protección de la identidad. En la tabla 3 se pueden observar las recomendaciones de UIT-T-X aplicadas a los sistemas biométricos.

Tabla 3 Recomendaciones de UIT-T X aplicadas a sistemas biométricos.

Normalización Aplicada a los Sistemas Biométricos	
X.1081	Propone el Marco para la especificación de los aspectos de la biometría relativos a la protección y seguridad, proporcionando un modelo para identificar y especificar aspectos de seguridad de la biometría y la clasificación de las tecnologías biometrías implementadas en el reconocimiento e identificación.
X.1082	Propone el Marco para la biometría relativa a la fisiología humana.
X.1083	Propone el Protocolo para la implementación de la tecnología de información biométrica y el funcionamiento con interfaces de programación.
X.1084	Propone Mecanismos del sistema de biometría con el Protocolo general de autenticación biométrica y perfiles para sistema de telecomunicaciones. Parte 1.
X.1085	Propone Mecanismos del sistema de biometría con el Protocolo general de autenticación biométrica y perfiles para sistema de telecomunicaciones. Parte 2.
X.1086	Establece guías sobre medidas técnicas de gestión para la protección de seguridad de los datos biométricos.
X.1088	Propone el Marco de protección claves digitales de biometría.
X.1089	Establece lineamiento para la infraestructura de autenticación biométrica (Gestión).
X.1090	Establece Marco de autenticación por medio de plantilla biométrica de un solo uso.
X.1091	Establece la directriz para la evaluación de técnicas de protección de la plantilla biométrica.

Fuente: Biometrías 2 Disponible en: http://www.biometria.gov.ar/media/74948/biometrias2.pdf.

5.4.2 ISO/IEC35 19794. La norma ISO/IEC 19794 define los formatos que deben ser cumplidos por cada técnica biométrica para el uso de los datos. En la Tabla 4 podemos observar las recomendaciones aplicadas a los sistemas biométricos.

Tabla 4. Recomendaciones ISO/IEC 19794 aplicadas a sistemas biométricos.

Normalización Aplicada a los Sistemas Biométricos	
ISO/IEC 19794-3: 2006	Normaliza el formato de los datos para sistemas biométricos basados en patrones de dedos.
ISO/IEC 19794-1: 2011	Normaliza el formato de datos biométricos para el intercambio entre aplicaciones, también describe aspectos y requisitos generales para el intercambio de datos biométricos, con la finalidad de proporcionar independencia a la plataforma.

[34] . UIT *International Telecomunication Unión*
[35] ISO, *The International Organization for Standardization*

Tabla 4. (Continuación)

Normalización Aplicada a los Sistemas Biométricos	
ISO/IEC 19794-2: 2013	Normaliza el formato de los datos para sistemas biométricos basados en minucias de los dedos.
ISO/IEC 19794-4: 2011	Normaliza el formato de los datos para sistemas biométricos basados en imágenes de dedo con formatos JPEG, JPEG2000, WSQ.
ISO/IEC 19794-5: 2011	Normaliza el formato de los datos para sistemas biométricos basados en imágenes del rostro con formatos PNG, JPEG2000 *lossless*.
ISO/IEC 19794-6: 2011	Normaliza el formato de los datos para sistemas biométricos basados en imágenes del iris.
ISO/IEC 19794-7: 2014	Normaliza el formato de intercambio de datos para sistemas biométricos en base a la realización de firmas que utilizan dispositivos como tabletas o sistemas bolígrafo inteligente.
ISO/IEC 19794-8: 2011	Normaliza el formato de los datos para sistemas biométricos basados en el esqueleto del dedo.
ISO/IEC 19794-9: 2011	Normaliza el formato de los datos para sistemas biométricos basados en imágenes vasculares, realizando la definición del contenido del formato y las unidades de medida para el intercambio de datos estableciendo elementos obligatorios y opcionales.
ISO/IEC 19794-10: 2011	Normaliza el formato de los datos para sistemas biométricos basados en la geometría de la mano.
ISO/IEC 19794-11: 2013	Normaliza el formato de los datos para sistemas biométricos basados en firmas dinámicas.
ISO/IEC 19794-13	Normaliza el formato de los datos para sistemas biométricos basados en la Voz.
ISO/IEC 19794-14: 2013	Normaliza el formato de los datos para sistemas biométricos basados en el ADN.
ISO/IEC 19794-15	Normaliza el formato de los datos para sistemas biométricos basados en el patrón de líneas de la palma de la mano.

Fuente: Biometrías 2 Disponible en: http://www.biometria.gov.ar/media/74948/biometrias2.pdf

5.4.3 ISO/IEC 27018: 2014 Requisitos para la protección de la información de identificación de información personal (PII)

5.4.4 CBEFF [36] (*Common Biometric Exchane File Format*)**.** La primera versión del estándar CBEFF 1.0, se remonta del año 2001 la cual fue respaldada por las NIST (Instituto Nacional de Estándares y Tecnología americano), en la actualidad está disponible la CBEFF 2.0 y define los formatos de patrones biométricos para facilitar el acceso e intercambio de diferentes tipos de datos biométricos entre diferentes sistemas. Lo anterior se realiza por medio de la asignación de un formato en la cabecera de los ficheros, estableciendo campos obligatorios y opcionales proporcionando opciones de seguridad, integridad de datos, fecha de creación del fichero, firma y tipo de parámetro biométrico, favoreciendo positivamente la interoperabilidad entre diferentes aplicaciones biométricas y los sistemas,

[36] CBEFF, Common Biometric Exchange File Format.

facilitando la integración de *software*, *hardware* y finalmente establecer un método común para el manejo de los datos biométricos.

5.4.5 BioAPI. consorcio apoyado por compañías internaciones informáticas de gran reconocimiento como IBM y *Hewlett Packard* y con el respaldo del Subcomité SC337 normaliza la comunicación entre las aplicaciones y los dispositivos biométricos y el almacenamiento de los datos por medio de funciones que permiten interactuar modularmente con los dispositivos biométricos.

5.4.6 AENOR (Asociación Española de Normalización y Certificación). AENOR en el año de 2006 creó el Subcomité de Identificación Biométrica AEN/CTN71/SC37 quien es responsable de la Normalización y certificación de sistemas biométricos en España.

5.4.7 ANSI X.9.84. El ANSI/NIST ITL[37] es el estándar utilizado para la transmisión de datos biométricos e información asociada utilizado por las fuerzas y organismos de seguridad, principalmente en los Estados Unidos y a nivel internacional, además participa con otras organizaciones que también desarrollan diversos estándares de biometría como son: OACI[38], INCITS/M1, ISO/SC37 y recomendaciones de mejores prácticas (BPR)[39] que describen opciones adecuadas para los diferentes tipos de escenarios.

Dentro del marco Legal de los sistemas de patrones de identificación biométrica, es importante tener en cuenta, las expectativas y los requisitos de protección legal, cultural y de la privacidad. El estándar X9.84 proporciona integridad y privacidad mediante métodos criptográficos con la finalidad de cifrar la integridad y la privacidad.

5.4.8 Marco Regulatorio. Con el creciente avance de la tecnología y la globalización, también se están planteando nuevos retos para la Protección de Datos Personales, debido a la creciente demanda de captura e intercambio de datos de identificación e información personal.

---

[37] ANSI / NIST-ITL es el acrónimo de American National Standards Institute / National Institute of Standards and Technology, Information Technology Laboratory. Esto significa que el NIST-ITL está acreditado por ANSI como una SDO. ANSI/NIST-ITL 1-2011 y sus predecesores se encuentran disponibles en inglés en: *http://www.nist.gov/itl/iad/ig/ansi_standard/cfm*. El gobierno de Argentina traducirá la norma en español.

[38] El estándar de la OACI para documentos de viaje, Documento 9303.

[39] La BPR Está disponible sólo en inglés.

La protección de datos personales biométricos requiere adicionalmente contemplar unas medidas de seguridad jurídicas, principalmente contemplando los datos según su naturaleza como los datos sensibles, ya que se puede incurrir en diferentes riesgos que afectan la intimidad y privacidad de una persona. La legislación que tiene influencia en la protección de datos aplicada a los sistemas biométricos se puede identificar en la tabla 5.

Tabla 5. Legislación Aplicada a Sistemas biométricos.

Lugar	Legislación	Descripción
Europea	Directiva 95/46/CE Parlamento Europeo y del Consejo 24/10/1995	Protección de tratamiento de datos personales y libre circulación de datos.
Europea	Reglamento (UE) 2016/679 Parlamento Europeo y del Consejo 27/04/2016	Deroga la Directiva 95/46/CE Aprueba el Reglamento General de Protección de Datos. El Reglamento aplica a toda Europa y contempla algunos aspectos como: • Consentimiento y derechos de los usuarios. • Evaluaciones de Impacto. • Privacidad desde el diseño por defecto. • Medidas de seguridad. • Ámbito de aplicación. • Régimen Sancionador. • Obligación de Informar sobre vulneraciones de seguridad. (Brechas de Seguridad) • Figura del delegado de protección de datos (Data Protection Officer)
Europea	Ley Orgánica 15/1999 13/12/199	Protección de Datos de Carácter personal Establece principios de protección de datos personales en España en el sector público o privado que traten datos de carácter personal para el desarrollo de su actividad.
Europea	Real Decreto 1720/2007 21/12/2007	Reglamento de Desarrollo de la LOPD Establece principios de protección de datos personales en España en el sector público o privado que traten datos de carácter personal para el desarrollo de su actividad y medidas de seguridad de carácter físico, técnico y organizativo que deben ser implantadas sobre los datos en sistemas biométricos.
Europea	Reglamento (EU) 2016/679	Reglamento concerniente al Tratamiento de Datos personales y a la Libre Circulación el cual se encuentra vigente.

Tabla 5. (Continuación)

Colombia	Ley 1581 de 2012 MINTIC 27/06/2013	Marco general de Protección de Datos Personales en Colombia. La cual ordena el tratamiento de datos sensibles (biométricos)
Colombia	Decreto Reglamentario 1377 de 2013	Que advierte que, al tener información sensible, las entidades tendrán unos controles superiores, acordes con la norma ISO/IEC 27001 y demás estándares técnicos.

Fuente: El Autor

6. MARCO DE METODOLOGÍCO

6.1 METODOLOGIA DE LA INVESTIGACIÓN

La investigación a realizar será de tipo cualitativo porque se identificarán las variables para la identificación de parámetros de los sistemas biométricos.

6.1.1 Tipo de Investigación. El tipo de investigación a utilizar en este proyecto es investigación documental argumentativa exploratoria, el proceso investigativo inicia con la búsqueda de antecedentes y las referencias del tema seleccionado en documentos como trabajos de investigación, ensayos, artículos, documentados publicado en revistas indexadas, tesis de grado a nivel de pregrado, maestrías y doctorado. Este tipo de investigación permite una vez recopilada la información sea posible realizar un análisis para dar cumplimiento a cada uno de los objetivos definidos.

6.1.2 Técnicas de Análisis de Datos. La metodología que será utilizada para este proyecto es la metodología de benchmarking, que consiste en un proceso sistemático y continuo para comparar o evaluar productos, servicios y procesos para encontrar las diferencias y de esta manera escoger la mejor opción. La metodología pretende alcanzar los siguientes aspectos:

- Implantar mejores prácticas referenciales conocidas
- Determinar el uso estratégico del análisis de la situación para determinar ¿Dónde estamos? Y ¿Dónde queremos ir?
- Fijar un plan de chequeo sobre los objetivos establecidos
- Facilitar la toma de decisiones

6.1.3 Técnicas de Procesamiento de Datos. Se usará el análisis de la percepción de la documentación publicada y de los datos obtenidos durante la investigación.

6.1.4 Población y Muestra. Dentro del marco de los sistemas biométricos se tendrá en cuenta sistemas biométricos de identificación de los patrones de las personas para el control de acceso y autenticación a los sistemas por medio de Reconocimiento de huella dactilar, iris, facial, dedo y mano y autenticación por voz y firma.

6.2. METODOLOGÍA DE DESARROLLO

La metodología de desarrollo planteada contempló el desarrollo de las siguientes actividades, definidas para lograr cumplir los objetivos propuestos para la consolidación del proyecto.

- Hacer la investigación de sistemas biométricos.
- Búsqueda de fuentes bibliográficas confiables, los artículos y estudios sobre sistemas de control biométrico, de sistemas biométricos.
- Buscar las técnicas aplicadas para el reconocimiento de técnicas biométricas de los sistemas biométricos.
- Realizar la búsqueda de herramientas usadas para el control de acceso.
- Establecer criterios o variables para medir las características usabilidad los sistemas biométricos.
- Establecer criterios o variables para medir las características la seguridad de los sistemas biométricos.
- Realizar la comparación para sacar las mejores características de los sistemas biométricos.
- Elaborar la Guía para identificar los mejores sistemas para el control de acceso biométrico

6.2.1 Alcance del Proyecto. Se enfocó la presente investigación, donde se estableció la delimitación de la temática de investigación documental.

6.2.2 Levantamiento de Información de Sistemas Biométricos. La fase de levantamiento de información, por medio de la cual se logró identificar las referencias bibliográficas que se encuentran disponibles orientadas a indagar el pasado, presente y algunas vistas de cómo se posicionarán los sistemas biométricos orientados a apoyar la seguridad desde la implementación de controles de acceso, los cuales colaboran en el presente y un futuro mediato conforme avanza la revolución tecnológica, las actividades realizadas fueron:

- Escoger el tema
- Recolección de bibliografía de acuerdo a los siguientes criterios:
    - Sistemas biométricos actualmente utilizados
    - Uso y aplicabilidad de los sistemas biométricos
    - Seguridad de sistemas biométricos
- Elaboración de fichas con la información básica de los documentos

- Lectura rápida del material recolectado, con el fin de ubicar ideas principales, tener un concepto de la calidad de la bibliografía y escoger las fuentes confiables
- Delimitar el tema con base a la información recolectada
- Elaborar un cronograma de trabajo

6.2.3 Determinación de usabilidad y seguridad de los Sistemas Biométricos.

La fase de determinación de usabilidad y seguridad de los Sistemas biométricos, nos permite dar una mirada detallada sobre cada uno de los sistemas, las condiciones que deben ser contempladas y las cuales lograron llegar a obtener el resultado final.

