

**BIOMETRÍA Y LA SEGURIDAD INFORMÁTICA EN LOS MÉTODOS
DE AUTENTICACIÓN**

JONNY JULIÁN SÁNCHEZ GÓMEZ

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CIUDAD
2020**

**BIOMETRÍA Y LA SEGURIDAD INFORMÁTICA EN LOS MÉTODOS
DE AUTENTICACIÓN**

JONNY JULIÁN SÁNCHEZ GÓMEZ

**Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA**

**Yina Alexandra González Sanabria
Tutora de Curso**

**Martín Camilo Cancelado
Director**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CIUDAD
2020**

NOTA DE ACEPTACIÓN:

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogota D.C., Dia – Mes - Año

DEDICATORIA

Terminando nuestro proceso de formación académica como especialista en Seguridad Informática, quiero dar gracias a Dios primeramente y a todas aquellas personas que hicieron posible la culminación de esta Especialización, que, con cada palabra, nos alentaron en todo momento para que siguiéramos avanzando hacia este importante logro.

RESUMEN

Con el desarrollo de esta monografía, se pretende realizar una búsqueda de información y análisis de los diferentes mecanismos biométricos, la seguridad informática y los distintos métodos que utilizan las organizaciones e individuos para la autenticación, por lo tanto, esta tecnología mide e identifica algunas características propias de un individuo. El documento monográfico tiene como objetivo exponer los diferentes tipos de sistemas biométricos, disponibles para autenticar, reconocer, verificar e identificar un rasgo único de un individuo.

La seguridad informática es crucial para que las organizaciones funcionen, por consiguiente las organizaciones implementan diferentes mecanismos de autenticación que se describen a continuación:

El procedimiento saber algo, se fundamenta en el hecho de que el individuo tiene conocimiento de algo, como una credencial lógica, PIN o códigos que se usaría para ingresar a una aplicación de S.O., computadora, tableta, teléfono o instalación física. El procedimiento tener algo, se fundamenta en el hecho de que el individuo tiene un objeto físico como una USB, credenciales físicas, llaves, token. Simultáneamente, cuando estos procedimientos de autenticación se fusionan, aumentan el nivel de seguridad. Un ejemplo claro son las tarjetas de crédito, para que un individuo pueda usarla, debe conocer el PIN y tener la tarjeta física para poder usarla. Además, estos procedimientos de autenticación tienen cierto grado de debilidad. El procedimiento de saber algo, el individuo puede olvidar el pin o un extraño la puede adivinar, el procedimiento de tener algo, el individuo puede extraviar la tarjeta o un extraño la puede hurtar. El procedimiento algo que eres, son propiedades morfológicas y de comportamiento de un individuo, estas singularidades siempre acompañan al individuo. Por esta razón, no son olvidados, ni perdidos ni robados, este procedimiento se conoce como biometría. La ventaja de usar esta tecnología es que las características del individuo son universales, medibles, únicas y permanentes. El interés de las aplicaciones que usan biometría se puede resumir en dos clases: facilitar el estilo de vida y evitar el fraude por suplantación de identidad la cual es un fenómeno que crece día tras día, el phishing representa una seria amenaza, ya es un método de estafa en el que un delincuente se hace pasar por una persona o empresa.

Pero ¿cómo se define biometría? Según la definición que del libro Seguridad Informática "La biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas. La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de

datos"¹ Hoy en día esta tecnología ya cuenta con un alto grado de desarrollo, esto ha generado que muchas organizaciones estén utilizando estas herramientas con el fin de garantizar los servicios de autenticación y proporcionar una mayor seguridad en los procedimientos.

Las empresas buscan nuevos mecanismos para proteger sus procedimientos de autenticación y neutralizar vulnerabilidades con el robo de datos informáticos. Asimismo, los sistemas biométricos actuales son uno de los métodos más importantes que actúan como escudos para que las organizaciones e individuos protejan transacciones riesgosas del fraude, phishing, modificación de documentos y robo de información. La tecnología también puede ahorrar tiempo a las organizaciones e individuos al eliminar métodos tradicionales de autenticación. La autenticación es importante ya que permite a los usuarios y a las organizaciones mantener su información segura al permitir que solo individuos autenticados (o procesos) accedan a sus recursos lógicos y físicos protegidos, que pueden incluir lugares físicos, sistemas informáticos, entre otros.

Los sistemas biométricos como toda herramienta tecnológica también sufren amenazas y vulnerabilidades, pero son más las ventajas que desventajas que presenta esta tecnología. los usos de esta tecnología son importantes en el mundo de hoy, esta herramienta es segura y conveniente, el desarrollo y sus usos aumentan rápidamente, el alcance de estos sistemas se está expandiendo apresuradamente y haciendo la vida más cómoda, más directa, más inteligente y garantizada.

¹ Costas Santos, Jesús, Seguridad Informática. # ed.b1. Madrid: Ra-Ma S.A. Editorial y Publicaciones, 2010. 55 p. ISBN: 978-84-9964-313-7

ABSTRACT

With the development of this monograph, it is intended to carry out an information search and analysis of the different biometric mechanisms, computer security and the different methods that organizations and individuals use for authentication, therefore, this technology measures and identifies some characteristics characteristic of an individual. The monographic document aims to expose the different types of biometric systems, available to authenticate, recognize, verify and identify a unique trait of an individual.

Computer security is crucial for organizations that work, due to the organizations that have implemented different authentication mechanisms that are described below:

The know something procedure is based on the fact that the individual has knowledge of something, such as a logical credential, PIN or logical code that would be used to enter an S.O. application, computer, tablet, telephone or physical installation. The procedure has something, it is based on the fact that the individual has a physical object such as a USB, physical credentials, keys, token. Simultaneously, when these authentication procedures are merged, they increase the level of security. A clear example is credit cards, so that an individual can use it, they must know the PIN and have the physical card to be able to use it. Furthermore, these authentication procedures have a certain degree of weakness. The procedure of knowing something, the individual can forget the pin or a stranger can guess it, the procedure of having something, the individual can misplace the card or a stranger can steal it. The procedure that you are, are morphological and behavioral properties of an individual, these singularities always accompany the individual. For this reason, they are not forgotten, lost or stolen, this procedure is known as biometrics. The advantage of using this technology is that the characteristics of the individual are universal, measurable, unique and permanent. The interest of applications that use biometrics can be summarized in two classes: facilitating lifestyle and avoiding fraud by identity theft which is a phenomenon that grows day after day, phishing represents a serious threat, it is already a method Scam in which a criminal impersonates a person or company.

But how is biometrics defined? According to the definition in the book Computer Security "Biometrics is a technology that performs measurements in electronic form, saves and compares unique characteristics for the identification of people. The form of identification consists of comparing the physical characteristics of each person with a known pattern and stored in a database "Today this technology is already highly developed, which has led many organizations to be using these tools in order to guarantee authentication services and provide greater security in procedures.

Companies are looking for new mechanisms to protect their authentication procedures and neutralize vulnerabilities with theft of computer data. Furthermore,

today's biometric systems are one of the most important methods that act as shields for organizations and individuals to protect risky transactions from fraud, phishing, document modification, and information theft. Technology can also save organizations and individuals time by eliminating traditional authentication methods. Authentication is important because it allows users and organizations to keep their information secure by allowing only authenticated individuals (or processes) to access their protected logical and physical resources, which can include physical places, computer systems, among others.

Biometric systems, like any technological tool, also suffer threats and vulnerabilities, but there are more advantages than disadvantages that this technology presents. The uses of this technology are important in today's world, this tool is safe and convenient, the development and its uses are increasing rapidly, the scope of these systems is expanding rapidly and making life more comfortable, more direct, smarter and guaranteed.

Keywords: Analysis, Authentication, Biometrics, Computer Decree. Device, Encrypt, Identification, Information, Law, Policies, Regulation, Regulation, Regulations, Security, Systems, Technology, Users, Vulnerabilities,

CONTENIDO

	pág.
RESUMEN.....	5
ABSTRACT.....	7
INTRODUCCIÓN.....	15
1. PLANTEAMIENTO DEL PROBLEMA.....	16
2. JUSTIFICACIÓN.....	18
3. OBJETIVO.....	20
4.1. Objetivo General.....	20
4.2. Objetivos Específicos.....	20
4. MARCO REFERENCIAL.....	21
5.1. MARCO CONCEPTUAL.....	21
5.2. MARCO TEÓRICO.....	26
5.2.1 Factores de Autenticación.....	26
5.2.2 Métodos de autenticación.....	27
5.2.3 Biometría.....	27
5.2.4 Línea Cronológica de la Biometría.....	30
5.2.5 Sistema Biométrico.....	34
5.2.6 Verificación e Identificación.....	35
5.2.7 Medición del rendimiento del sistema biométrico.....	38
5.2.8 Características biométricas.....	39
5.2.9 Autenticación basada en biometría.....	40
5.2.10 Tipos De Biometría Fisiológicos.....	42
5.2.11 Tipos De Biometría Conductual.....	49
5.2.12 Ventajas de la Biometría.....	53
5.2.13 Desventajas de la Biometría.....	54
5.3. MARCO LEGAL.....	56
5.3.1 Entidades.....	56
5.3.2 Estándares Internacionales.....	59
5.3.3 Normatividad para Acceder a Datos biométricos en Colombia.....	68