- Realizar la búsqueda de nueva información de acuerdo a la delimitación definida
- Lectura detallada del material bibliográfico recolectado
- Elaborar fichas de contenido con el fin de sintetizar el tema, extraer las ideas más relevantes y generar nuestro análisis, reflexiones y comentarios del tema
- Organización de las fichas de contenido y del esquema definido
- Organización definitiva del fichero, con el fin de evaluar si todos los datos esenciales del tema están contemplados
- Redacción del trabajo final

7. TECNICAS DE RECONOCIMIENTO DE PATRONES DE SISTEMAS BIOMETRICOS

La alta demanda que día a día conllevan a disminuir la sensación de inseguridad en diferentes contextos, que proponen realizar un control de acceso con técnicas nuevas y con menos probabilidad de ser vulneradas, debido a ello, se incrementa la demanda del uso de sistemas biométricos, con la finalidad de poder realizar de manera eficiente y precisa el reconocimiento de los individuos. Por lo anteriormente mencionado se realiza una descripción de las técnicas de reconocimiento de patrones de sistemas biométricos.

7.1 COMPONENTES DE UN SISTEMA BIOMÉTRICO

Los sistemas biométricos están diseñados con el propósito de reconocer y autenticar personas con base al análisis de sus patrones físicos o de comportamiento, para realizar estos procesos es necesario conocer los siguientes conceptos que aclaran el funcionamiento de un sistema biométrico.

7.1.1 Sensor. Es un dispositivo que se clasifica como captador y está diseñado para recibir y transformar información. En el enfoque biométrico el sensor es el encargado de capturar rasgos biométricos o características de identificación del individuo y convertirlos en datos digitales. La Figura N° 19 relaciona los sensores por tipo de sistema biométrico.

Figura 19. Sensores según tipos de tecnología biométrica

Sistemas Biométricos de Reconocimiento	Dispositivos de Captura
Escritura de Teclado	Teclado
Facial	Cámara de Video o Cámara integrada del PC
Firma	Tableta de Firma, Puntero Sensor al Movimiento
Geometría de la Mano	Unidad Propietaria de Pared o píe
Huella Dactilar	Periférico de Escritorio, tarjeta Lector Integrado

Figura 19. (Continuación)

Biométricos de Autenticación y Reconocimiento	Dispositivos de Captura
Voz	Micrófono o Teléfono
Retina	Unidad Propietaria de Pared o pared
Iris	Cámara de Infrarrojos

Fuente: Adaptada Estudio sobre las Tecnologías Biométricas aplicadas a la Seguridad Disponible en: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnologíasBiométricasASeguridad.pdf

7.1.2 Repositorio. Este componente es de almacenamiento y se encarga de guardar las plantillas biométricas, debe contar con un protocolo de seguridad adecuado, los datos deben estar encriptados y digitalizados.

7.1.3 Algoritmos. Son operaciones sistemáticas que tienen como funcionalidad registrar, verificar e identificar los datos, por medio de la recolección de muestras biométricas que usan diferentes algoritmos.

7.2 REGISTRO DEL SISTEMA BIOMETRICO

Cada usuario realiza el proceso de registro de su identidad en el sistema biométrico, esto se hace mediante la obtención y captura de muestra biométrica y se compone de tres fases:

7.2.1 Captura. Recoge la imagen o señal de la característica biométrica del usuario y la convierte en un formato digital que va a ser procesado en una fase posterior. Este dispositivo es diferente para cada sistema biométrico. Para implementar el proceso de los sistemas biométricos se requieren el registro de los datos de los usuarios por medio de parámetros biométricos descritos en la Figura 20.

Figura 20. Parámetros de Sistemas Biométricos

Sistemas Biométricos de Reconocimiento	Patrón Biométrico
Escritura de Teclado	Registro de las teclas pulsadas y registro de medidas relacionadas con la dinámica

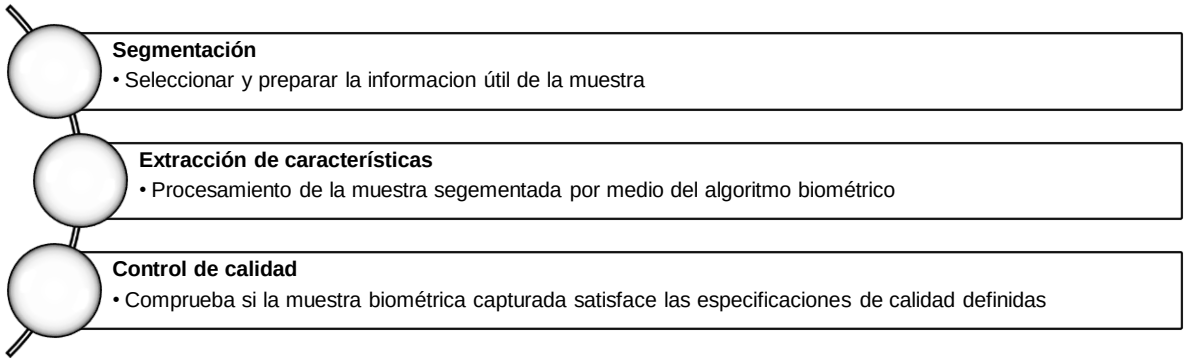
Figura 20. (Continuación)

Sistemas Biométricos de Reconocimiento	Patrón Biométrico
Facial	Imagen Facial
Firma	Imagen de firma y registro de medidas relacionadas con la dinámica
Geometría de la Mano	Imágenes 3D de la parte superior y lateral de manos y dedos.
Huella Dactilar	Imagen o minucia de la huella dactilar
Iris	Imagen del Iris
Sistemas Biométricos de Reconocimiento	**Patrón Biométrico**
Retina	Imagen de la Retina
Autenticación e Identificación	Patrón Biométrico
Sistemas Biométricos de Autenticación e Identificación	**Patrón Biométrico**
Voz	Grabación de voz

Fuente: Adaptada Estudio sobre las Tecnologías Biométricas aplicadas a la Seguridad Disponible en: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnologíasBiométricasASeguridad.pdf

7.2.2 Procesamiento. Este proceso genera un vector o plantilla de las características extraídas de la muestra biométrica y se realiza una vez se haya capturado la muestra, se ejecuta las siguientes fases relacionadas en la Figura 21. Cada sistema biométrico tiene unas características extraídas, las cuales se pueden apreciar en la Figura 22.

Figura 21. Fases realizadas en el procesamiento



Fuente: El Autor

Figura 22 Características Extraídas de los sistemas biométricos

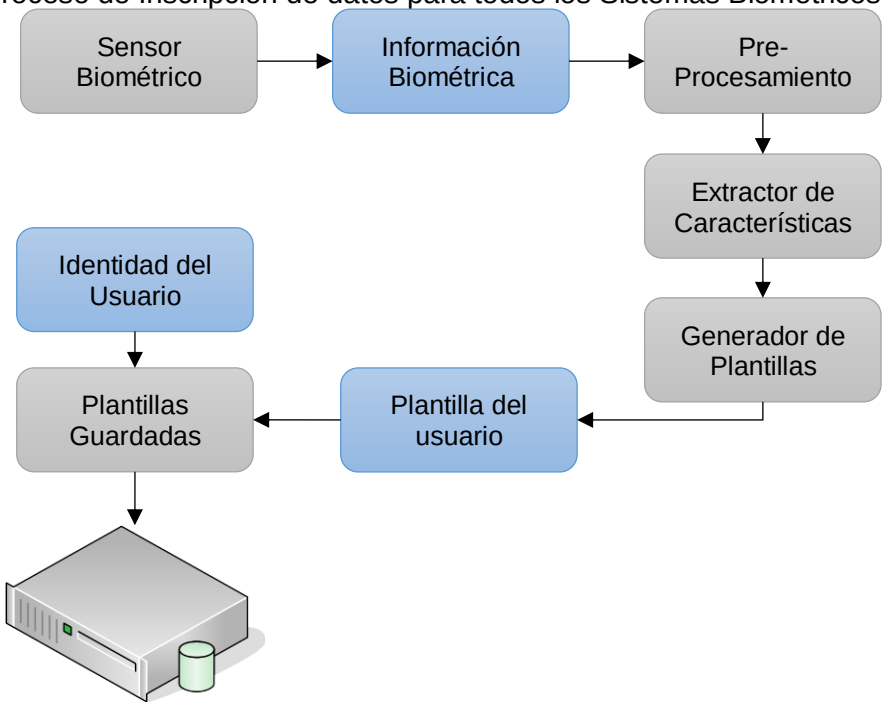
Sistemas Biométricos de Reconocimiento	Característica Extraída
Escritura de Teclado	Secuencia de teclas y pausa entre pulsaciones
Facial	Posición relativa y forma de la nariz, posición de la mandíbula.
Firma	Velocidad orden de los trazos, presión y apariencia de la firma.
Geometría de la Mano	Altura y anchura de los huesos y las articulaciones de los dedos de la mano.
Huella Dactilar	Ubicación y dirección del final de las minucias o formas de las huellas.
Iris	Surcos y estrías del Iris
Retina	Patrones de los vasos sanguíneos de la retina.
Autenticación e Identificación	Patrón Biométrico
Sistema Biométrico de Autenticación e Identificación	**Característica Extraída**
Voz	Frecuencia, cadencia y duración del patrón vocal

Fuente: Adaptada Estudio sobre las Tecnologías Biométricas aplicadas a la Seguridad Disponible en: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/

7.2.3 Inscripción. Es el primer paso en el proceso de reconocimiento, esta función genera una referencia biométrica para un usuario a partir del patrón biométrico seleccionado y así guardar la información para futuras comparaciones. En la siguiente Figura 23, se describe paso a paso la función de inscripción. El proceso de inscripción realiza los siguientes pasos:

- Recibe la muestra biométrica por medio del sensor
- Realiza el pre-procesamiento de los datos extrayendo el patrón de la muestra biométrica
- Genera un registro de datos como plantilla de usuario de la información capturada guardándola en un medio de almacenamiento adecuado

Figura 23. Proceso de Inscripción de datos para todos los Sistemas Biométricos



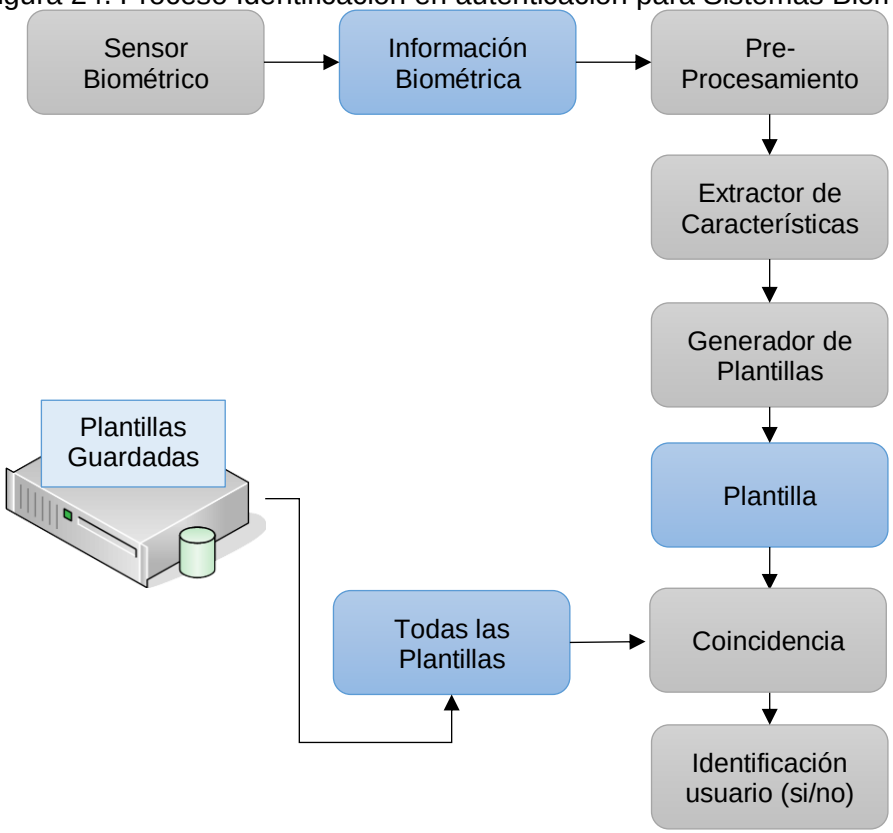
Fuente: Estudio sobre las tecnologías biométricas aplicadas a la seguridad, disponible en: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnologíasBiométricasASeguridad.pdf

7.3 AUTENTICACIÓN

Es la función biométrica que realiza el proceso de reconocimiento de las personas, mediante la captura de la muestra biométrica para compararla con la información biométrica de las plantillas ya registradas. Existen dos métodos para la autenticación:

7.3.1 Identificación. Proceso de reconocimiento de usuario en el que la muestra biométrica es comparada con todas las referencias de rasgos biométricos registradas previamente en la base de datos. Como se explica en la Figura 24, se utiliza un proceso de comparación de 1:N, genera como resultado una identificación correcta si el usuario ha sido incluido en la base de datos y una identificación incorrecta si el usuario no ha está registrado en la base de datos. La identificación tiene la siguiente clasificación:

Figura 24. Proceso Identificación en autenticación para Sistemas Biométricos



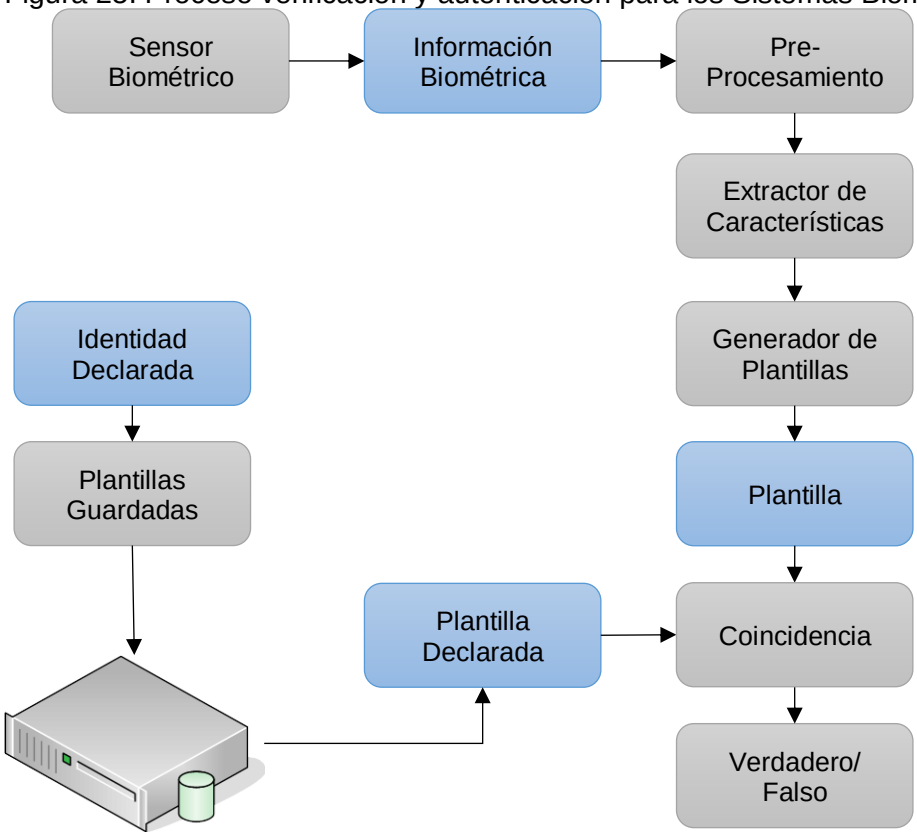
Fuente: Estudio sobre las tecnologías biométricas aplicadas a la seguridad, disponible en: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnologíasBiométricasASeguridad.pdf

7.3.1.1 Identificación abierta. Cualquier usuario puede utilizar el sistema biométrico, no hay restricción de uso.

7.3.1.2 Identificación cerrada. Grupo específico de usuarios que utilizan el sistema biométrico.

7.3.2 Verificación. Proceso de reconocimiento de usuario una vez realizada la identificación, como se puede apreciar en la Figura 25., el sistema biométrico compara la muestra biométrica obtenida con la referencia biométrica del usuario almacenada previamente en el proceso de inscripción. Es un proceso simple de comparación 1:1, genera como resultado una puntuación de similitud entre las muestras, que indican si el usuario es aceptado o rechazado.

Figura 25. Proceso verificación y autenticación para los Sistemas Biométricos

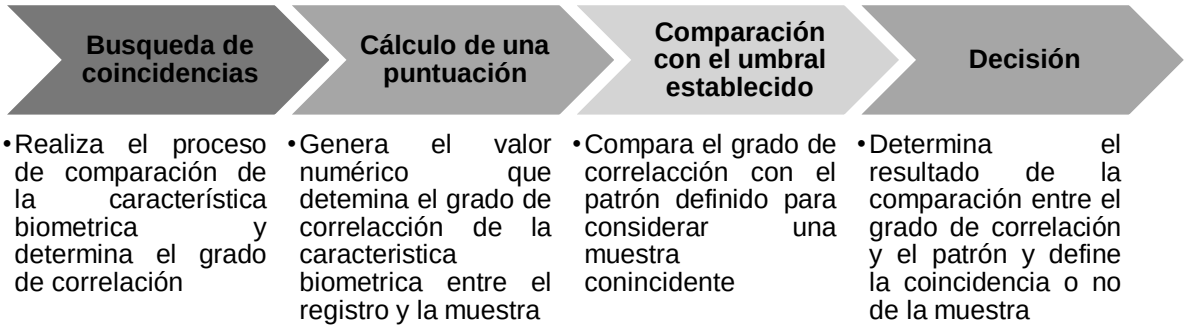


Fuente: Estudio sobre las tecnologías biométricas aplicadas a la seguridad, disponible en: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnologíasBiométricasASeguridad.pdf

7.4 TOMA DE DECISIONES

Está funcionalidad decide el resultado final del proceso de reconocimiento. Para los sistemas biométricos de verificación el resultado es la aceptación o rechazo del usuario y para los sistemas biométricos de identificación el resultado es una lista de candidatos para los cuales las referencias biométricas coinciden con la muestra biométrica. Para la toma de decisiones se contempla cuatro etapas que se describen en la Figura 26.

Figura 26. Etapas del proceso de decisión de los sistemas biométricos.

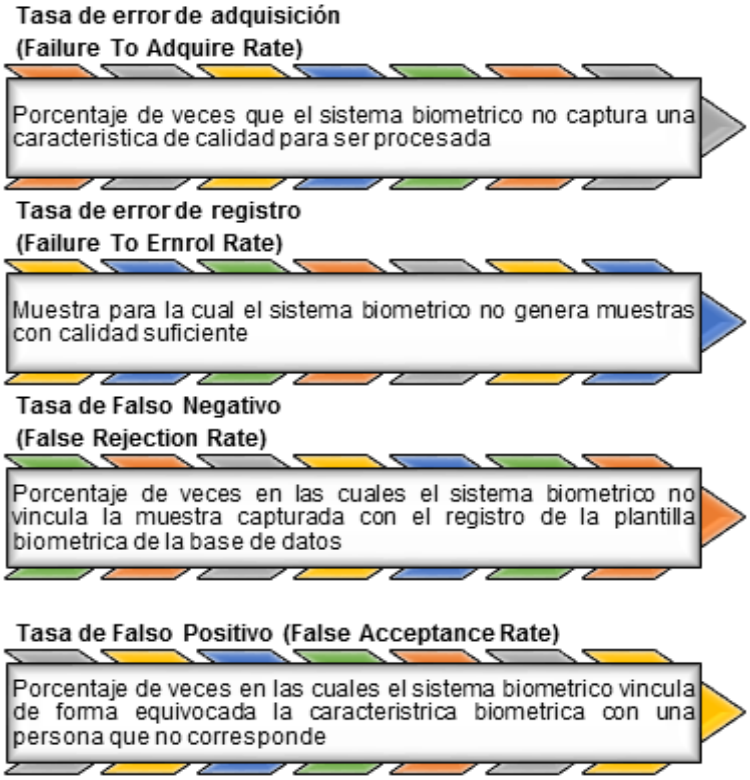


Fuente: El Autor

7.5 FUNCIONAMIENTO DEL SISTEMA

Los sistemas biométricos tienen su funcionamiento y fiabilidad valorados a través de una serie de tasas, que permite garantizar calidad en los datos capturados. En la Figura 27, se enuncian y se definen las tasas establecidas para lograr el funcionamiento del sistema biométrico.

Figura 27. Tasas de valoración de un sistema biométrico:



Fuente: El Autor

8. HERRAMIENTAS DE CONTROL DE ACCESO DE LOS SISTEMAS BIOMÉTRICOS

En la actualidad existe en el mercado muchos proveedores que suministran dispositivos de identificación biométrica para el control de acceso, con una gama de variedad de dispositivos con sensores de acuerdo a biometría de huella, facial, iris, voz, mano, estás pueden variar de acuerdo al proveedor.

Adicionalmente se encontró que las herramientas permiten la autenticación *offline* por decisión o en caso de perderse la comunicación y online dependiendo las necesidades de implantación. A continuación, mostraremos algunas opciones de herramientas de control de acceso. Las soluciones ofrecidas también incluyen el *software* compatible con el dispositivo biométrico, este cumple con funcionalidad estándar y en algunas opciones con algunas configuraciones especiales en el *software*, las cuales se adecuarán a cada tipo de necesidad.

8.1 SENSORES SEGÚN TIPO DE BIOMÉTRICO

Para ampliar la información relacionada con los tipos de sensores apropiados para cada tipo de sistema biométrico, a continuación, se exponen algunos ejemplos dentro de la gran variedad con la que hoy en día el mercado suple las necesidades de las organizaciones.

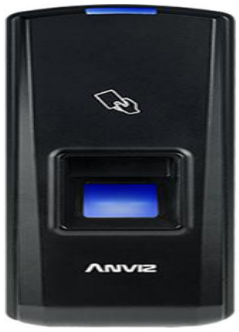
8.1.1 Sensores de Reconocimiento de Huella Dactilar. Existen muchos sensores de reconocimiento de huella dactilar en el mercado, y se adecúan de acuerdo a la necesidad del proyecto donde se requiera implementar, como se pude ver en la tabla 6, se realiza la descripción de algunos de los sensores disponibles.

Tabla 6. Sensores de Reconocimiento de Huella Digital

Representación gráfica FPC 1011F3	
	Sensor de huella basado en tecnología capacitiva. Cuenta con 256 valores en la escala de grises por cada pixel. Tiene resolución de 363 dpi y su funcionamiento consiste en enviar una señal eléctrica directamente hacia el dedo, determinará si hay espacio entre las crestas de la huella, delimitando su forma.[40]

[40] KIMALDI, Fabricante y Distribuidor de biométricos

Tabla 6. (Continuación)

Representación gráfica NB -3010-U	
	Sensor de huella basado en tecnología térmica para a captación de la huella. Tiene resolución de 385 dpi y cuenta con plantillas de 256 posiciones en escala de grises. Cuenta con un diseño ergonómico especialmente diseñado para uso de un computador personal con conexión por USB. Su comportamiento como sensor térmico permite captar la imagen mediante las variaciones de temperatura[41]
Representación gráfica de Biométrico T5-PRO	
 **http://www.isec.com.co/detalle-producto/t5-pro/[42]**	Sensor de huella basado en tecnología de zona sensible y genera una secuencia de imágenes las cuales son re-ensambladas por medio de un procesador convirtiéndola en una imagen completa. El T5 Pro es una Innovadora lectora de Tarjetas y Huellas Digitales, con control de acceso, que integra completamente tecnología RFID y lector de huella digital, en un dispositivo muy compacto el cual puede ser instalado en el marco de una puerta. [43]

Fuente: El Autor

8.1.2 Sensores de Reconocimiento del Iris. Existen muchos sensores de reconocimiento de reconocimiento del iris en el mercado, y se adecúan de acuerdo a la necesidad del proyecto donde se requiera implementar, como se pude ver en la tabla 7, se realiza la descripción de algunos de los sensores disponibles.

[41] KIMALDI, Fabricante y Distribuidor de biométricos
[42] ISEC, Biométricos
[43] ISEC, Op. Cit.

Tabla 7. Sensores de Reconocimiento del Iris

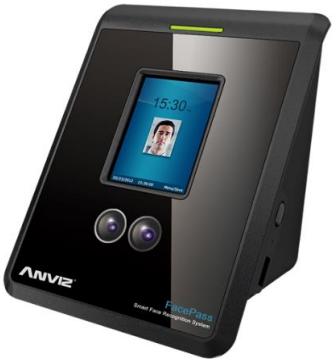
Representación gráfica IRIS PUNCH	
 **https://jaramillovillegas.co/irispunch.html#caracter[44]**	*Iris Punch* ® es la solución ideal para situaciones en las que se requiere una identificación biométrica rápida y confiable, teniendo un nivel de precisión superior a otras tecnologías de identificación biométrica, haciendo uso de la tecnología *Iritech, Inc*.[45]
Representación gráfica de Biométrico UltraMatch	
 **http://www.isec.com.co/[46]**	El *UltraMatch* posee un funcionamiento robusto y un elegante diseño. Con algoritmo BioNANO el sistema proporciona el reconocimiento de iris más preciso, estable y más rápido al tiempo que ofrece seguridad de alto nivel en inscripción biométrica, identificación y control de acceso. El reconocimiento de iris es la más precisa y más rápida opción para autenticar alguien con absoluta certeza. [47]

Fuente: El Autor

8.1.3 Sensores de Reconocimiento Facial. Existen muchos sensores de reconocimiento de reconocimiento facial en el mercado, y se adecúan de acuerdo a la necesidad del proyecto donde se requiera implementar, como se pude ver en la tabla 8, se realiza la descripción de algunos de los sensores disponibles.

[44] JARAMILLO & VILLEGAS, Artículos Biométricos
[45] JARAMILLO & VILLEGAS, Op. Cit.
[46] ISEC, Biométricos
[47] ISEC, Op. Cit.

Tabla 8. Sensores de reconocimiento facial

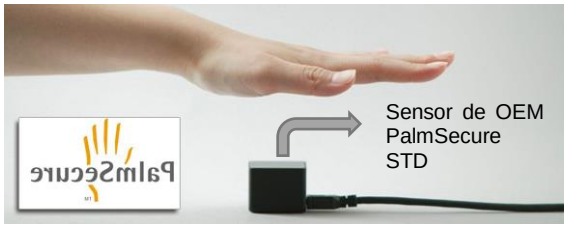
Representación gráfica de Biométrico *FacePass Pro*	
 **http://www.isec.com.co/**[48]	El terminal de reconocimiento facial Anviz *FacePass* Pro es un dispositivo de reconocimiento facial que incorpora el nuevo algoritmo núcleo BioNANO y una plataforma de *hardware* que garantiza la velocidad de identificación de menos de 1 segundo (1:300). Su diseño con luz infrarroja permite al terminal trabajar en las peores condiciones de iluminación. Este es un dispositivo seguro y apropiado para cualquier tipo de usuario independientemente de su piel, estilo de pelo o expresión facial. [49]
Representación gráfica de Biométrico Terminal Reconocimiento Facial 3D HANVON FACEID F710	
 **http://www.kimaldi.com/productos/sistemas_biometricos**[50]	La doble cámara permite un reconocimiento biométrico facial 3D de seguridad usando luz visible e infrarroja. Tecnología biométrica sin contacto segura y rápida. Tecnología 3D: La retícula de *leds* y la doble cámara (visible e infrarroja) permite capturar el patrón 3D de la fisonomía craneal. Altamente preciso: muy Baja tasa de error en la identificación. Funcionamiento Autónomo u *Offline* conectado a TCP/IP. Fácil de usar, de instalar y de integrar con librerías SDK. Tecnología ampliamente probada y de prestigio internacional.[51]

Fuente: El Autor

8.1.4. Sensores de Reconocimiento Geometría De Dedo Y Mano. Existen muchos sensores de reconocimiento de reconocimiento de geometría de dedo y mano en el mercado, y se adecúan de acuerdo a la necesidad del proyecto donde se requiera implementar, como se pude ver en la tabla 9, se realiza la descripción de algunos de los sensores disponibles.