5.4.	MARCO TECNOLÓGICO	71
4.1	Cuotas del Mercado.....	71
4.2	Compañías desarrolladoras de sistemas Biométricos	73
4.3	Sensores biométricos	77
4.4	Tipos Sensores de Captura	77
4.5	Aplicaciones Horizontales y verticales.....	79
4.6	Comparativa de los sistemas biométricos.....	79
4.7	Aplicaciones de la biometría.....	80
4.8	Sensores de Reconocimiento de Huella	81
4.9	Sensores de Reconocimiento de la Firma	82
4.10	Lector de Venas del Dedo	83
4.11	Lector de Reconocimiento del Iris.....	84
4.12	Lector de Reconocimiento Facial.....	85
4.13	Lector de Reconocimiento Geometría Mano	86
5.	METODOLOGÍA.....	87
5.1	Sistemas de Seguridad Biometría en Colombia	87
5.2	Requisitos para acceder a la Registraduría.....	91
5.3	Convenios con la Registraduría.....	93
5.4	Historial de Convenios de Autenticación Biométrica.....	94
5.5	Historial de Contratos de biometría	95
5.6	Consultas y autenticación biométrica en línea.....	96
5.7	Historial de Consultas y autenticación biométrica en línea.....	97
5.8	Operadores Biométricos	98
5.9	Dispositivos Biométricos.....	99
	CONCLUSIONES	101
	RECOMENDACIONES.....	102
	REFERENCIAS BIBLIOGRÁFICAS.....	103
	ANEXOS.....	106

LISTA DE FIGURAS

pág.

Figura 1. Técnicas de ciberataque utilizadas contras las organizaciones colombianas.....	16
Figura 2. Entidades que utilizan Autenticación Biométrica.	19
Figura 3. Factores de autenticación.....	26
Figura 4. Tipos de factores de autenticación	27
Figura 5. Biometría	29
Figura 6. Sistemas Biométrico	34
Figura 7. Verificación e Identificación	36
Figura 8. Proceso típico de inscripción interna	37
Figura 9. Sistema de reconocimiento biométrico típico.....	37
Figura 10. Elementos principales de un sistema de autenticación biométrica.	38
Figura 11. Tipos de Biometría.....	40
Figura 12. Características de Biométricas	41
Figura 13. Reconocimiento Rostro.....	42
Figura 14. Reconocimiento de la Retina e Iris	44
Figura 15. Reconocimiento por Voz	45
Figura 16. Reconocimiento de la Huella Dactilar	46
Figura 17. Reconocimiento de la Palma de la Mano	47
Figura 18. Reconocimiento Vascular	48
Figura 19. Reconocimiento del oído	49
Figura 20. Dinámica del Tecleo	50
Figura 21. Reconocimiento de Firma	51
Figura 22. Estilo de Marcha	52
Figura 23. Movimiento de los labios	53
Figura 24. Ventajas de Biometría.....	53
Figura 25. Estandarización en biometría	58
Figura 26. Agencias especializadas de la ONU	58
Figura 27. consorcios internacionales.....	58

Figura 28. Número de dispositivos móviles biométricos vs no-biométricos en Latinoamérica	71
Figura 29. Uso tipos de autenticación biométrica	72
Figura 30. Dispositivos biométricos y sensores Participación en el mercado de ingresos por tipo	73
Figura 31. Ingresos totales de dispositivos biométricos por mercado final	73
Figura 32. Características y factores sociales de distintas modalidades biométricas (comparativo)	78
Figura 33. Tasa de respuesta encuesta 1.....	88
Figura 34. Tasa de respuesta encuesta 2.....	88
Figura 35. Tasa de respuesta encuesta 3.....	89
Figura 36. La biometría a 2020 en los servicios financieros	89
Figura 37. Tipos de organización en las que las personas confían más para proteger su información biométrica (perspectiva global).....	90
Figura 38. Uso de banca online.	90
Figura 39. Historial convenios y autenticación biométrica.	94
Figura 40. Historial contratos.	95
Figura 41. Historial consultas y autenticación biométrica en línea.....	97

LISTA DE TABLAS

pág.

Tabla 1. Métodos de autenticación..	27
Tabla 2. Línea de Tiempo de la Biometría..	30
Tabla 3. Características biométricas.	39
Tabla 4. Estándares ITU-T.	59
Tabla 5. Pruebas de rendimiento biométrico y estándares de informes	59
Tabla 6. Lista de estándares de calidad de muestra e informes técnicos	60
Tabla 7. Estándares de prueba de conformidad	60
Tabla 8. Interfaces técnicas	61
Tabla 9. Estandarización de interfaz	62
Tabla 10. Estándares de formato de datos	63
Tabla 11. Pruebas de rendimiento	65
Tabla 12. Perfiles biométricos para interoperabilidad e intercambio de datos	66
Tabla 13. Perfiles.	66
Tabla 14. Normas de seguridad	67
Tabla 15. Normatividad para Acceder a Datos biométricos en Colombia	68
Tabla 16. Compañías desarrolladora sistemas Biométricos	73
Tabla 17. Sensores para la captura.	77
Tabla 18. Comparativa de sistemas biométricos.	79
Tabla 19. Aplicaciones Horizontales y verticales	79
Tabla 20. Aplicaciones de la biometría.	80
Tabla 21. Lectores biométricos de reconocimientos de huellas dactilares..	81
Tabla 22. Lectores biométricos de reconocimientos de Firma.	82
Tabla 23. Lectores biométricos de reconocimientos vascular.	83
Tabla 24. Lectores biométricos de reconocimientos del Iris....	84
Tabla 25. Lectores biométricos de reconocimientos Facial..	85
Tabla 26. Lector de Reconocimiento Geometría Mano.	86
Tabla 27. Requisitos entidades Publicas.	91
Tabla 28. Requisitos entidades Privadas.	92
Tabla 29. Convenios.	93

Tabla 30. Historial de Convenios.	94
Tabla 31. Historial de Contratos.....	95
Tabla 32. Consultas y autenticación biométrica en línea 2019..	96
Tabla 33. Historial Consultas y autenticación biométrica en línea..	97
Tabla 34. Operadores Biométrico en Colombia..	98
Tabla 35. Dispositivos Biométricos..	99

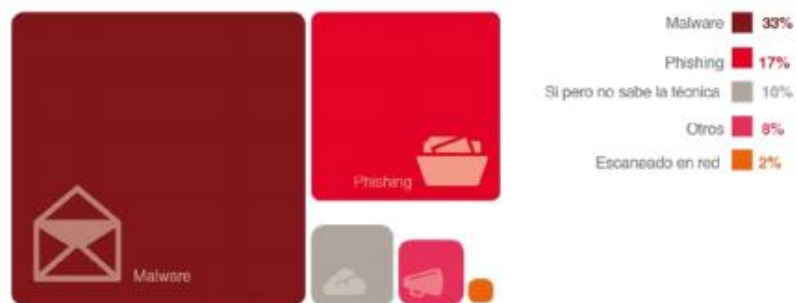
INTRODUCCIÓN

El siguiente documento monográfico se presenta como una propuesta para obtener el título de especialista en seguridad informática y, a través de él, se llevará a cabo una investigación de los diferentes dispositivos biométricos existentes hoy en día como mecanismo de autenticación a través de esta tecnología, asimismo el propósito es ayudar a fortalecer la seguridad informática de los usuarios, instituciones y organizaciones. Como se prueba su identidad si alguien la cuestiona, el proceso de probar su identidad se conoce como autenticación, De esta manera, los sistemas de información biométricos permiten gestionar adecuadamente los principios fundamentales de la seguridad informática la cual establece tres pilares como son la confidencialidad, la integridad y la disponibilidad de la información, La biometría no es más que una herramienta tecnología de reconocimiento automatizado y sistemático con el fin de autenticar a los individuos basada en sus características biológicas y de comportamiento. En la actualidad, estos sistemas biométricos brindan a las empresas la posibilidad de hacer los procesos más rápidos y confiables, debido a que permite que el acceso a la información se haga de forma inmediata, evitando la pérdida de tiempo y que los datos se dupliquen. Lo anterior le garantiza a las organización y usuarios más competitividad y mejor productividad, esto se debe a que estos sistemas de información agilizan los procedimientos en las organizaciones e individuos de una manera segura, permitiendo que las organizaciones estén a la vanguardia de las nuevas tecnologías garantizando información concreta, rápida y de fácil acceso. esta sistemas de información es muy madura de igual forma es bastante utilizada en muchas aplicaciones gubernamentales y civiles esto con el fin de agilizar sus servicios y brindar mayor seguridad a los trámites, esta tecnología es una de las principales escudos de organizaciones para proteger las transacciones de riesgos como, el fraude, la suplantación de identidad, la alteración de documentos y el robo de información. Como todos los avances no todo iban a ser ventajas, los sistemas biométricos como en cualquiera otra herramienta tecnológica tendrá errores siempre existirá un margen de error.