[48] ISEC, Biométricos
[49] KIMALDI, Fabricante y Distribuidor de biométricos
[50] KIMALDI, Op. Cit.
[51] KIMALDI, Op. Cit.

Tabla 9. Sensores de Reconocimiento de Geometría dedo y mano

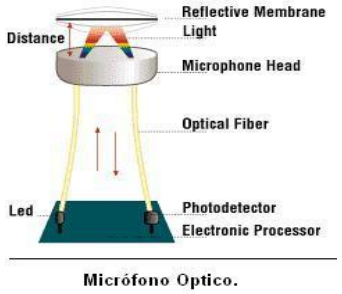
Handkey	
 **http://www.biosys.es/productos/handkey-ii/**[52]	Sistema de control de acceso integrado que concentra el sistema de información en su propio lector. Esta tecnología analiza y verifica el tamaño y la forma de la mano en un lapso de tiempo de un segundo. Utilizado para el control del acceso, es de bajo costo y el nivel de seguridad es alto. La comunicación se realiza a través de: RS232, RS422, RS485, módem y Ethernet. [53]
Sistema Palm Secure	
 **http://www.fujitsu.com/es/products/others/biometric/**[54]	Este sistema de autenticación es uno de los avances más significativos en soluciones de identificación biométrica. Esta tecnología captura la imagen del tramado de las venas de la palma de la mano mediante el reflejo de los rayos emitidos, generando el retrato de las venas como un patrón negro en la imagen capturada. Es considerada una solución idónea e higiénica para sistemas de identificación de múltiples usuarios. E usuario final solo debe poner la mano encima del escáner a una pequeña distancia y este realiza el proceso de autenticación. [55]

Fuente: El Autor

8.1.5. Sensores de Autenticación de La Voz. Existen muchos sensores de reconocimiento de reconocimiento de autenticación por voz en el mercado, y se adecúan de acuerdo a la necesidad del proyecto donde se requiera implementar, como se pude ver en la tabla 10, se realiza la descripción de algunos de los sensores disponibles.

[52] Biosys, Sistemas Biométricos
[53] Biosys, Op. Cit.
[54] FUJITSU, Biometría
[55] FUJITSU, Op. Cit.

Tabla 10. Sensores de Autenticación por voz

BatVoz	
	Herramienta avanzada que permite comparar voces y verificar la identidad de las mismas. Utiliza la 4ta generación del motor de biometría vocal de AGNITIO, logrando rapidez y precisión.
Micrófono Óptico Unidereccional	
 Micrófono Optico. **http://sistemasbiomet.blogspot.com.co/**	El micrófono utiliza la luz de diodo emitida en la membrana reflectora, cuando las ondas golpean la membrana vibra y la luz reflejada cambia sus características, se genera un foto-detector que registra la luz reflejada y obtiene las ondas de sonido.

Fuente: El Autor

8.1.6. Sensores de Reconocimiento de la Firma. Existen muchos sensores de reconocimiento de reconocimiento de reconocimiento de firma electrónica en el mercado, y se adecúan de acuerdo a la necesidad del proyecto donde se requiera implementar, como se pude ver en la tabla 11, se realiza la descripción de algunos de los sensores disponibles.

Tabla 11. Sensores de reconocimiento de firma electrónica.

STU 130	
 **https://www.google.com.co/search?q=STU-530&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiToPfN2srTAhVETCYKHbluCvAQ_AUICCgB&biw=1366&bih=662#imgrc=ZwEJG0S5KbgCGM:**	Dispositivo utilizado en los sistemas biométricos de reconocimiento de firma, que incluye cifrado AES de 256 bits e intercambio de claves RSA de 2048 bits. Diseñada para el manejo de un alto volumen de transacciones. Identifica de manera exacta el espacio utilizado para cada firma. El lápiz inalámbrico con el que cuenta esta Tablet genera un alto nivel de precisión en el trazado de la firma porque cuenta con 1024 niveles de sensibilidad.

Tabla 11 (Continuación)

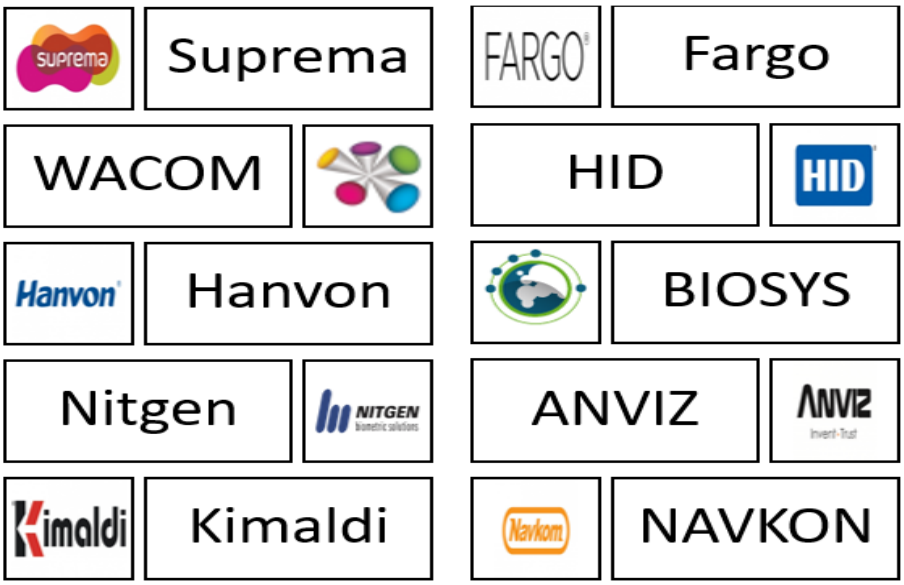
DTU 1031 X	
 **http://www.batemat.es/digitalizador-de-firmas-y-formularios-dtu-1031x**	Digitalizador de firmas y formularios, utilizado cifrado RSA/AES de última generación generando mayor seguridad a las transacciones realizadas. Es una solución integral que permite ver, completar y firmar documentos en tamaño real. Una de sus ventajas es el tamaño de su pantalla que da una mayor visibilidad del documento, otra ventaja es que solo tiene un cable USB que alimentar energía y datos.

Fuente: El Autor

8.2 FABRICANTES RECONOCIDOS DE SENSORES BIOMETRICOS

Existen diferentes tipos de fabricantes y distribuidores que ofrecen soluciones para todo tipo de necesidades, según los requerimientos de los usuarios que optan por implantar sistemas biométricos para el control de acceso. A continuación, se mencionan algunos de las opciones de los fabricantes y distribuidores de acuerdo a su especialidad, dentro de un grupo identificado que se puede observar en la Figura 28.

Figura 28. Fabricantes y Distribuidores de herramientas biométricas.



Fuente: El Autor

- Kimaldi. Es uno de los fabricantes mayoristas que cuentan con productos de sistemas biométricos reconocido en el mercado por ser proveedor de productos de alta calidad y precio, para implementar sistemas de identificación de personas, control de acceso, control de presencia, control de producción y trazabilidad de personas.
- Suprema. Empresa líder en proporcionar tecnologías para implementar sistemas biométricos, caracterizado por ofrecer aplicaciones de equipos y una integración con los sistemas de tecnología RFID también para el control de acceso y presencia.
- Nitgen. Fabricante de sensores de huella dactilar, lectores y sistemas biométricos. Nitgen es considerado líder mundial en tecnología y aplicaciones biométricas, especialista en soluciones con reconocimiento de huella dactilar.
- HANVON. Distribuidores y desarrolladores de sistemas y productos relacionados con el reconocimiento biométrico facial, como el Face ID.
- ANVIZ. HID Global desarrolla, fabrica y comercializa productos y servicios para soluciones de control de acceso y gestión de identificación.
- WACOM. Proveedor líder en dispositivos de reconocimiento de firma como las tabletas de firma electrónica y cuya mayor característica es la facilidad de uso.
- Biosys. Ofrece soluciones de seguridad en sistemas biométricos para control de acceso e integración de sistemas.

9. USABILIDAD Y SEGURIDAD EN LOS SISTEMAS BIOMETRICOS.

Existen diferentes variables sobre los usos de la biometría, pero todas tienen en común el grado de confianza que el sistema biométrico proporcionará un nivel de seguridad y que los resultados son correctos dentro de un nivel de tolerancia aceptable.

La implementación de un sistema biométrico debe considerar limitaciones operativas y de costos asociados, algunas de las restricciones operativas son: la política, la legislación, la integridad de los datos, la seguridad y la protección de la privacidad, la interoperabilidad con otros sistemas, las consideraciones ergonómicas, las condiciones ambientales dentro de muchos que se pueden presentar de acuerdo a las necesidades de los usuarios.

9.1 COMPARACIÓN DE LOS SISTEMAS BIOMÉTRICOS.

Para poder realizar una comparación de Usabilidad de los Sistemas Biométricos, se tendrá en cuenta la información recopilada de diferentes fuentes documentales, puesto que no existe mucha información confiable, comparable o reciente, pero si se identificarán los factores más relevantes con la finalidad de identificar potencialidades o limitaciones de cada uno de los sistemas biométricos como parte del desarrollo del presente trabajo de grado,

El funcionamiento de los biométricos puede ser influenciado directa o indirectamente por factores que afectan su rendimiento, estos factores se pueden dividir en 2 grupos, los que son inherentes al sensor empleado y los que se consideran ajenos a los sensores, que de igual forma alteran los resultados.[56]

9.1.1 Comparación de Factores Ambientales en Sistemas Biométricos. Algunos de los factores ambientales que afectan los sistemas biométricos se pueden observar en la Tabla 12 y su relación con el tipo de biométrico del caso de estudio.

[56] Tecnologías biométricas aplicadas a la ciberseguridad – Guía de aproximación para el empresario [online].

Tabla 12. Factores ambientales relacionados con los sistemas biométricos

Sistema Biométrico Factor Ambiental	Huella Dactilar	Iris	Facial	Mano	Voz
Luz	✓	✓	✓	✓	
Ruido					✓
Temperatura	✓			✓	
Ruido electromagnético	✓	✓	✓	✓	✓
Humedad	✓			✓	
Suciedad y contaminantes	✓	✓	✓	✓	
Variaciones del Voltaje	✓	✓	✓	✓	✓
Golpes y vibraciones	✓	✓	✓	✓	✓
Afectación	***7***	***5***	***5***	***7***	***4***

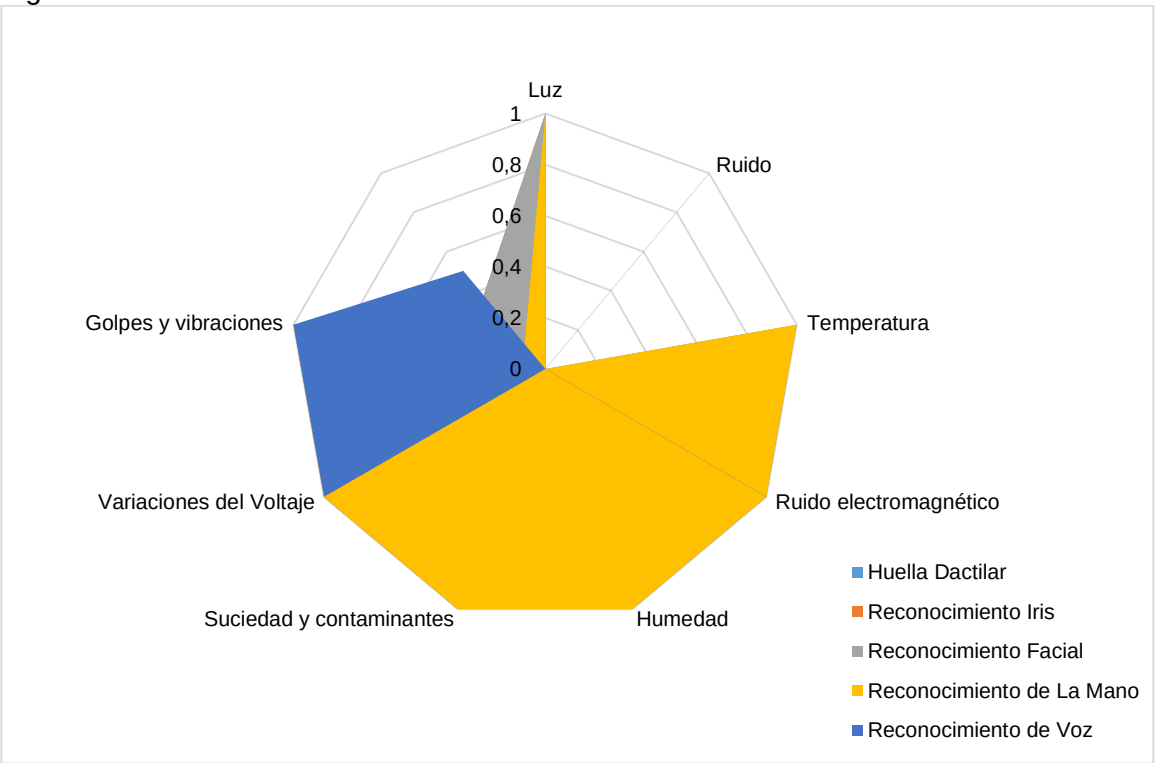
Fuente: Adaptada de Tecnologías biométricas aplicadas a la ciberseguridad. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

Una vez graficados los resultados de la Tabla 12 se puede ver que los factores ambientales inciden en gran medida en los sistemas biométricos de huella dactilar, como se observa en la Figura 29, la única condición que no afecta en su desarrollo es el ruido. Los factores ambientales tienen gran relevancia en el resultado generado por los sistemas biométricos, se observa en el análisis que hay un promedio de afectación visible para los sistemas biométricos seleccionados.

Los sistemas biométricos de Huella dactilar e Iris, son los más afectados por diversos factores ambientales, es necesario tener en cuenta como solventar dichas amenazas o vulnerabilidades antes de implementar este tipo de sistemas biométricos.

El reconocimiento facial y de mano, aunque está por encima de la media también se afecta por factores ambientales a menor escala, se deben tener en cuenta en la escalabilidad del sistema.