1. PLANTEAMIENTO DEL PROBLEMA

Las organizaciones hoy en día buscan diferentes mecanismos para contrarrestar el fraude como son los ataques de Phishing o suplantación de identidad, En la siguiente (Figura 1). se evidencia las técnicas de ciberataque utilizadas contra las organizaciones colombianas y el phishing tiene un porcentaje de un 17% de fraude. Una de las medidas que diversos sectores de la sociedad han adoptado para combatir este delito es la implementación de sistemas biométricos para ayudar a mitigar este fenómeno. La presente monografía pretende recolectar información sobre los diversos mecanismos de autenticación biométricos. Los métodos tradicionales de gestión de identidad, si bien son efectivos, suelen ser incómodos ya que cada uno presenta debilidades. la contraseña se olvidada o la descifran un tercero y en el segundo caso, los objetos pueden ser hurtados o perderse con facilidad y esto afecta al usuario final. La investigación de esta monografía se basa en la formulación de las siguientes preguntas a pesar del atractivo de usar datos biométricos para autenticar, ¿son estos sistemas realmente más seguros que los métodos tradicionales de gestión de identidad? Y, lo que es más importante, ¿podrían poner en riesgo la seguridad y la privacidad de la información del usuario? Aunque la tecnología ha avanzado ¿son los procesos biométricos 100% seguro? y ¿son los sistemas biométricos perfectos? Hay otro tema a considerar y es la confiabilidad de la biometría. Las caras cambian con la pérdida o ganancia de peso, y las personas se ven diferentes a medida que envejecen. Las huellas digitales, si bien son exclusivas de las personas, también tienen similitudes. ¿Y qué hay de cortes o quemaduras en un dedo? ¿Es realmente un sistema tan perfecto para la autenticación ?

Figura 1: Técnicas de ciberataque utilizadas contra las organizaciones colombianas



Fuente: Fraude al descubierto Encuesta Global Crimen Económico 2018 ²

Si bien las tasas de error son bajas, los sistemas deben permitir tolerancias de medición basadas en el hecho de que con todas las diferentes mediciones

² PwC, Fraude al descubierto Encuesta Global Crimen Económico 2018 Colombia [En Línea]. Ciudad: Bogotá. Autores: PwC 2018; Disponible en: https://www.pwc.com/co/es/assets/document/crimesurvey_2018.pdf

involucradas, la huella dactilar, signatura, iris, voz nunca entregan exactamente los mismos datos porque el iris o la huella dactilar puede estar en un ángulo diferente. Esto significa que solo se puede determinar una coincidencia aproximada. Aunque los sistemas de seguridad biométrica pueden mitigar los problemas asociados con el uso de contraseñas, tokens y tarjetas inteligentes, estos sistemas son algo susceptibles a ataques de falsificación y capacidad de enlace. Por ejemplo, un dedo falso creado con gelatina y un molde de plástico se puede usar para engañar a los dispositivos de reconocimiento de huellas digitales.

Los riesgos del uso de la biometría se dividen en algunas categorías, que incluyen la piratería de datos y redes, capacidad de fraude que evolucionan rápidamente, seguridad de inscripción biométrica, fraude familiar (es decir, causado por un miembro de la familia o un amigo), sensores falsificados e inexactitud del sensor. Aunque los sistemas de identidad biométrica son más difíciles de vulnerar, cosas como las máscaras y las caras falsas a veces pueden engañar a los sistemas de reconocimiento facial. Las huellas digitales también tienen sus problemas., se ha utilizado el aprendizaje automático para crear huellas digitales que combinaba las características de muchas huellas digitales en una impresión maestra falsa para engañarlos a todos. Con este tipo de huella digital maestra se puede iniciar sesión en dispositivos con una sola rutina de autenticación, como un teléfono inteligente, tableta o incluso el sistema de seguridad de su hogar. En otras palabras, se demostró que las huellas digitales son pirateables.

2. JUSTIFICACIÓN


La presente monografía pretende hacer una investigación, un análisis y una interpretación en relación con los diversos mecanismos biométricos y cómo las organizaciones e individuos pueden reducir el fraude, vulnerabilidades, riesgos y las amenazas cibernéticas con la utilización esta tecnología. Estos sistemas pueden hacer uso de una gran variedad de características fisiológicas y morfológicas como: palma de la mano, rostros, retina, iris voz, vascular o estructura del oído. Asimismo esta tecnología también usa características conductuales, como una firma escrita, el movimiento de los labios, estilo de marcha, olor, dinámica de tecleo dichas funciones crean una señal individual que puede medirse mediante tecnología biométrica. La tecnología biométrica no es nueva y su utilización ha resultado ser cada vez más frecuente de lo que la mayoría de la gente imaginaba. Se podría interpretar que la biometría ofrece un alto nivel de detección y operaciones de seguridad que tienen muchos beneficios sobre los métodos convencionales. La biometría tiene grandes ventajas, frente a otros sistemas de autenticación, como son el uso de pulseras, contraseñas o tarjetas. Es más cómodo porque es algo que hace parte de la persona, no se pierde, no se olvida, no tiene gastos de mantenimiento y es extremadamente difícil de imitar. Las ventajas que proporciona la biometría es que la información es distintiva para cada persona y puede utilizarse como una técnica para la identificación individual.

Los principales beneficios de estos sistemas son autenticación, privacidad o discreción de datos, autorización o control de acceso, veracidad de datos y no repudio. La tecnología biométrica es capaz de garantizar un acceso protegido rápido y confiable a la información. Esta tecnología está constante creciendo a un ritmo acelerado en Colombia y está siendo adoptada como solución de seguridad ya que ha desempeñado un papel importante proporcionando accesibilidad, simplicidad, confidencialidad y precisión absoluta en la autenticación, identificación y verificación de un individuo. Por tal motivo estos sistemas gozan de una amplia aceptación en diversos sectores como entidades gubernamentales, bancarios, salud, educación, comercio, industria, social, entre otros, ya que aumenta la productividad, eficiencia y garantizar la autenticidad de los individuos cuando realizan diversa operaciones o transacciones. De esta manera esta tecnología se emplea eficazmente en medicina forense, también se usa para la identificación de criminal y la seguridad penitenciaria. además se puede utilizar para evitar el acceso ilícito a cajeros automáticos, teléfonos celulares, computadoras de escritorio, estaciones de trabajo y redes de computadoras, un ejemplo claro son las entidades bancarias, según RCN en su portal web "El 60% de las entidades financieras del país usan la autenticación biométrica"³ otra entidad es la Registraduría Nacional del Estado Civil

³ RCN Radio, El 60% de las entidades financieras del país usan la autenticación biométrica [En Línea]. Ciudad: Bogotá. Autores: RCN 2020; Disponible en: <https://www.rcnradio.com/colombia/el-60-de-las-entidades-financieras-del-pais-usan-la-autenticacion-biometrica>

de Colombia " ha utilizado durante los últimos 12 años la biometría como una herramienta para identificar a los colombianos"⁴.

Figura 2: Entidades que utilizan Autenticación Biométrica.

 REGISTRADURÍA <small>NACIONAL DEL ESTADO CIVIL</small>		AUTENTICACIÓN BIOMÉTRICA			
		2015	2016	2017	Total general
	UNIÓN COLEGIADA DEL NOTARIADO COLOMBIANO	1.123.251	8.982.232	9.655.458	19.760.941
	CÁMARA DE COMERCIO DE BOGOTÁ	208.075	918.715	549.808	1.676.598
	NOTARIOS INDEPENDIENTES	-	2.108.443	2.767.389	4.875.832
	CONFECÁMARAS	-	708.986	706.895	1.415.881
	AERONAUTICA CIVIL	-	1.567	19.866	21.433
	ASOBANCARIA - BBVA	-	681	232.201	232.882
	BANCO COLPATRIA	-	555	145.417	145.972
	BANCO AGRARIO	-	51	9.685	9.736
	PROTECCIÓN	-	-	370.119	370.119
	COMCEL	-	-	180.731	180.731
	TELMEX	-	-	2.502	2.502
	ASOBANCARIA - BANCOOMEVA	-	-	918	918
	ASOBANCARIA - BANCO POPULAR	-	-	33.026	33.026
	ASOBANCARIA - RCI	-	-	4.110	4.110
	ASOBANCARIA - PORVENIR	-	-	66.711	66.711
	ASOBANCARIA - BANCO CAJA SOCIAL	-	-	9.720	9.720
	ASOBANCARIA - TUYA	-	-	1.169	1.169
	ASOBANCARIA - BANCOLOMBIA	-	-	1.669	1.669
	SERFINANSA	-	-	95.659	95.659
	POLICIA NACIONAL	-	-	189.385	189.385
	COLOMBIA TELECOMUNICACIONES S.A. E.S.P.	-	-	30.632	30.632
	FONDO NACIONAL DEL AHORRO	-	-	2.270	2.270
	INSCRIPCIÓN DE CÉDULAS	-	-	519.776	519.776
	Total consultas biométricas	1.331.326	12.721.230	15.595.116	29.647.672

61 Convenios

8 Contratos

Fuente: Registraduría Nacional del estado civil, Autenticación biométrica en Colombia⁵.

⁴ Registraduría Nacional del Estado Civil de Colombia, Identificación Biométrica: cada vez con más Usos En La Vida Cotidiana [En Línea]. Ciudad: Bogotá. Autores: Registraduría Nacional del Estado Civil de Colombia 2020; Disponible en: <https://www.registraduria.gov.co/Identificacion-biometrica-cada-vez.html>

⁵ Registraduría Nacional del estado civil, Autenticación biométrica en Colombia. [En Línea]. Ciudad: Bogotá. Autores: Registraduría Nacional del estado civil 2018; Disponible en: <https://web.certicamara.com/media/221765/autenticacion-biometrica-en-colombia.pdf>

3. OBJETIVO

4.1. Objetivo General

Describir el funcionamiento de los diferentes sistemas biométricos y sus procesos de autenticación, verificación y almacenamiento de datos los cuales garanticen que la información sea confiable, precisa y rápida.

4.2. Objetivos Específicos

Se muestran los objetivos específicos, los cuales nacen tras diseñar el objetivo general y a través de ellos poder cumplir lo planteado.

- Exponer el funcionamiento de la autenticación en los diferentes mecanismos de los sistemas biométricos en la seguridad informática.
- Determinar las ventajas y desventajas de autenticación en los diversos sistemas de biométricos en la seguridad informática.
- Establecer los riesgos asociados con el uso de esta herramienta tecnológica en el ámbito de la seguridad informática.
- Investigar la efectividad y la eficiencia de la autenticación con el uso de los sistemas biométricos en la seguridad informática.

4. MARCO REFERENCIAL

5.1. MARCO CONCEPTUAL

Para la comprensión de los diferentes aspectos que comprende esta monografía, se hace necesario la definición de algunos conceptos y procesos, descritos a continuación.

- Acceso. Los permisos para el acceso a la información deben ser adecuados, pero estrictamente controlados.⁶
- Almacenamiento de Datos: refiere al uso de medios de grabación para conservar los datos utilizando PC y otros dispositivos. Las formas más frecuentes de almacenamiento de datos son el almacenamiento de archivos, el almacenamiento en bloque y el almacenamiento de objetos, cada uno de los cuales resulta adecuado para un fin diferente⁷
- Amenazas: Portantier define "es cualquier peligro potencial sobre la información y/o los sistemas".⁸
- Ataque: ISO define "Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo." ⁹
- Autenticación de usuarios: Asegura la identidad de los sujetos participantes en una comunicación o sesión de trabajo, mediante contraseñas, biometría (huellas dactilares, identificación de retina, etc.), tarjetas inteligentes o de banda magnética, o procedimientos similares¹⁰
- Autenticación: Amarañon define como el "procedimiento para comprobar que alguien es quién dice ser cuando accede a un ordenador o a un servicio

⁶ Universidad Nacional Autónoma de México - Revista Digital Universitaria, El Fraude y la Delincuencia Informática: Un Problema Jurídico y Ético [En Línea]. Ciudad: México. Autores: Begoña Albizuri. 2002;

Disponible en: <http://www.revista.unam.mx/vol.3/num2/art3/>

⁷ Hewlett Packard, ¿Qué Es El Almacenamiento De Datos? [En Línea]. Ciudad: . Autores: Hewlett Packard Enterprise Development LP 2020; Disponible en: <https://www.hpe.com/es/es/what-is/data-storage.html>

⁸ Fabian Portantier. Seguridad Informática, Gestión de la Seguridad En: USERS. 2012. vol. 1. no. 192, p. 38.

⁹ iso27000, ¿Glosario? [En Línea]. Ciudad: . Autores: iso27000 2020; Disponible en: <http://www.iso27000.es/glosario.html>

¹⁰ Amarañon Gonzalo, Álvarez Seguridad Informática Para La Empresa Y Particulares. # ed. MADRID: MCGRAW-HILL, 2004. 96 p. ISBN: 84-481-4008-7.

online. Este proceso constituye una funcionalidad característica para una comunicación segura".¹¹

- Autorización: Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.¹²
- Biometría: La biometría es un método de reconocimiento de personas basado en sus características fisiológicas (huellas dactilares, retinas, iris, cara, etc.) o de comportamiento (firma, forma de andar, tecleo, etc.).¹³
- Confidencialidad: consiste en garantizar que los datos, objetos y recursos solamente pueden ser leídos por sus destinatarios legítimos¹⁴
- Contraseña: Información secreta, en general un grupo de caracteres, utilizada para autenticación¹⁵
- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo¹⁶
- Datos Biométricos: es toda aquella propiedad física, fisiológica, de comportamiento o rasgo de la personalidad, atribuible a una sola persona y que es medible¹⁷

¹¹ Instituto Nacional de Ciberseguridad, Glosario de términos de ciberseguridad [En Línea]. Ciudad: Madrid. Autores: INCIBE 2017; Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

¹² Amarañon Gonzalo, Álvarez Seguridad Informática Para La Empresa Y Particulares. # ed. MADRID: MCGRAW-HILL, 2004. 96 p. ISBN: 84-481-4008-7

¹³ Instituto Nacional de Ciberseguridad, Glosario de términos de ciberseguridad [En Línea]. Ciudad: Madrid. Autores: INCIBE 2017; Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

¹⁴ Amarañon Gonzalo, Álvarez Seguridad Informática Para La Empresa Y Particulares. # ed. MADRID: MCGRAW-HILL, 2004. 95 p. ISBN: 84-481-4008-7.

¹⁵ Centro Criptológico Nacional, GUÍA DE SEGURIDAD - GLOSARIO Y ABREVIATURAS [En Línea]. Ciudad: Madrid. Autores: ccn-cert 2015; Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html

¹⁶ Ministerio de Tecnologías de la Información y las Comunicaciones, Modelo de Seguridad y Privacidad de la Información [En Línea]. Ciudad: Bogotá. Autores: Mintic 2018; Disponible en: https://www.mintic.gov.co/gestionti/615/articulos-5482_Modelo_de_Seguridad_Privacidad.pdf

¹⁷ El Economista, ¿Qué y cuáles son los datos biométricos? [En Línea]. Ciudad: Mexico. Autores: León A. Martínez 2018; Disponible en: <https://www.eleconomista.com.mx/tecnologia/Que-y-cuales-son-los-datos-biometricos-20180529-0068.html>

- Datos Personales: nos referimos a toda aquella información asociada a una persona y que permite su identificación¹⁸
- Disponibilidad: Situación que se produce cuando se puede acceder a los servicios de un sistema en un periodo de tiempo considerado aceptable¹⁹
- Dispositivo electrónico: son aquellos que utilizan la electricidad para el almacenamiento, transporte, o transformación de información²⁰
- Fraude Informático: entendido como el uso indebido o la manipulación fraudulenta de los elementos informáticos de cualquier tipo, que produce un beneficio ilícito.²¹
- Huella Dactilar: es la captura de las crestas de fricción de un dedo humano.
- Identificación De Huellas Digitales: (a veces denominada dactiloscopia [3]) es el proceso de comparar las impresiones de la cresta de la piel de fricción cuestionadas y conocidas (ver Minutiae) de los dedos, palmas y dedos de los pies para determinar si las impresiones son del mismo dedo (o palma, dedo del pie, etc.)
- Identificación Electrónica: , el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica²²

¹⁸ Superintendencia de Industria y Comercio, ¿Protección de Datos Personales? [En Línea]. Ciudad: Bogotá. Autores: SIC 2018; Disponible en: <https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>

¹⁹ Centro Criptológico Nacional, GUÍA DE SEGURIDAD - GLOSARIO Y ABREVIATURAS [En Línea]. Ciudad: Madrid. Autores: ccn-cert 2015; Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html

²⁰ Asociación General de Consumidores, Dispositivos electrónicos [En Línea]. Ciudad: Madrid. Autores: ASGECO. 2019; Disponible en: <http://asgeco.org/consumeoriginal/dispositivos-electronicos/>

²¹ Universidad Nacional Autónoma de México - Revista Digital Universitaria, El Fraude y la Delincuencia Informática: Un Problema Jurídico y Ético [En Línea]. Ciudad: México. Autores: Begoña Albizuri. 2002; Disponible en: <http://www.revista.unam.mx/vol.3/num2/art3/>

²² Centro Criptológico Nacional, GUÍA DE SEGURIDAD - GLOSARIO Y ABREVIATURAS [En Línea]. Ciudad: Madrid. Autores: ccn-cert 2015; Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html

- Impacto: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.²³
- Integridad: La información debe mantenerse completa (íntegra) y libre de manipulaciones fortuitas o deliberadas, de manera que siempre se pueda confiar en ella.²⁴
- Ley de Protección de datos Personales: reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada²⁵
- Phishing: Phishing es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta²⁶
- Privacidad: Derecho de los individuos a controlar e influir en la recogida y almacenamiento de datos referentes a los mismos, así como por quien y a quien pueden ser dados a conocer estos datos²⁷
- Riesgo: es la probabilidad de que algo negativo suceda dañando los recursos.
- Seguridad de la información: un conjunto de medidas de prevención, detención y corrección orientadas de proteger la confidencialidad, la integridad y la disponibilidad.²⁸

²³ iso27000, ¿Glosario? [En Línea]. Ciudad: . Autores: iso27000 2020; Disponible en: <http://www.iso27000.es/glosario.html>

²⁴ Amarañón Gonzalo, Álvarez Seguridad Informática Para La Empresa Y Particulares. # ed. MADRID: MCGRAW-HILL, 2004. 96 p. ISBN: 84-481-4008-7