Figura 29. Influencia de los factores ambientales en los sistemas biométricos



Fuente: El Autor

La captura de los datos recogidos, almacenados, transmitidos y usados de un sistema biométrico deberían contemplar aspectos tales como:

- Integridad de las características biométricas
- Evaluación del entorno y los procedimientos de recolección de datos
- Niveles tolerables
- Tiempo medio de fallos
- Requisitos de mantenimiento razonables
- Garantizar la protección de la privacidad de los datos.

Los aspectos de seguridad en los sistemas biométricos se enfocan principalmente en la detección de fraudes, la suplantación y la seguridad de la información, es por esto, que todo sistema implementado debería contar con controles como la encriptación, el *hashing* de los datos. Es recomendable hacer uso de la versión actualizada de *Public Key Infraestructure* o PKI del estándar de la OACI.

9.1.2 Comparación de Propiedades en Sistemas Biométricos. Para la correcta identificación de los individuos, se debe tener en cuenta la compatibilidad de las características biométricas en cada tipo de sistema, las cuales se pueden observar en la Tabla N° 13 construida con base en diferente Estudios de Seguridad de los sistemas biométricos de identificación.

Tabla 13. Compatibilidad, propiedades y características sistemas biométricos.

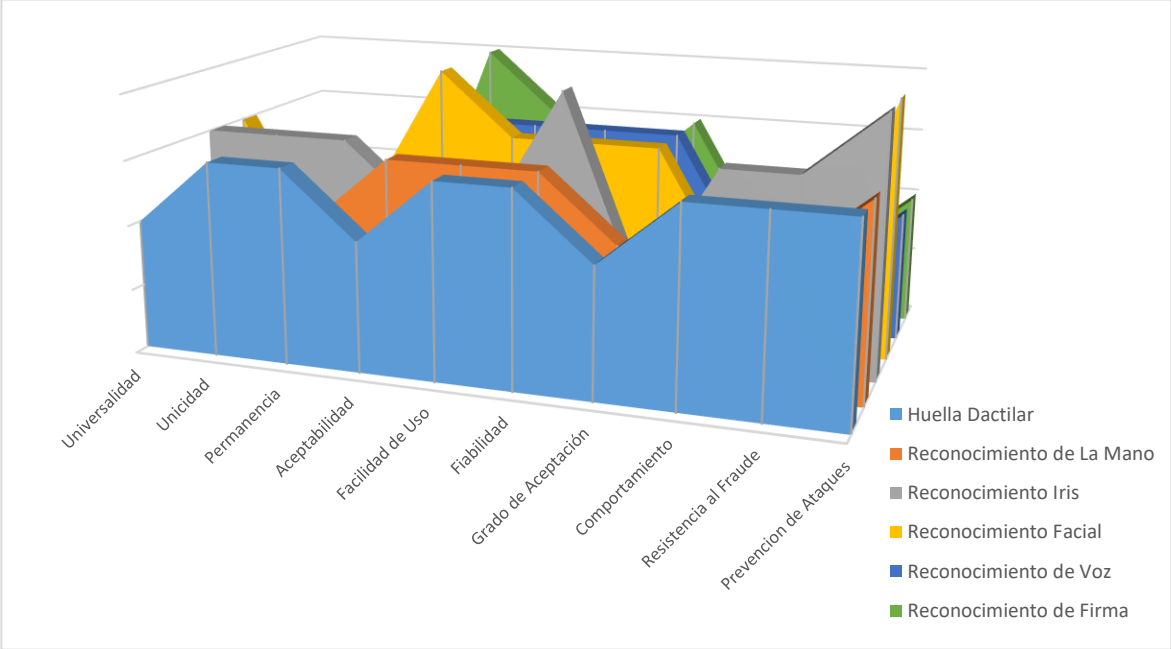
Sistema Biométrico	Universalidad	Unicidad	Permanencia	Aceptabilidad	Facilidad de Uso	Fiabilidad	Grado de Aceptación	Comportamiento	Resistencia al Fraude	Prevención de Ataques	% Efectividad
Huella Dactilar	2	3	3	2	3	3	2	3	3	3	**3**
Reconocimiento de La Mano	2	2	2	3	3	3	2	2	2	3	**2**
Reconocimiento Iris	3	3	3	2	2	4	1	3	3	4	**3**
Reconocimiento Facial	3	1	2	4	3	3	3	1	1	4	**3**
Reconocimiento de Voz	2	1	2	3	3	3	3	1	1	2	**2**
Reconocimiento de Firma	1	1	1	4	3	2	3	1	1	2	**2**

Fuente: El Autor

Se diseñó una valoración para identificar el nivel de compatibilidad de cada sistema biométrico, asignando una valoración para establecer una métrica de evaluación de las propiedades y características de los sistemas biométricos, donde 1 es el nivel menos compatible y 4 es el nivel más compatible con las propiedades y características de un sistema biométrico.

A continuación, en la Figura 30, se realizó la representación gráfica de los resultados obtenidos en la valoración de la compatibilidad de propiedades y características de los sistemas biométricos.

Figura 30. Compatibilidad de los Sistemas Biométricos.



Fuente: El Autor

Como se observa en la Figura 24, el sistema biométrico de Huella dactilar arrojó como resultado del análisis que está posicionado en el segundo lugar, con un nivel de compatibilidad del 68%, generando un alto nivel de aprobación por los usuarios y empresas que lo implementan.

También se puede evidenciar que el Sistema Biométrico de reconocimiento de iris tiene el más alto valor de compatibilidad con las características y propiedades de los sistemas biométricos en cuanto a su funcionalidad, aunque demuestra un valor muy bajo en aceptación.

9.1.3 Comparación de Algoritmo Biométrico en Sistemas Biométricos. En el proceso de verificación para determinar el nivel de similitud de la comparación de los patrones biométrico del individuo y la información de la plantilla almacenada en la base de datos, se requiere de un algoritmo biométrico de reconocimiento que evalúa los siguientes parámetros:

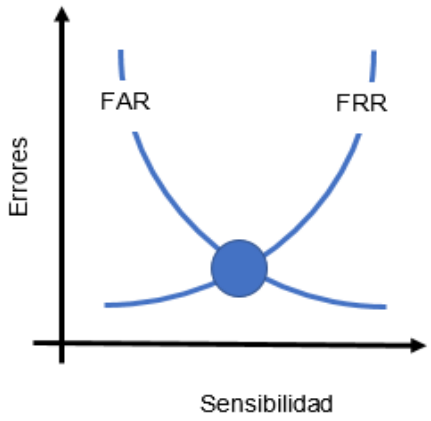
- FAR (*False Acceptance Rate*): Tasa de falso positivo, es la proporción de transacciones verdaderas que se deniegan incorrectamente.
- FRR (*False Rejection Rate*): Tasa de falso negativo, es la proporción de transacciones de impostor que se aceptan incorrectamente.

Además, los parámetros FAR y FRR tienen como función calcular:

- El número de intentos por transacción recibidos en el sistema biométrico.
- El umbral de calidad y de decisión del sistema biométrico.

En la tabla 14, se observa el nivel de precisión del algoritmo de verificación según el tipo de sistema biométrico.

Tabla 14. Nivel de precisión del algoritmo biométrico

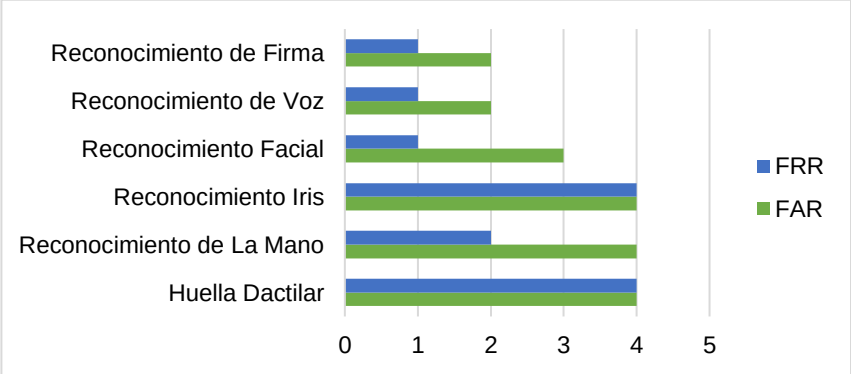


Sistema Biométrico	Precisión del Algoritmo Biométrico	
	FAR	FRR
Huella Dactilar	4	4
Reconocimiento de La Mano	4	2
Reconocimiento Iris	4	4
Reconocimiento Facial	3	1
Reconocimiento de Voz	2	1
Reconocimiento de Firma	2	1

Fuente: Ciclo de Conferencias UPM – TASSI Aplicaciones de la Biometría a la seguridad Disponible en: http://oa.upm.es/20071/

A continuación, en la Figura 31. Se realizó la representación gráfica con los resultados obtenidos de la valoración de la precisión del algoritmo biométrico.

Figura 31Precisión del algoritmo biométrico.



Fuente: El autor

En el resultado del análisis de la representación gráfica se puede observar que el sistema biométrico de huella e iris, obtuvo una puntuación de 4 (cuatro) en FRR y FAR, donde 1 es el nivel menos preciso y 4 es el nivel más preciso frente algoritmo de precisión de un sistema biométrico. Una tasa de error de usuarios erróneamente rechazados o aceptados en el proceso de verificación es el de Huella Dactilar, razón que corresponde a las características de sistema biométrico estático y a su patrón biométrico.

El sistema biométrico con menor tasa de error es la firma, se puede analizar que su FRR es menor, es decir, que la probabilidad de aceptar un impostor como usuario válido es mínima en este sistema biométrico, aunque la posibilidad de rechazo de un usuario válido es mayor, este sistema tiene el nivel de error más bajo.

9.2 CARACTERÍSTICAS DE USO Y SEGURIDAD EN LOS SISTEMAS BIOMÉTRICOS

A continuación, se relacionan las características de uso y seguridad que fueron evaluadas, manteniendo relación con las condiciones de seguridad de los sistemas biométricos, como se observa en la Tabla 15.

Tabla 15. Compatibilidad de beneficios de los sistemas biométricas.

Características	**Beneficios**
Necesidad de Secreto	No usa esta opción, solo se depende del usuario
Posibilidad de Robo	Los rasgos biométricos pertenecen a la persona
Posibilidad de pérdida	Los rasgos biométricos pertenecen a la persona
Registro inicial y posibilidad de generación.	Requiere la presencia del individuo
Características	Beneficios
Proceso de comparación	Se requiere tener infraestructura con capacidad pertinente.
Comodidad del usuario	No se requiere esfuerzo
Vulnerabilidad ante el espionaje	El espionaje no permite identificar información para acceder
Vulnerabilidad a un ataque por fuerza bruta	Una muestra biométrica contiene cientos de bytes, lo que dificulta facilitar un ataque de fuerza bruta.
Medidas de prevención	No cuenta con medidas de prevención con la madurez requerida
Autenticación de Usuarios Reales	La autenticación de los individuos no puede ser prestada, ni compartida

Tabla 21 (Continuación)

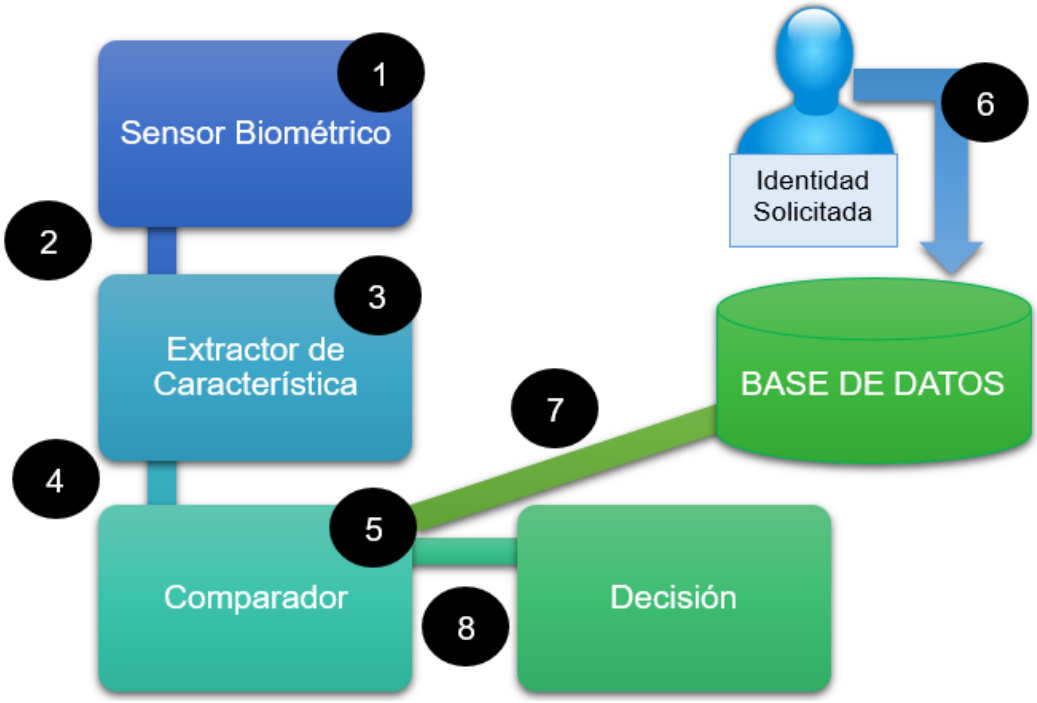
Características	Beneficios
Coste de implantación	Un sistema de biometría requiere costos más elevados
Coste de Mantenimiento	No genera gastos asociados a la pérdida u olvido de credenciales.

Fuente: Adaptada de Tecnologías biométricas aplicadas a la ciberseguridad. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

9.3 ASPECTOS DE SEGURIDAD DE LOS SISTEMAS BIOMÉTRICOS

Para evaluar aspectos de seguridad de los sistemas biométricos se identificaron algunas amenazas, vulnerabilidades y ataques en algunos puntos estratégicos en el flujo de la técnica de reconocimiento de los biométricos, como podemos ver en la Figura 32 se tuvieron identificaron puntos vulnerables como el sensor, la extracción de características, el comparador, la base de datos, la identidad solicitada y la decisión.

Figura 32. Vulnerabilidades en puntos estratégicos técnica de reconocimiento



Fuente: Adaptado de Seguridad e inseguridad en los sistemas biométricos: seguridad vs privacidad. http://oa.upm.es/43786/

9.3.1 Vulnerabilidades y medidas defensivas. Los sistemas biométricos tienen ciertas ventajas las cuales se vieron en los capítulos anteriores, pero además tienen unas limitaciones que pueden comprometer la seguridad por medio de ataques que pueden materializarse cuando son objeto de amenazas.

Para evaluar fueron considerados los puntos estratégicos observados en la figura 32, y los canales que intercambian el flujo de información entre los diferentes puntos, se realizó la verificación de dispositivos físicos con técnicas para generar datos biométricos falsos y los canales de comunicación, los cuales están expuestos a técnicas de ataque de captura o de inyección de paquetes en el canal de comunicación.

Para reducir la posibilidad de explotación de las vulnerabilidades en las diferentes etapas de las técnicas de reconocimiento, se realizó la sugerencia de algunas medidas defensivas las cuales serán descritas en la tabla 16 para disminuir los ataques que podrían alterar el funcionamiento correcto de un sistema biométrico.

Tabla 16. Vulnerabilidades y medidas defensivas de etapas de reconocimiento.

Pto	Nombre	Tipo	Descripción Ataque	Medidas Defensivas
1	Sensor	Dispositivo Físico	Ataque al sistema con características biométricas falsas al sensor	-Los sensores cuentan con detección del tejido vivo. -Autenticación multifactor. Implementar otro mecanismo de identificación. -Uso de tecnología de calidad, para evitar capturas erróneas.
2 **4** **7** **8**	Comunicación	Canal de Comunicación	Interceptación de canal para capturar paquetes con los patrones biométricos legítimos y generar pérdida de la integridad. Utilizar los datos de patrones biométricos para atacar otros sistemas biométricos Suplantación de Identidad.	-Cifrado de las comunicaciones. -Encripción y cifrado de los datos transmitidos, para evitar el análisis y la interpretación de paquetes por parte de un intruso. -Firma digital para validar que la transmisión de la información, sea del emisor correspondiente.
2	Comunicación	Canal de Comunicación	Ataque por repetición, reenvío de rasgos biométricos	-Cifrado de las comunicaciones

Tabla 16 (Continuación)

Pto	Nombre	Tipo	Descripción Ataque	Medidas Defensivas
4	Extracción del vector de características	Canal de Comunicación	Modificación de información, reemplazando el vector por uno nuevo. Ataques de suplantación *Spoofing* Ataque de *Hill climbing* (Acceso de colina) que consiste en modificar de forma iterativa, la puntuación de los parámetros biométricos, hasta que el módulo comparador devuelva un resultado favorable.	-Borrado de memorias temporales a bajo nivel, para evitar almacenar información de los patrones biométricos.
7	Plantillas de los Usuarios	Canal de Comunicación	Interceptación en el canal de comunicación para obtener las plantillas de los usuarios registrados en la base de datos.	-Cifrado de las comunicaciones -Encripción y cifrado de los datos transmitidos, para evitar el análisis y la interpretación de paquetes por parte de un intruso.
8	Decisión Final	Dispositivo Físico	Modificación de la información del resultado de la decisión final, permitiendo dar acceso a usuarios ilegítimos o denegando acceso a usuarios legítimos-	-Implementación de Políticas de restricción de Equipos. -Control de Acceso a modificación de las plantillas
3	Extracción del vector de características	Dispositivo Físico	Modificación de información, reemplazando el vector de características, por medio de la instalación de un troyano, el cual deja abierta la puerta trasera al intruso para que el atacante manipule la información. Ataques por ofuscación de datos biométricos, que consiste en impedir la identificación correcta del individuo, enmascarando los datos.	-Sistemas de detección de Intrusos IDS para la protección en bloques. -Control de instalación de Software

Tabla 16 (Continuación)

Pto	Nombre	Tipo	Descripción Ataque	Medidas Defensivas
5	Comparador	Dispositivo físico	Modificación de información, reemplazando el vector de características, por medio de la instalación de un troyano, el cual deja abierta la puerta trasera al intruso para que el atacante manipule la información. Corrupción del algoritmo de comparación para engañar y generar un falso positivo.	-Implementación de Políticas de restricción de Equipos. -Restricción de instalación de software -Controles de acceso lógicos del algoritmo de cifrado.
6	Base de Datos	Dispositivo Físico	Modificación de plantillas para suplantar usuarios legítimos. Ataques de inyección de código a la base de datos. Ataques de denegación del servicio, por medio de la inyección de grandes cantidades de biométricos, para desestabilizar la base de datos.	-Control de Accesos no autorizados, por medio de procedimiento de gestión de usuarios. -Implementación de un *Firewall* de Base de Datos -Controles de seguridad IDS/IPS

Fuente: El Autor

9.3.2 Otros Aspectos de Seguridad. Los sistemas biométricos tienen ciertas ventajas las cuales se vieron en los capítulos anteriores, pero además tienen unas limitaciones que pueden comprometer la seguridad por medio de ataques que pueden materializarse cuando son objeto de amenazas.

Adicionalmente a los aspectos evaluados anteriormente, es de gran importancia en la seguridad de un sistema biométrico, cumplir con los requisitos de seguridad como la confidencialidad, la integridad, la autenticidad, no repudio, y la disponibilidad.[57]

9.3.2.1 La Autenticidad. Un sistema biométrico cuenta con dos autenticidades una de entidad, la cual se encarga de la validación de las entidades en el procesamiento “son las que dicen ser”. Y la de origen de datos, que se encarga de validar la originalidad de los datos.

[57] W3II. Biométrico de Seguridad de Sistemas [online].

9.3.2.2 La confidencialidad. Un sistema biométrico debe limitar el acceso y divulgación de información para quienes estén autorizados, y que mantiene el secreto de la información de autenticación biométrica a entidades no autorizadas.

9.3.2.3 No Repudio. Un sistema biométrico cuenta con rendición de cuentas y así permite garantizar la validez del emisor y receptor en la comunicación de la información biométrica.

9.3.2.3 La Integridad. Un sistema biométrico cuenta con la precisión, la consistencia, la exactitud y la integridad, que son características primordiales para evitar manipulaciones intencionales y no intencionales de la información biométrica.

9.3.3 Seguridad en los sistemas biométricos. Según el VIII Ciclo de la Conferencia de Aplicación de la Biometría en la seguridad, muestra una valoración sobre la seguridad de cada tipo de sistema biométrico, como se evidencia en la Tabla 17.

Tabla 17. Nivel de seguridad de los sistemas biométricos.

Sistema Biométrico	Nivel de Seguridad
Huella Dactilar	**A**
Geometría de La Mano	**M**
Reconocimiento Iris	**A**
Reconocimiento Facial	**M**
Reconocimiento de Voz	**M**
Reconocimiento de Firma	**M**

Fuente: Ciclo de Conferencias UPM – TASSI Aplicaciones de la Biometría a la seguridad Disponible en: http://oa.upm.es/20071/

9.3.4 Incidentes de Seguridad de Sistemas Biométricos. La implementación de soluciones para el control de acceso de sistemas biométricos, ha contribuido en la disminución de la materialización de riesgos asociados al control de acceso de los usuarios y el cierre de brechas de seguridad relacionadas, la implementación de soluciones de identificación biométrica, como se puede apreciar en la tabla 18 a continuación:

Tabla 18. Disminución de incidentes de seguridad.

Concepto	Descripción
Comodidad y facilidad de acceso:	Ha disminuido los incidentes de control de acceso causados por riesgos de administración de claves por parte de usuarios y administradores, garantizando los accesos seguros a la información y la disminución de ataques.
Precisión:	Ha disminuido los incidentes de control de acceso causados por engaños en la verificación de la identidad incorporando sensores de calor, incrementando el nivel de seguridad en la identificación de las personas, generando mayor aceptación.
Optimización de la gestión:	Ha permitido optimizar los recursos de administración disminuyendo riesgos de asignación de cuentas de usuarios.
Seguridad integral:	Disminución de perdida de confidencialidad o robo de contraseñas de acceso.
Versatilidad:	Ha permitido establecer combinaciones de diferentes mecanismos biométricos generando mayor seguridad integrando mecanismos tradicionales de autenticación dura elevando los niveles de seguridad

Fuente: Adaptado de: Cinco razones para implementar la identificación biométrica. Disponible en: https://colombiadigital.net/actualidad/articulos-informativos/item/8802-cinco-razones-para-implementar-la-identificacion-biometrica.html

10. BENCHMARKING DE SEGURIDAD EN BIOMETRICOS

En este capítulo se hizo la comparación de los parámetros de los sistemas biométricos seleccionaos, para mostrar las diferencias entre cada sistema y generar así una guía de consulta que permita determinar qué sistema biométrico pueden ser aplicados de acuerdo a sus necesidades y requerimientos.

El análisis de resultados de los parámetros seleccionados en el capítulo 9 “Usabilidad y Seguridad en los Sistemas Biométricos”, se estableció el proceso de evaluación el cual consiste en asignar una valoración y calificación de los sistemas biométricos de reconocimiento de Huella Dactilar, Iris, Facial. Mano y Voz, con el objetivo de cuantificar y analizar resultados.

10.1 PARAMETROS DE BENCHMARKING DE SEGURIDAD EN BIOMETRICOS

El análisis de la información se realizó con una escala de calificación de 1 a 5 para cada parámetro, y cada característica tiene una valoración distinta de acuerdo al nivel de importancia en el sistema biométrico. En la tabla 19, se describen los parámetros establecidos para realizar el análisis del benchmarking, para los sistemas biométricos:

Tabla 19. Parámetros de Benchmarking Sistemas Biométricos

Parámetro	Descripción	Evaluación
Factores ambientales	Este ítem evalúa la influencia de los factores ambientales inherentes que afectan a los sistemas biométricos	La valoración de estos parámetros se mide por el grado de afectación a cada sistema biométrico
Propiedades y Características	Este ítem evalúa la información de las propiedades y características ajenas a los sistemas biométricos	La valoración de este parámetro se mide por el nivel de efectividad en cada sistema biométrico
Algoritmo Biométrico	Este ítem hace referencia a la probabilidad de falso positivo (FAR) y de falso negativo (FRR) del algoritmo de un sistema biométrico	La valoración de este parámetro mide el nivel de precisión en el proceso de verificación de un usuario en un sistema biométrico
Seguridad	Este ítem sea ha considerado un parámetro con alto grado de ponderación. Hace referencia a la seguridad del sistema biométrico	La valoración de este parámetro mide el nivel de seguridad de los puntos estratégicos en la técnica de reconocimiento

Fuente: El autor

10.2 DEFINICION DE VALORACIÓN DE LOS PARAMETROS BIOMETRICOS

La valoración aplicada en el Benchmarking se estableció por medio de unas escalas de valoración para cada parámetro, lo que permitió definir el alcance de cada nivel, de acuerdo la información vista en los capítulos anteriores, producto de la investigación de estudios recientes sobre seguridad en sistemas biométricos.

10.1.1 Factores ambientales: La valoración de los factores ambientales, está estimada de acuerdo a la valoración otorgada en la Tabla 20.

Tabla 20. Valoración de factores ambientales

Nivel	Descripción	Ponderación
A	Nivel de afectación Alto	=> 7
M	Nivel de afectación Medio	=< 6
B	Nivel de afectación Bajo	=< 3

Fuente: El autor

10.1.2 Propiedades y Características: La valoración de las propiedades y características, está estimada de acuerdo a la valoración otorgada en la Tabla 21.

Tabla 21. Valoración propiedades y características

Nivel	Descripción	Ponderación
D	Nivel de efectividad Deficiente	1% a 24%
B	Nivel de efectividad Bajo	25% a 49%
M	Nivel de efectividad Medio	50% a 74%
A	Nivel de efectividad Alto	75% al 100%

Fuente: El autor

10.1.3 Precisión del algoritmo biométrico: La valoración de la precisión del algoritmo biométrico, está estimada de acuerdo a la valoración otorgada en la Tabla 22.

- FAR: Indica la probabilidad de aceptación de un intruso como usuario válido del sistema.
- FRR: Indica la probabilidad de rechazo de un usuario válido del Sistema.

Tabla 22. Valoración precisión algoritmo biométrico

Nivel	Descripción	Ponderación
D	Nivel de precisión Deficiente	1
B	Nivel de precisión Bajo	2
M	Nivel de precisión Medio	3
A	Nivel de precisión Alto	4

Fuente: El autor

10.1.4 Nivel de Seguridad: La valoración de nivel de seguridad, está estimada de acuerdo a la valoración otorgada en la Tabla 23.

Tabla 23. Valoración nivel de seguridad

Nivel	Descripción	Ponderación
D	Nivel de seguridad Deficiente	1
B	Nivel de seguridad Bajo	2
M	Nivel de seguridad Medio	3
A	Nivel de seguridad Alto	4

Fuente: El autor

10.3 RESULTADO DEL BENCHMARKIG DE SEGURIDAD EN SISTEMAS BIOMÉTRICOS

La estrategia aplicada en el benchmarking es un proceso de comparación de los parámetros definidos, su descripción y su valoración para cada uno de los sistemas biométricos de reconocimiento e identificación: la huella dactilar, el iris, facial, la mano, la firma y la voz, permitiendo construir una propuesta de evaluación de los sistemas biométricos.

Este proceso de benchmarking contempla dos partes: la primera parte describe los parámetros definidos en la evaluación, la correspondiente descripción y su valoración; la segunda parte establece la calificación con una ponderación de acuerdo a la importancia de cada uno de los aspectos de seguridad que requieren los sistemas biométricos frente a las características de usabilidad, la funcionalidad y la seguridad.

La valoración para cada parámetro, está definida en tres niveles B (bajo), M (medio) y A (alto), con la finalidad de evaluar la influencia del parámetro en el sistema biométrico, así como fueron establecidos unos rangos de ponderación, dándole

mayor puntuación a los parámetros más relevantes en la evaluación, como se puede observar en a Tabla 24.

Tabla 24. Valoración Parámetro.

Nivel	Descripción	Ponderación
B	El parámetro no influye de manera significativa en la evaluación.	0% a 14.99%
M	El parámetro influye en cierta medida en la evaluación	15% a 29,99%
A	El parámetro es vital importancia en la evaluación.	30% a 100%

Fuente: El autor

A continuación, se encuentra en la Tabla 25. Se observa el resultado de valoración de los parámetros definidos en la evaluación de los sistemas biométricos.