²⁵ Superintendencia de Industria y Comercio, ¿Protección de Datos Personales? [En Línea]. Ciudad: Bogotá. Autores: SIC 2018; Disponible en: <https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>

²⁶ Instituto Nacional de Ciberseguridad, Glosario de términos de ciberseguridad [En Línea]. Ciudad: Madrid. Autores: INCIBE 2017; Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

²⁷ Centro Criptológico Nacional, GUÍA DE SEGURIDAD - GLOSARIO Y ABREVIATURAS [En Línea]. Ciudad: Madrid. Autores: ccn-cert 2015; Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html

²⁸ (CONCEPTOS DE SEGURIDAD INFORMATICA, 2020)

- **Sistemas Biométricos:** un sistema automatizado que realiza tareas de biometría. Es decir, un sistema que basa sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida y/o verificada de forma automatizada.²⁹
- **Sistemas de Información:** Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar (tratar), mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.³⁰
- **Suplantación de Identidad:** Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (cyberbullying)³¹
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).³²
- **Verificación:** confirmación mediante la aportación de evidencia objetiva de que se han cumplido los requisitos especificados.³³
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.³⁴

²⁹ Observatorio tecnológico, Sistemas físicos y biométricos de seguridad [En Línea]. Ciudad: Madrid. Autores: Elvira Misfud 2012; Disponible en: <http://recursostic.educacion.es/observatorio/web/fr/cajon-de-sastre/38-cajon-de-sastre/1045-sistemas-fisicos-y-biometricos-de-seguridad>

³⁰ Centro Criptológico Nacional, GUÍA DE SEGURIDAD - GLOSARIO Y ABREVIATURAS [En Línea]. Ciudad: Madrid. Autores: ccn-cert 2015; Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html

³¹ Instituto Nacional de Ciberseguridad, Glosario de términos de ciberseguridad [En Línea]. Ciudad: Madrid. Autores: INCIBE 2017; Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

³² Ministerio de Tecnologías de la Información y las Comunicaciones, Modelo de Seguridad y Privacidad de la Información [En Línea]. Ciudad: Bogotá. Autores: Mintic 2018; Disponible en: https://www.mintic.gov.co/gestionti/615/articulos-5482_Modelo_de_Seguridad_Privacidad.pdf

³³ Centro Criptológico Nacional, GUÍA DE SEGURIDAD - GLOSARIO Y ABREVIATURAS [En Línea]. Ciudad: Madrid. Autores: ccn-cert 2015; Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html

³⁴ iso27000, ¿Glosario? [En Línea]. Ciudad: . Autores: iso27000 2020; Disponible en: <http://www.iso27000.es/glosario.html>

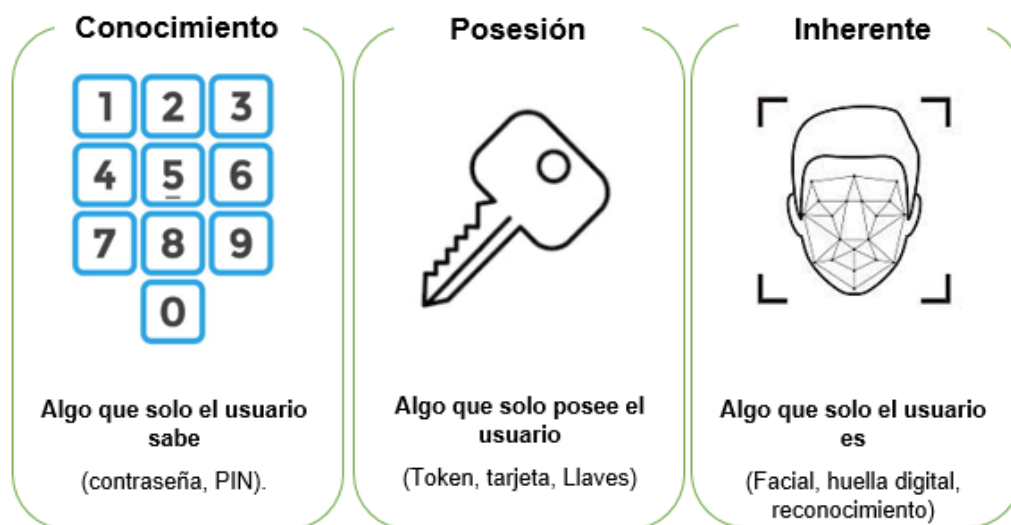
5.2. MARCO TEÓRICO

Para la comprensión de los diferentes aspectos de la presente monografía, se hace necesario la definición de algunos aspectos teóricos, que orienten al lector. Así mismo muchos de nosotros creíamos que la biometría solo consistía en la lectura de huellas digitales, pero la realidad es que abarca muchos métodos de reconocimiento de personas basados en propiedades fisiológicas o de conducta.

5.2.1 Factores de Autenticación

Las formas en que se puede autenticar a alguien se pueden agrupar en tres categorías básicas, en función de lo que se conoce como factores de autenticación: algo que el usuario sabe, algo que tiene el usuario o algo que es el usuario. Cada factor de autenticación cubre una gama de elementos utilizados para autenticar o verificar la identidad de una persona antes de que se le otorgue acceso, apruebe una solicitud de transacción, firme un documento, otorgue autoridad a otros, etc.

Figura 3. Factores de autenticación.

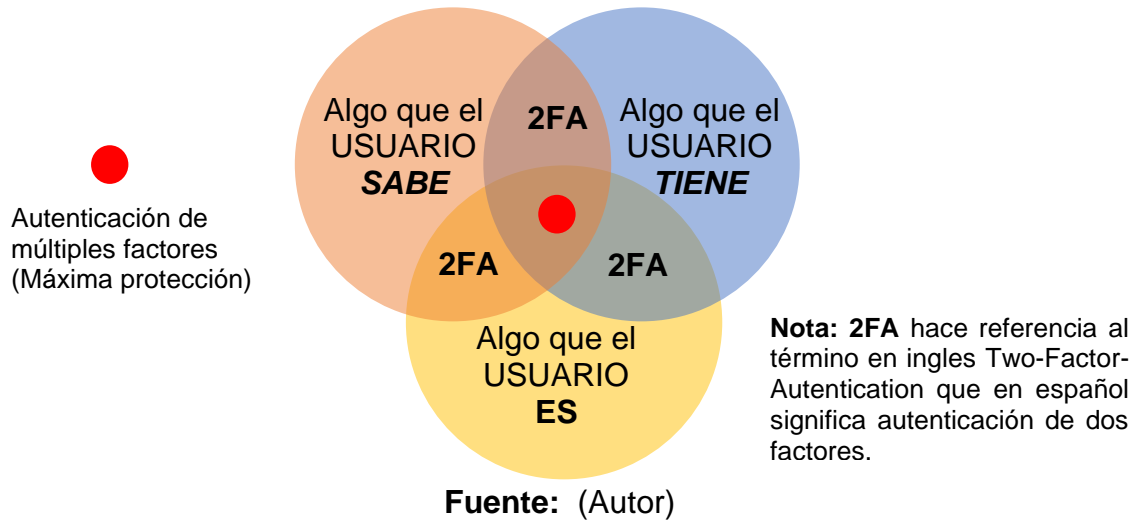


Fuente: (Autor)

- **Factores de conocimiento** son algo que el usuario conoce y, con suerte, recuerda, como una contraseña, un código PIN, una respuesta a una pregunta de seguridad, etc.
- **Factores de propiedad** son algo que el usuario tiene, por ejemplo, una tarjeta de identificación, token de seguridad, teléfono celular, llave física, etc.
- **Factores de inherencia** son algo que el usuario es o hace, por ejemplo, una huella digital, firma, voz, etc. La autenticación biométrica, que es el alcance

de este documento, aprovecha varios factores de inherencia para validar la identidad de un usuario

Figura 4 . Tipos de factores de autenticación.



5.2.2 Métodos de autenticación.

Tabla 1. Métodos de autenticación en la seguridad.

	Conocimiento secreto	Posesión personal	Biometría
Ejemplo	Contraseña, PIN	Llave, tarjeta de identificación, token	Huella digital, cara, Palma de la mano.
Copiado	Software	fácil a muy difícil	difícil
Perdió	Olvidado	Fácil	difícil
Robado	Espiada	Posible	difícil
Circulado	Fácil	Fácil	difícil
Cambiado	Fácil	Fácil	difícil

Fuente: El Autor.

5.2.3 Biometría

De acuerdo con la lectura de la revista (USERS) el cual afirma que "la biometría es el estudio de métodos automáticos para el reconocimiento de personas basados en rasgos de conducta o físico. Etimológicamente, proviene del griego bios (vida) y metro (medida). En nuestro campo, es la aplicación de método matemáticos y tecnológicos para identificar o verificar identidad"³⁵ asimismo controlar el acceso,

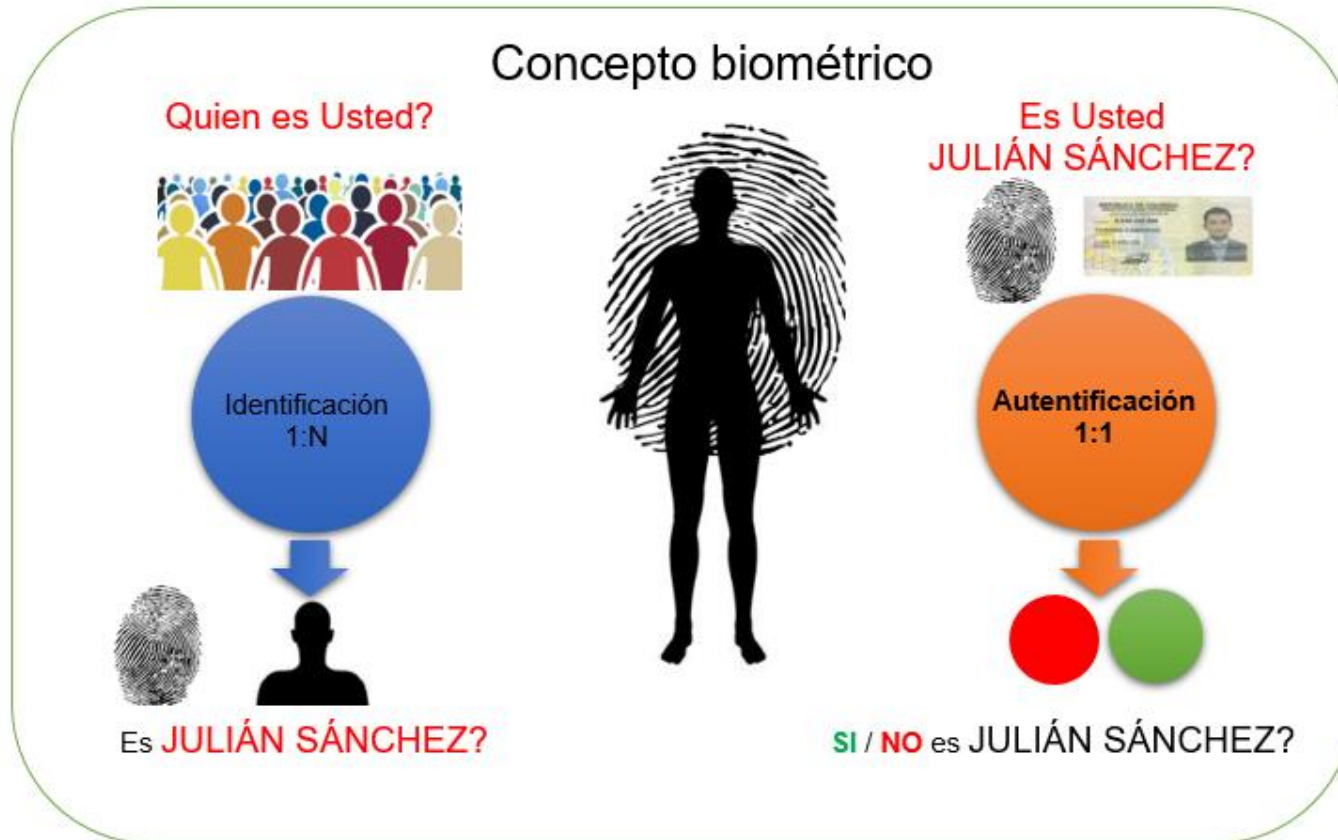
³⁵ Pacheco, Federico G. Jara, Héctor. Seguridad Física y Biometría. En: USERS. 2009. vol. 173. no. 352, p. 59.

autorización de usuarios, protección de datos y gestión de seguridad. En contraste con la seguridad tradicional como son los sistemas contraseñas de inicio de sesión y PIN, las técnicas de seguridad biométrica han demostrado un mayor nivel de seguridad. "Esta tecnología se encarga de verificar la identidad del usuario comprobando factores que este relacionados con la biología de la persona (de ahí el nombre "biometría") alguna de las características más utilizadas son el escaneo de iris, escaneo de retina y escaneo de la huella dactilar. "³⁶ La identificación del usuario se produce en base a rasgos propios e irrepitibles de su persona, como sus huellas dactilares, su voz, la geometría de la palma de su mano o la configuración de su retina. Este método sí que identifica al usuario, ya que cuando estos dispositivos funcionan correctamente, sólo un individuo puede ser identificado con éxito, en virtud de una acertada elección de los parámetros fisiológicos a evaluar.³⁷

³⁶ Fabian Portantier. Seguridad Informática - Sistemas Operativo - Biometría En: USERS. 2012. vol. 1. no. 192, p. 129.

³⁷ Amarañon Gonzalo, Álvarez Seguridad Informática Para La Empresa Y Particulares. # ed. Madrid: MCGRAW-HILL, 2004. 147. ISBN: 84-481-4008-7.

Figura 5. Biometría



Fuente: Registraduría Nacional del estado civil, Autenticación biométrica en Colombia³⁸.

³⁸ Registraduría Nacional del estado civil, Autenticación biométrica en Colombia. [En Línea]. Ciudad: Bogotá. Autores: Registraduría Nacional del estado civil 2018; Disponible en: <https://web.certicamara.com/media/221765/autenticacion-biometrica-en-colombia.pdf>

5.2.4 Línea Cronológica de la Biometría

Durante las últimas décadas, la biometría basada en sistemas de seguridad ha obtenido una gran popularidad y una considerable cantidad de atención. Esta tecnología automatizada ha estado disponible en las últimas décadas, exactamente comenzó a surgir en la segunda mitad del siglo XX, debido a los grandes avances significativos en el campo del procesamiento de las computadora y sistemas de información. El campo naciente experimentó una explosión de actividad en la década de 1990 y comenzó a surgir en las aplicaciones cotidianas a principios de la década de 2000. Sin embargo, muchas de estas nuevas técnicas automatizadas se basan en ideas que fueron concebidas originalmente cientos, incluso miles de años atrás. En la Tabla 3 se realiza una línea de tiempo de la biometría.

Tabla 2. Línea de Tiempo de la Biometría.

Tiempo	Acontecimiento
31,000 años	Existen registros de paredes de cuevas adornadas con pinturas creadas por hombres prehistóricos el cual vivió allí. Alrededor de estas pinturas hay numerosas huellas de manos que "han actuado como una firma inolvidable" de su creador.
Comienzo de la civilización	El ejemplos más antiguos y básicos de una característica que se utiliza para el reconocimiento por parte de los humanos es la cara
500 a.C	También hay evidencia de que las huellas digitales se usaron como marca de una persona ya en 500 a.C. "Las transacciones comerciales de Babilonia se registran en tabletas de arcilla que incluyen huellas digitales".
Egipto	los rasgos físicos identificaban a los comerciantes para diferenciar entre comerciantes confiables de reputación conocida y transacciones exitosas anteriores, y aquellos nuevos en el mercado.
Siglo XIV	Los comerciantes estampaban en la palma de mano de los niños impresiones en el papel con tinta para distinguirlos.
	El libro persa del siglo XIV "Jaamehol-Tawarikh" incluye comentarios sobre la práctica de identificar a las personas a partir de sus huellas digitales.
1684	El Dr. Nehemiah Grew publicó observaciones de la piel de la cresta de fricción en el documento "Transacciones filosóficas de la Royal Society of London".
1685	El libro del anatomista holandés Govard Bidloo de 1685, "Anatomía del cuerpo humano" también describió los detalles de la piel de la cresta de fricción.

1686	Marcello Malpighi, profesor de anatomía de la Universidad de Bolonia, observó en su tratado los bordes de las huellas digitales, las espirales y los bucles.
1788	el anatomista y médico alemán JCA Mayer escribió Placas anatómicas de cobre con explicaciones apropiadas Mayer fue el primero en declarar que la piel de la cresta de fricción es única.
1800	La gente ya implementaba las huellas digitales con tinta y papel en las sociedades occidentales para sus diferentes actividades
1858	William Herschel recolectó en Bengala, India, las huellas de toda la mano o el índice y el dedo medio correctos para verificar la identidad de las personas que firman contratos con la East India Company de propiedad británica ³⁹
1870	Alphose Bertillon, jefe del departamento fotográfico de la policía de París desarrolló un sistema antropométrico para identificar criminales, funcionaba mediante la medición de ciertas longitudes y ancho de la cabeza y del cuerpo, y con el registro de las marcas características (tatuajes, cicatrices, etc.). ⁴⁰
1883	1883 - Twain escribe sobre huellas digitales en "La vida en el Mississippi"
1892	Francis Galton publicó su libro Huellas digitales que declaraba por primera vez que las huellas dactilares tenían individualidad y permanencia Vucetich hizo la primera identificación criminal de huellas dactilares llevada a los tribunales ⁴¹
1896	Henry desarrolla un sistema de clasificación de huellas digitales
1900	Azizul Haque desarrolló el primer sistema robusto en India para Sir Edward Henry, Inspector General de Policía en Bengala, India
1903	Las prisiones estatales de Nueva York comienzan a usar huellas digitales El sistema Bertillon se derrumba
1936	Se propone el concepto de usar el patrón de iris para la identificación
1960	El reconocimiento facial se vuelve semiautomático Se crea el primer modelo de producción acústica del habla.
1963	Se publica el trabajo de investigación de Hughes sobre automatización de huellas digitales
1965	Comienza la investigación de reconocimiento de firma automatizada

³⁹ Woodward, John D. Jr. Orleans Nicholas M. Higgins Peter T. Biometrics # ed 1. Washington, D.C: MCGRAW-HILL, 2004. 45 p. ISBN: 978-0072222272.