Tabla 25. Parámetros y Ponderación para comparación por Sistema Biométrico

Parámetro	Valoración	Ponderación	Huella Dactilar	Iris	Facial	Mano	Voz	Firma
Factores Ambientales	Media	15%	A	M	M	A	M	N/A
Propiedades y Características	Media	15%	M	M	M	M	M	B
Precisión del Algoritmo Biométrico	Alta	30%	A	A	B	M	B	B
Nivel de Seguridad	Alta	40%	A	A	M	M	M	M

Fuente: El autor

Tabla 26. Valoración del Benchmarking

Escala	Calificación	Valoración
Desfavorable	El nivel de madurez de los parámetros es bajo, dentro del grupo de biométricos de identificación de patrones de reconocimiento y autenticación.	>=0 a <0.99
Medianamente Favorable	El nivel de madurez de los parámetros es Medio, dentro del grupo de biométricos de identificación de patrones de reconocimiento y autenticación.	>=1 a <2.99
Favorable	El nivel de madurez de los parámetros es Alto, dentro del grupo de biométricos de identificación de patrones de reconocimiento y autenticación.	>=3 a <3.99
Muy Favorable	El nivel de madurez de los parámetros es Muy Alto, dentro del grupo de biométricos de identificación de patrones de reconocimiento y autenticación.	>= 4

Fuente: El autor

Se realizó la asignación de la valoración del benchmarking por medio de la evaluación de los parámetros determinados en el numeral 10.2 Definición de la valoración de seguridad en sistemas biométricos.

El resultado del *Bechmarkig* en sistemas biométricos de reconocimiento y autenticación, es una herramienta que nos permite identificar y seleccionar el sistema biométrico más favorable para implementar el control de acceso, como se puede apreciar en la Tabla 27.

El resultado determino que el sistema biométrico de reconocimiento por huella dactilar es más favorable, el cual arrojo una puntuación de 4.30 de una valoración total de 5 (El nivel de madurez de los parámetros es Muy Alto, dentro del grupo de biométricos de identificación de patrones de reconocimiento y autenticación), destacándose parámetros como: precisión del algoritmo y niveles de seguridad. El sistema biométrico de reconocimiento del iris, toma la segunda posición que cuenta con una diferencia de 0.33%, la cual destaca los mismos parámetros que el de huella dactilar.

Para completar el proceso de decisión final de la evaluación, se procede a realizar la valoración del Benchmarking de los sistemas biométricos, de acuerdo a los parámetros y la ponderación de cada sistema biométrico por medio de una calificación nominal, la cual está definida, como se observa en la Tabla 27.

$$Calificación\ nominal\ (CN) = Valoración\ del\ Parametro(C) * La\ Ponderación(P)$$
$$CN = C * P$$

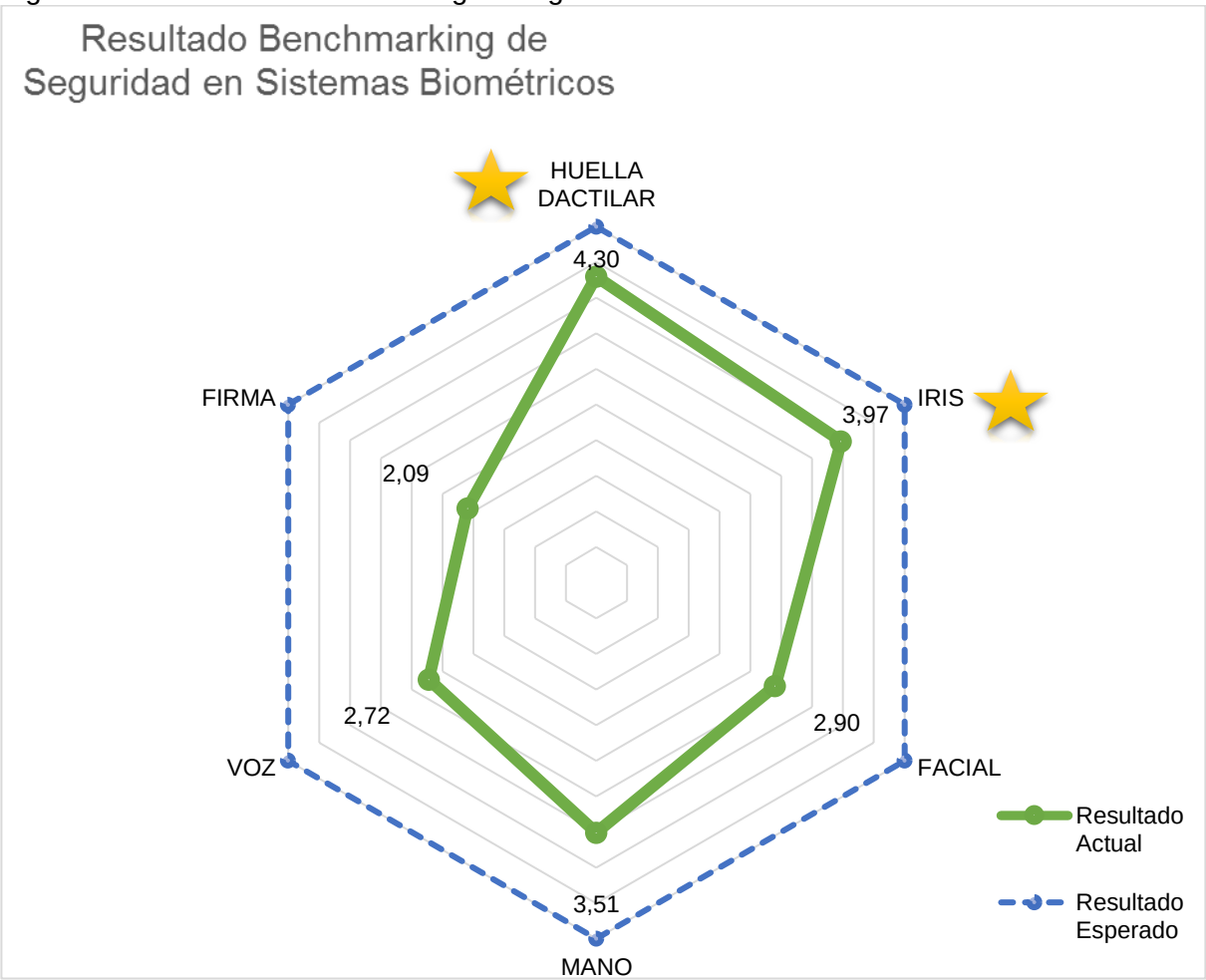
Tabla 27. Resultado Benchmarking Sistemas Biométricos

PARAMETRO		Factores Ambientales	Propiedades Características	Precisión Algoritmo Biométrico	Nivel de Seguridad	Total	Valoración Benchmarking
PONDERACION (P)		15%	15%	30%	40%	100%	
HUELLA DACTILAR	C	7	2,7	4	4	**4,3**	**Muy Favorable**
	CN	1,05	0,41	1,2	1,6		
IRIS	C	5	2,8	4	4	**3,97**	**Favorable**
	CN	0,75	0,42	1,2	1,6		
FACIAL	C	5	2,5	2	3	**2,90**	**Medianamente Favorable**
	CN	0,75	0,38	0,6	1,2		
MANO	C	7	2,4	3	3	**3,51**	**Favorable**
	CN	1,05	0,36	0,9	1,2		
VOZ	C	4	2,1	2	3	**2,72**	**Medianamente Favorable**
	CN	0,6	0,32	0,6	1,2		
FIRMA	C	0	1,9	2	3	**2,09**	**Medianamente Favorable**
	CN	0	0,29	0,6	1,2		

Fuente: El Autor

En la figura 33, se presentan lo reultado obtenidos, dondde se puede evidenciar la brecha que posee cada uno de los sistemas biométricos que fueron objeto del alcance del presente proyecto.

Figura 33. Resultado Benchmarking de seguridad en sistemas biométricos.



Fuente: El Autor

CONCLUSIONES

El auge y la necesidad de mejorar la seguridad en los sistemas de control de acceso e identificación, ha generado que hoy en día los sistemas tradicionales sean sustituidos por sistemas automáticos de reconocimiento e identificación biométrica, los cuales permiten responder más eficazmente a un entorno tecnológico creciente.

A lo largo del documento se muestra una visión general de los sistemas biométricos, desde los antecedentes hasta tendencias futuras y conceptos fundamentales sobre: como están clasificados los sistemas biométricos, factores ambientales, propiedades y características y la comparación del algoritmo de precisión y la influencia en cada sistema biométrico, aspectos que se deben contemplar para la implementación de un sistema biométrico de acuerdo a las necesidades.

Uno de los aspectos más destacados en el presente trabajo son una serie de amenazas y vulnerabilidades a los que están expuestos los componentes de un sistema biométrico, que pueden ser previsto teniendo en cuenta el uso de estándares definidos por varias organizaciones a nivel mundial y unas recomendaciones relacionadas en el flujo del sistema, sin dejar a un lado las implicaciones legales que pueden incurrirse en caso de no cumplir con las disposiciones dispuestas.

La recopilación de información nos permitió establecer un análisis por medio de un Bechmarking de los sistemas biométricos, donde fueron establecidos unos parámetros que fueron identificados como los más relevantes en el presente proyecto y unas escalas de valoración de acuerdo a la relevancia de cada parámetro.

Finalmente, al realizar está proyecto fue posible identificar que los sistemas biométricos de reconocimiento y autenticación con mayor valoración en el Bechmarking, es decir los más favorables según la evaluación son: el de reconocimiento de huella dactilar, iris y el facial. Durante todo el proceso comparativo estos tres sistemas biométricos son los que marcan la diferencia y los que tienen mayor porcentaje de en la comparación de los parámetros seleccionados, factores ambientales, propiedades y características, algoritmo biométrico y seguridad

BIBLIOGRAFÍA

AWARE. Biometrics Software [online]. Disponible en: https://www.aware.com/es/que-es-la-biometria/seguridad/

BATEMAT. Digitalizador de firmas y formularios DTU-1031X [online]. Disponible en: http://www.batemat.es/digitalizador-de-firmas-y-formularios-dtu-1031x

BENEDETO, Alvez., Identificación de personas mediante Sistemas Biométricos. Estudio de factibilidad y su implementación en organismos Estatales [online]. Disponible en: http://pcient.uner.edu.ar/index.php/Scdyt/article/view/7

BHALCHANDRA, A. S.; DESHPANDE, N. M. y PANTAWANE, N. G. Iris Recognition [online]. Diciembre, 2008. p. 1073-1078. Disponible en: http://connection.ebscohost.com/c/articles/65534673/efficient-speech-based-random-number-generators

BIOMETRIA. Métodos Biométricos de Reconocimiento de Huella Dactilar [online]. 2016. Disponible en: https://www.nist.gov/programs-projects/biometrics

BIOSYS. HandKey II [online]. Disponible en: http://www.biosys.es/productos/handkey-ii/

BORJA, Cesar. Sistemas Biométricos [online]. Disponible en: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

BOUIHROUZAN BELHAJ, Omar. Seguridad e inseguridad en los sistemas biométricos: seguridad vs privacidad [online]. Proyecto Fin de Carrera / Trabajo Fin de Grado, E.T.S.I. y Sistemas de Telecomunicación (UPM) [online]. Madrid 2016. Disponible en: http://oa.upm.es/43786/

CARRASCO OCHOA, Jesús Ariel. Reconocimiento de Patrones [online]. Disponible en: https://ccc.inaoep.mx/~ariel/recpat.pdf reconocimiento de patrones

CBEFF, Common Biometric Exchange File Format [online]. Disponible en ingles en: https://www.ibia.org/cbeff/biometric-identifier-overview

CONGRESO DE COLOMBIA. Ley Estatutaria 1581 de 2012 [online]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

CORTES OSORIO, Jimy Alexander; MEDINA AGUIRRE, Franciso Alejandro y MURIEL ESCOBAR, José A. Sistemas de Seguridad Basados en Biometría

[online]. Scientia et Technica. 2010. vol. 17, p. 98-102. Disponible en: http://www.redalyc.org/pdf/849/84920977016.pdf

CUZME RODRIGUEZ, Fabian Geovanny. El internet de las cosas y las consideraciones de seguridad [online]. Tesis de Maestría en Redes de Comunicaciones. Ecuador: Pontificia Universidad Católica del Ecuador. Facultad de Ingeniería, 2015. 179 p. Disponible en: http://repositorio.puce.edu.ec/xmlui/bitstream/handle/22000/8492/INTERNET%20DE%20LAS%20COSAS%20TESIS%20Y%20CONSIDERACIONES%20DE%20SEGURIDAD%20-%20FINAL.pdf?sequence=1&isAllowed=y

FERNANDEZ SAAVEDRA, María Belén. Evaluation Methodologies for Security Testing of Biometric Systems beyond Technological Evaluation [online]. Tesis Doctoral. Madrid: Universidad Carlos III de Madrid. Departamento de Tecnología Electrónica, 2013. 206 p. Disponible en: http://guti.uc3m.es/data/_uploaded/thesis/PhD_Thesis_BFS.pdf

FUJITSU. PalmSecure [online]. Disponible en: http://www.fujitsu.com/es/products/others/biometric/

GARCIA, Apolinar E. Estrategias empresariales: una visión holística [online]. Bilineata Publishing Bogotá 2013. ISBN 978-958-57943-1-3. Disponible en: https://books.google.com.co/books/about/Estrategias_empresariales.html?id=2QnSAwAAQBAJ&redir_esc=y

HERNANDEZ, Carlos. Estudio del rendimiento biometrico de dispositivos de huella dactilar: análisis de la influencia del tamaño de la muestra [online]. España 2015. Disponible en: http://e-archivo.uc3m.es/bitstream/handle/10016/23621/TFG_Sergio_Sanchez_Martin.pdf

HERNANDEZ BRIONES, Avril. Propuesta de estándar para el uso seguro de Tecnologías Biométricas [online]. Trabajo de grado. México: Universidad Nacional Autonoma de México. Facultad de Ingenieria. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/biometria/index.html

INCIBE. Tecnologías biométricas aplicadas a la ciberseguirdad – Guía de aproximación para el empresario [online]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

JOYANES, Luis. Big Data, análisis de grandes volúmenes de datos en organizaciones. 2016 [online] Disponible en: https://books.google.com.co/books?id=1GywDAAAQBAJ&pg=PT49&dq=CARACTERISTICAS+BIOM%C3%89TRICAS+DE+IDENTIFICACI%C3%93N+Y+RECONOCIMIENTO&hl=es&sa=X&ved=0ahUKEwj27Zjv-

o_XAhWC6iYKHdS8CbkQ6AEIOTAE#v=onepage&q=CARACTERISTICAS%20BIOM%C3%89TRICAS%20DE%20IDENTIFICACI%C3%93N%20Y%20RECONOCIMIENTO&f=false

JURADO PEREZ, Luis Alberto; VELASQUEZ VARGAS, Washington Adrián y VINUEZA ESCOBAR, Nelson Fernando. Estado del Arte de las Arquitecturas de Internet de las Cosas (IoT) [online]. Departamento de Ingeniería de Sistemas Telemáticos - ETSIT - UPM. 2014. Disponible en: http://www.academia.edu/7197061/Estado_del_Arte_de_las_Arquitecturas_de_Internet_de_las_Cosas_IoT_

KIMALDI, Fabricante y Distribuidor de biométricos para el control de acceso y presencia [online]. Disponible en: http://www.kimaldi.com/

LOPEZ GARCIA, Juan. Algoritmo para la identificación de personas basados en huellas dactilares [online]. Trabajo de grado Ingeniero Electrónico. Disponible en: http://upcommons.upc.edu/bitstream/handle/2099.1/8082/proyecto final de carrera.pdf?sequence=1

LOPEZ PEREZ, Nicolas y TORO AGUDELO, Juan José. Técnicas de Biometría basadas en patrones Faciales del ser humano. Trabajo de grado Ingeniero de Sistemas y Computación [online]. Pereira: Universidad Tecnologica de Pereira. Facultad de Ingenieria Electrica, Electronica, Física y Ciencias de la Computación, 2012. 82 p. Disponible en: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2738/0053682L864.pdf?sequence=1&isAllowed=y

MCMAHON, Z. Biometrics History [online]. Indiana University Computer. Agosto, 2005.p. 1-27. Disponible en:

MISFUD-K IDATZIA, Elvira. Sistemas Físicos y biométricos de seguridad [online]. Observatorio Tecnologico. 2012. Disponible en: http://recursostic.educacion.es/observatorio/web/eu/cajon-de-sastre/38-cajon-de-sastre/1045-sistemas-fisicos-y-biometricos-de-seguridad

MORENO DIAZ, Ana Belén. Reconocimiento Facial Automático mediante Técnicas de Visión Tridimensional [online]. Tesis Doctoral. Madrid: Universidad Politécnica de Madrid. Facultad de Informática, 2004. 263 p. Disponible en: http://oa.upm.es/625/1/10200408.pdf

MURIEL ESCOBAR, José A. Sistemas de Seguridad Basados en Biometría [online]. Scientia et Technica. 2010. vol. 17, p. 98-102. Disponible en: http://www.redalyc.org/pdf/849/84920977016.pdf

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL. Face Recognition [online].

NSTC, Committee on Homeland and National Security, Subcommittee on Biometrics. Enero, 2001. p. 1-10. Disponible en: https://www.dhs.gov/biometrics

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL. Biometrics Overview [online]. Biometrics. Marzo, 2006. vol. 3, p. 1-10. Disponible en: https://www.nist.gov/programs-projects/biometrics

ONDATA. Productos profesionales de seguridad informática y computers forensics [online]. Disponible en: http://ondatashop.com/batvox/

PEREZ, Pablo. Estudio sobre las Tecnologías Biométricas aplicadas a la Seguridad [online]. Instituto Nacional de Tecnología de la Comunicación. 2011. p. 100. Disponible en: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnologíasBiométricasASeguridad.pdf

PURIFICACIÓN AGUILAR. Control de acceso en el entorno físico (seguridad informática). 2011. P. 54. [online] Disponible en: https://books.google.com.co/books?id=BovTAwAAQBAJ&dq=control+de+acceso&hl=es&source=gbs_navlinks_s

RAMONET, Ignacio. Capitulo IV [online]. El Imperio de la Vigilancia. C . Intelectual, 2016. p. 168. Disponible en: http://www.periodismo.com/2016/05/03/adelanto-de-el-imperio-de-la-vigilancia-de-ignacio-ramonet/

SANCHEZ AVILA, Carmen. VIII Ciclo de Conferencias UPM – TASSI Aplicaciones de la Biometría a la seguridad [online]. Disponible en: http://oa.upm.es/20071/

SIASA. Distribuidor mayorista Tecnología de Seguridad [online]. Disponible en: http://www.siasa.com/producto.php?prod=0200006

SEGURIDAD. Sistemas Biométricos [online]. Disponible en: http://dis.um.es/~lopezquesada/documentos/IES_1213/SAD/curso/UT3/ActividadesAlumnos/13/bio.html sistema biometrico

THILL, Eduardo. Biometrías 2 [online]. Traducido por Liliana Bosch y Cecilia Pavón. 1 ed. Buenos Aires, Argentina. 2011. 590 p. ISBN 978-987-27495-0-7. Disponible en: http://www.biometria.gov.ar/media/74948/biometrias2.pdf

UNAM. Facultad de Ingeniería, Biometría Informática [online]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/biometria/basesteoricas/fisiologia.html fisiología

UIT. International Telecomunication Unión [online]. Disponbile en: http://www.itu.int/rec/T-REC-X/en

UNIVERSIDAD CATOLICA. Extracción de caracteristicas del Iris como mecánismo de identificación biometrica [online]. 2014. vol. 42, p. 1-15. Disponible en: http://revistavirtual.ucn.edu.co/index.php/RevistaUCN/article/view/503

VARGAS, Georgina A. T. y ARIAS DURA, Raquel. El cómputo ubicuo y su importancia para la construcción del internet de las cosas y el big data [online]. Revista General de Información y Documentación. 2014. vol. 24, no. 2, p. 217-232. Disponible en: http://dialnet.unirioja.es/servlet/articulo?codigo=4955835&info=resumen&idioma=SPA

WACOM BUSINESS SOLUTIONS. STU 530 [online]. Disponible en: http://www.wacom.com/es-ar/enterprise/business-solutions/hardware/signature-pads/stu-530

WAYMAN, James. Federal Biometric Technology Legislation [online]. Computer IEEE. 2000. p.76-80. Disponible en: http://dl.acm.org/citation.cfm?id=621412

W3II. Biométrico de Seguridad de Sistemas [online]. Disponible en: http://www.w3ii.com/es/biometrics/biometrics_system_security.html

WOODWARD, Jhon D.; ORLANS, Nicholas M. y HIGGINS, Peter T. Biometrics [online]. New York.: McGraw-Hill, 2003. ISBN 978-0072222272. Disponible en: https://books.google.com.co/books?id=TCCMAgAAQBAJ&pg=PA144&lpg=PA144&dq=Woodward+J,+Orlans+N,+Higgins+P+biometrics&source=bl&ots=Wk_-GI_Lnc&sig=c8eQrnFwiJZwNbEIvNeowEjokKA&hl=es-419&sa=X&ved=0ahUKEwjzgpiIscrTAhWFSSYKHcCMABYQ6AEIKjAB#v=onepage&q=Woodward%20J%2C%20Orlans%20N%2C%20Higgins%20P%20biometrics&f=false

WESTCORP. Westinghouse Electronics Security & Building Controls [online]. Disponible en: http://www.westcorp.com.ar/geometria_mano.htm

Zorita, Danilo Simón y ORTEGA GARCIA, Javier. Reconocimiento automático medinate patrones biométricos de huella dactilar [online]. Tesis de Doctorado. Madrid: Universidad Politecnica de Madrid. Escuela Técnica Superior de Ingenieros de Telecomunicación, 2003. 225 p. Disponible en: http://oa.upm.es/79/1/09200327.pdf?iframe=true&width=80%25&height=80%25

ANEXOS

Anexo A. RESUMEN ANALÍTICO DE EDUCACIÓN - RAE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

FECHA			**28 de diciembre :2 oko**				
TITULO:			Estado del arte de la Seguridad en Sistemas Biométricos				
AUTOR (ES):			Andrea Giraldo Diana Patricia Gómez Ramírez				
DIRECTOR(ES)/ ASESOR(ES)			Luis Fernando Zambrano				
AÑO ELABORACIÓN			2017				
DESCRIPCIÓN			Trabajo de Grado para optar al Título Especialista en Seguridad Informática				
PAGINAS	86	**TABLAS**	33	**FIGURAS**	27	**ANEXOS**	1
CONTENIDO							
PALABRAS CLAVES:							
Sistema biométrico, patrones, seguridad, verificación, autenticación, control de acceso, sensor, algoritmo, inscripción, autenticación.							
FORMULACION DEL PROBLEMA:							
¿Cuáles son las técnicas y especificaciones de seguridad que utilizan los sistemas biométricos de reconocimiento y autenticación, para el control de acceso e identificación en las organizaciones, que accedan a buenas prácticas de seguridad, funcionalidad y usabilidad, por medio de las características de una persona?							
CONTENIDO:							
En primer capítulo se encuentra la introducción allí se delimita el alcance del trabajo, se plantean los objetivos. En el segundo capítulo se identifica la problemática a la cual se quiere dar solución por medio del desarrollo del trabajo. El tercer capítulo corresponde a la Justificación del proyecto, donde se muestra la importancia e implementación de los sistemas biométricos en la identificación y reconocimiento de las personas a través de procesos automatizados para el control de acceso. El cuarto capítulo corresponde a los Objetivos del proyecto, siendo el objetivo general: “Elaborar el estado del arte de la seguridad en los sistemas biométricos							

para control de acceso e identificación". Adicional, se plantean cuatro objetivos específicos, que son coherentes al logro del objetivo general.

El quinto capítulo es el Marco Referencial el cual permitirá ubicar el estado actual del Proyecto, esté está compuesto del Marco Teórico y la revisión de los antecedentes de los Sistemas Biométricos de Reconocimiento de la Huella Digital, Iris, Facial y Firma, la Geometría de Mano y Dedo, Autenticación por Voz, según sus propiedades y características para la identificación y reconocimiento, además algunos aspectos de seguridad. El marco conceptual y Marco Legal hacen parte de este capítulo, en donde se definen los estándares y la legislación aplicada a los sistemas biométricos de identificación y reconocimiento, los cuales permitirán contribuir a dar solución al problema planteado

El sexto capítulo corresponde al marco metodológico utilizado para definir la forma como se llevará a cabo la investigación para identificar los parámetros de los sistemas biométricos, a través de la investigación documental, por medio del análisis y procesamiento de datos de la muestra seleccionada, por a través del desarrollo de unas actividades estructuradas que permitirá estructurar el análisis interpretación y presentación de resultados por medio del Benchmarking que identificará la mejor opción de los sistemas biométricos del alcance.

El séptimo capítulo corresponde a las técnicas de reconocimiento de patrones de sistemas biométricos, donde se describen los componentes principales del sistema biométrico y las etapas de registro, autenticación y toma de decisiones que surte al finalizar el proceso.

El octavo capítulo se presentan algunas muestras de las herramientas de control de acceso de los sistemas biométricos, y la descripción de las características de software y hardware con las que se cuenta actualmente para los dispositivos y algunos fabricantes reconocidos para la identificación biométrica para el control de acceso.

El noveno capítulo corresponde a la Usabilidad y Seguridad en los sistemas biométricos, en este capítulo se realiza el proceso de análisis de algunas características relacionadas con factores ambientales, propiedades y características y del algoritmo de comparación de los sistemas biométricos. Adicionalmente contempla algunas características de uso y aspectos de seguridad generando unos indicadores que determinan niveles de cada sistema biométrico.

El décimo capítulo corresponde al proceso de comparación por medio de un benchmarking de sistemas biométricos, donde se establecen los parámetros sobre los cuales se realizará la selección de valoración por parámetro y una

ponderación de acuerdo al nivel de influencia, permitiendo determinar el resultado esperado.

METODOLOGÍA DE INVESTIGACIÓN:

Para esta investigación se utilizó un Enfoque Cualitativo para identificar los parámetros de medición de los sistemas biométricos. El tipo de investigación aplicada fue documental argumentativo explorativa, que permitió realizar un análisis de la documentación encontrada para dar cumplimiento a los objetivos planteados.

CONCLUSIONES:

La recopilación de información nos permitió establecer un análisis por medio de un Bechmarking de los sistemas biométricos, donde fueron establecidos unos parámetros que fueron identificados como los más relevantes en el presente proyecto y unas escalas de valoración de acuerdo a la relevancia de cada parámetro.

Finalmente, al realizar está proyecto fue posible identificar que los sistemas biométricos de reconocimiento y autenticación con mayor valoración en el Bechmarking, es decir los más favorables según la evaluación son: el de reconocimiento de huella dactilar, iris y el facial. Durante todo el proceso comparativo estos tres sistemas biométricos son los que marcan la diferencia y los que tienen mayor porcentaje de en la comparación de los parámetros seleccionados, factores ambientales, propiedades y características, algoritmo biométrico y seguridad.

RECOMENDACIONES

Existen diversos parámetros que permiten establecer las características de los sistemas biométricos, las cuales no están en el alcance del presente documento, debido al tipo de proyecto.

FUENTES BIBLIOGRAFICAS:

El presente trabajo cuenta con Cuarenta y seis (48) referencias bibliográficas. A continuación, se anexan las más destacadas en el Proyecto.

Bhalchandra, A. S., Deshpande, N. M., & Pantawane, N. G. (2008). Iris recognition, (December), 1073–1078.

Biometria. (2016). Metodos Biometricos Reconocimiento de Huella Dactilar.

Borja, C. T. (n.d.). Sistemas Biométricos.

Bouihrouzan Belhaj, Omar. (2016) Seguridad e inseguridad en los sistemas biométricos: seguridad vs privacidad.

Fernandez Saavedra María Belén (2013). Evaluation Methodologies for Security Testing of Biometric Systems beyond Technological Evaluation.

INCIBE. Tecnologías biométricas aplicadas a la ciberseguirdad – Guía

Perez, Pablo. (2011) Estudio sobre las Tecnologías Biométricas aplicadas a la Seguridad