⁴⁰ Pacheco, Federico G. Jara, Hector. Hacking desde Cero – Seguridad Física y Biometría. En: USERS. 2011. vol. 173. no. 192, p. 66.

1969	El FBI presiona para que el reconocimiento de huellas digitales sea un proceso automatizado
1970	El reconocimiento facial da un paso más hacia la automatización Primero se modelan los componentes conductuales del habla
1974	Los primeros sistemas comerciales de geometría manual están disponibles
1975	FBI financia el desarrollo de sensores y tecnología de extracción de minucias
1976	Se desarrolla el primer prototipo de sistema para reconocimiento de altavoces
1977	Se otorga la patente para la adquisición de información dinámica de firma
1980	se establece NIST Speech Group
1985	Se propone el concepto de que no hay dos iris iguales
	Se otorga la patente para la identificación de la mano.
	Se otorga la patente para el reconocimiento del patrón vascular a Joseph Rice
1986	Se publica el intercambio del estándar de datos de minucias de huellas digitales
1986	Se otorga la patente que indica que el iris se puede usar para identificación
1988	Se implementa el primer sistema de reconocimiento facial semiautomático
	Se desarrolla la técnica Eigenface para el reconocimiento facial
1991	La detección de rostros es pionera, haciendo posible el reconocimiento facial en tiempo real
1992	Se establece el consorcio biométrico dentro del gobierno de los EE. UU.
1993	Se inicia el programa Face Recognition Technology (FERET)
1994	Se patenta el primer algoritmo de reconocimiento de iris.
	Se lleva a cabo la competencia del Sistema Automatizado de Identificación de Huellas Digitales (IAFIS)
	Palm System es comparado
	INSPASS se implementa
1995	El prototipo de Iris está disponible como producto comercial
1996	Se implementa la geometría de la mano en los Juegos Olímpicos
	NIST comienza a realizar evaluaciones anuales de reconocimiento de oradores
1997	Se publica el primer estándar comercial genérico de interoperabilidad biométrica
1998	El FBI lanza COOIS (base de datos forense de ADN)
	Se lanza un estudio sobre la compatibilidad de la biometría y los documentos de viaje de lectura mecánica.

1999	Los principales componentes de IAFIS del FBI entran en funcionamiento
2000	Se lleva a cabo la primera prueba de proveedor de reconocimiento facial (FRVT 2000)
2000	Se establece el programa de licenciatura en biometría de la Universidad de West Virginia
2001	El reconocimiento facial se usa en el Super Bowl en Tampa, Florida
2002	Se establece el comité de normas ISO / IEC sobre biometría
2002	Se forma el Comité Técnico M 1 de Biometría
2002	Palm Print Staff Paper se presenta al Comité de Servicios de Identificación
2003	Comienza la coordinación formal del gobierno de los Estados Unidos de actividades biométricas
2003	La OACI adopta un plan para integrar la biometría en documentos de viaje de lectura mecánica
2003	Se establece el Foro Europeo de Biometría
2004	El programa US-VISIT comienza a funcionar
2004	DOD implementa ABIS
2004	La directiva presidencial exige una tarjeta de identificación personal obligatoria para todo el gobierno para todos los empleados y contratistas federales
2004	Se implementan las primeras bases de datos automatizadas de impresión de palma en todo el estado en los EE. UU.
2004	Comienza el gran desafío de reconocimiento facial
2005	Expira la patente estadounidense para el concepto de reconocimiento del iris
2005	Iris on the Move se anuncia en la Conferencia del Consorcio de Biometría
2008	El gobierno de los EE. UU. Comienza a coordinar el uso de la base de datos biométrica
2010	El departamento de seguridad nacional de EE. UU. Utiliza datos biométricos para la identificación de terroristas
2011	Identificación biométrica utilizada para identificar el cuerpo de Osama Bin Laden
2013	Apple incluye escáneres de huellas digitales en teléfonos inteligentes dirigidos al consumidor

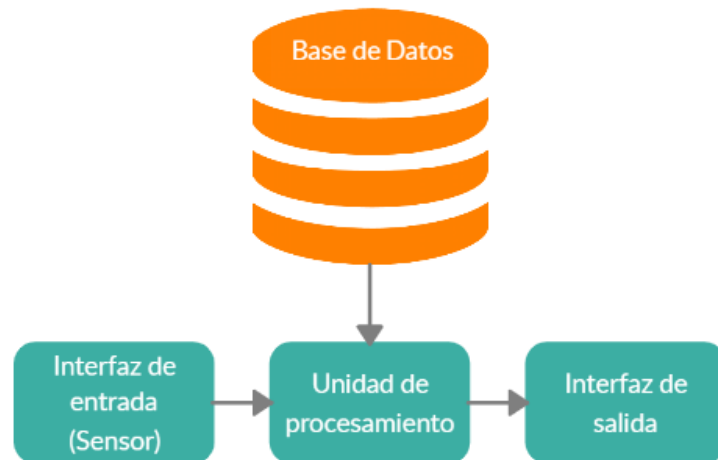
Fuente: Cronología Histórica de la Biometría.⁴²

⁴² Fuente: Mayhew Stephen, History of Biometrics [En Línea]. Ciudad Toronto: Autores: biometricupdate 2020; Disponible en: <https://www.biometricupdate.com/201802/history-of-biometrics-2>

5.2.5 Sistema Biométrico

Son sistema informático que implementa algoritmos de reconocimiento biométrico. Los sistemas biometría se basan en la comparación de una representación digital de un rasgo físico o de comportamiento con uno previamente registrado del mismo rasgo. Por lo tanto, un sistema de reconocimiento biométrico, o simplemente un sistema biométrico, es un sistema de reconocimiento de patrones que reconoce a los individuos en función de sus rasgos biométricos. Estos sistemas son métodos automatizados para verificar o reconocer la identidad de una persona viva sobre la base de algunas características fisiológicas, como la huella digital o el patrón de la cara, o algunos aspectos del comportamiento, como la escritura a mano o los patrones de pulsación de teclas. Un sistema biométrico basado en características fisiológicas es más confiable que uno que adopta características de comportamiento, incluso si este último puede ser más fácil de integrar dentro de ciertas aplicaciones específicas. De acuerdo con la lectura de libro (Handbook of Biometrics) el cual afirma que "Por lo tanto, se puede ver que un sistema biométrico genérico tiene cuatro módulos principales: un módulo sensor; un módulo de evaluación de calidad y extracción de características; un módulo a juego; y un módulo de base de datos. Cada uno de estos módulos se describe a continuación."⁴³

Figura 6. Sistema Biométrico



Fuente: El Autor

⁴³ Anil K. Jain. Patrick Flynn. Arun A. Ross. Handbook of Biometrics # ed 1. New York: ed. Springer Science+Business Media, LLC, 2007 3 p. ISBN: 978-0-387-71041-9.

Módulo de sensor: se requiere un lector o escáner biométrico adecuado para adquirir los datos biométricos sin procesar de un individuo. Para obtener imágenes de huellas digitales, por ejemplo, se puede usar un sensor óptico de huellas digitales para obtener imágenes de la estructura de la cresta de fricción de la punta del dedo. El módulo del sensor define la interfaz hombre-máquina y, por lo tanto, es fundamental para el rendimiento del sistema biométrico.

Evaluación de calidad y módulo de extracción de características: primero se evalúa la calidad de los datos biométricos adquiridos por el sensor para determinar su idoneidad para el procesamiento posterior. Por lo general, los datos adquiridos se someten a un algoritmo de mejora de señal para mejorar su calidad. Sin embargo, en algunos casos, la calidad de los datos puede ser tan pobre que se le pide al usuario que presente nuevamente los datos biométricos.

Módulo de coincidencia y toma de decisiones: las características extraídas se comparan con las plantillas almacenadas para generar puntuaciones de coincidencia. En un sistema biométrico basado en huellas dactilares, se determina el número de minucias coincidentes entre los conjuntos de características de entrada y de plantilla y se informa un puntaje de coincidencia.

La base de datos actúa como el depósito de información biométrica. Durante el proceso de inscripción, el conjunto de características extraídas de la muestra biométrica sin procesar (es decir, la plantilla) se almacena en la base de datos (posiblemente) junto con cierta información biográfica (como nombre, número de identificación personal (PIN), dirección, etc. .) caracterizando al usuario.

5.2.6 Verificación e Identificación

Los sistemas biométricos operan en dos modos básicos:

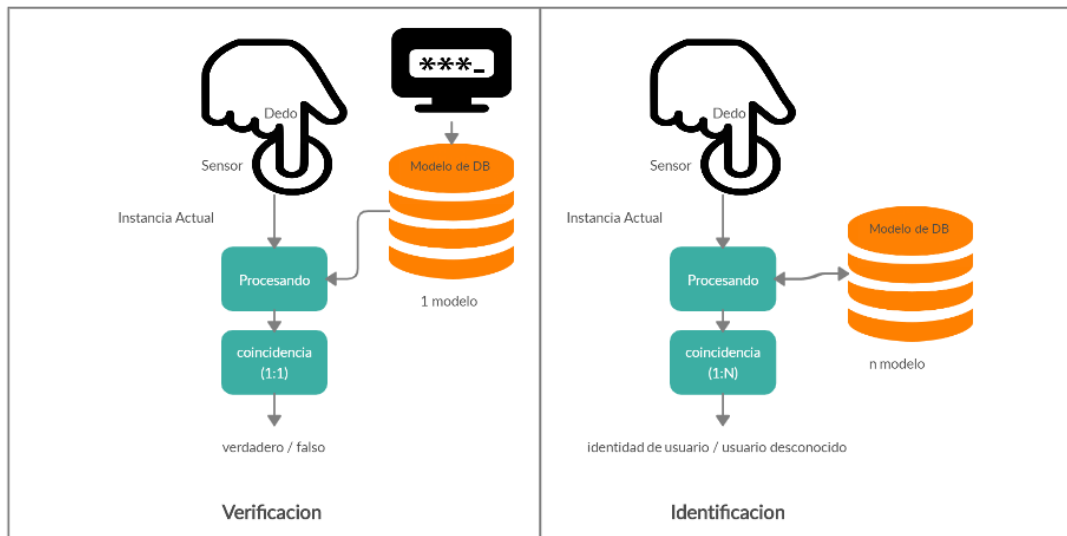
- Verificación ("¿Es esta la persona que dice ser?"). Por ejemplo, una persona afirma que él es Julián Sánchez y ofrece su huella digital; el sistema acepta o rechaza el reclamo basado en la comparación del patrón ofrecido (consulta o entrada) y el patrón registrado (referencia) asociado con la identidad reclamada (Julián Sánchez). Muchas aplicaciones comerciales como el control de acceso físico (p. Ej., Entrada a un edificio) o lógico (p. Ej., Inicio de sesión en la computadora), transacciones en cajeros automáticos bancarios, compras con tarjeta de crédito y gestión de registros médicos son ejemplos de aplicaciones de verificación.
- Identificación ("¿Está esta persona en la base de datos?"). Dada una muestra biométrica de entrada, el sistema determina si este patrón está asociado con cualquiera de un número generalmente grande (por ejemplo, millones) de identidades inscritas.

Hay dos tipos de escenarios de identificación.

- Identificación positiva: la persona afirma que el sistema biométrico lo conoce.
- identificación negativa: la persona afirma que el sistema biométrico no lo conoce.

En ambos escenarios, el sistema confirma o niega la afirmación de la persona al adquirir su muestra biométrica y compararla con todas las plantillas en la base de datos.

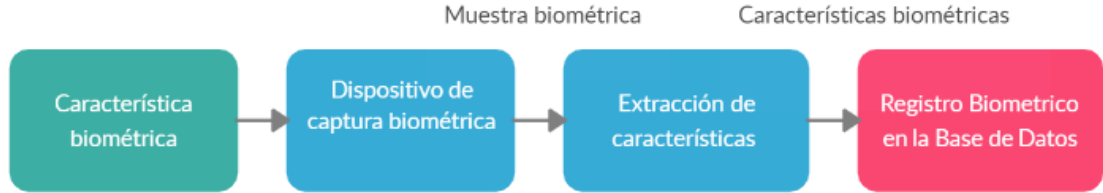
Figura 7. Verificación e Identificación.



Fuente: El Autor.

Antes de poder utilizar un sistema biométrico para verificación / identificación, todos los usuarios deben estar inscritos. El registro implica que el individuo proporcione una muestra de su característica biométrica que utiliza el sistema para generar un modelo (o plantilla) compacto que resuma las características discriminantes. Dependiendo de la aplicación específica, los modelos pueden almacenarse en una base de datos centralizada, pueden distribuirse a través de una red o pueden almacenarse en insignias lanzadas a los usuarios. Cada vez que un individuo requiere una verificación / identificación, él / ella proporciona una nueva muestra de su huella digital y el sistema compara esta instancia actual con los modelos almacenados. Para el registro se debe poder reconocer a una persona por sus características físicas y de comportamiento, primero debe tener lugar una fase de aprendizaje. El procedimiento se denomina inscripción y comprende la creación de un registro de datos de inscripción del sujeto de datos biométricos (la persona que se va a inscribir) y almacenarlo en una base de datos de inscripción biométrica. El registro de datos de inscripción comprende una o múltiples referencias biométricas y datos no biométricos arbitrarios, como un nombre o un número de personal.

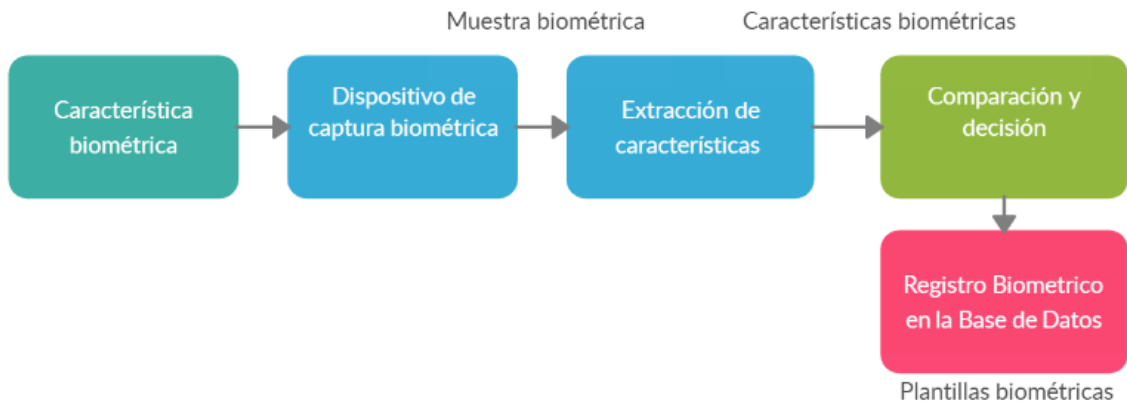
Figura 8. Proceso típico de inscripción interna.



Fuente: El Autor.

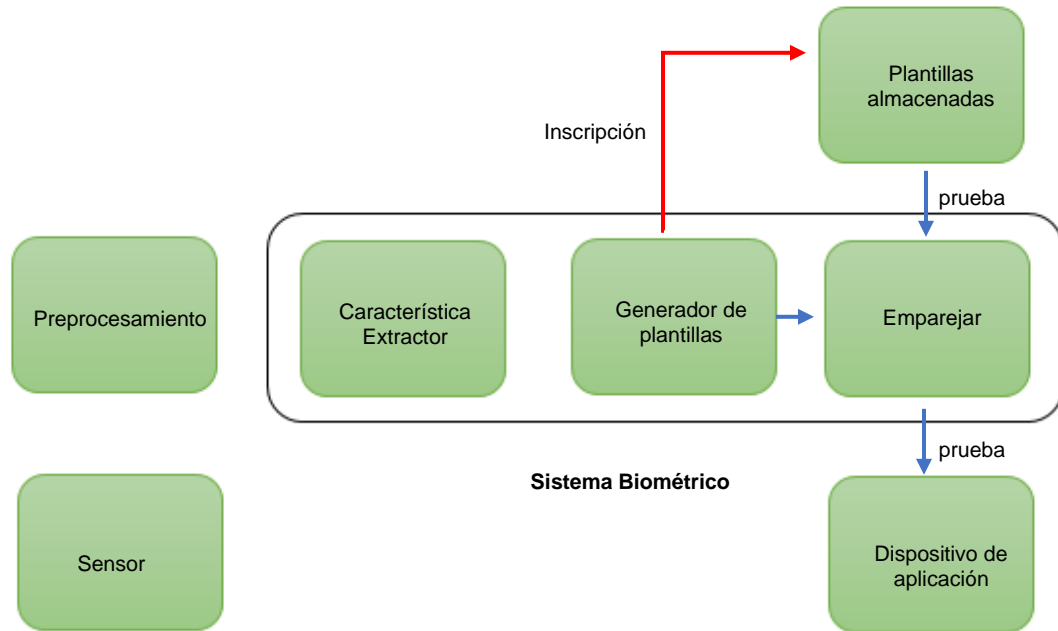
En un sistema de reconocimiento biométrico comúnmente para el reconocimiento, el sujeto de datos biométricos (la persona a ser reconocida) presenta sus características biométricas al dispositivo de captura biométrica que genera una muestra biométrica de reconocimiento a partir de él. A partir de la muestra biométrica de reconocimiento, la extracción de características biométricas crea características biométricas que se comparan con una o múltiples plantillas biométricas de la base de datos de inscripción biométrica. Debido a la naturaleza estadística de las muestras biométricas, generalmente no hay coincidencia exacta posible. Por esa razón, el proceso de decisión solo asignará los datos biométricos sujetos a una plantilla biométrica y confirmará el reconocimiento si la puntuación de comparación excede un umbral ajustable

Figura 9. Sistema de reconocimiento biométrico típico.



Fuente: El Autor.

Figura 10. Elementos principales de un sistema de autenticación biométrica.



Fuente: El Autor.

5.2.7 Medición del rendimiento del sistema biométrico

El sistema básico de medición para la precisión de un sistema biométrico con respecto a estos errores es la tasa de rechazo falso (FRR) y la tasa de aceptación falsa (FAR).

- FRR es la probabilidad de que un usuario genuino sea rechazado como impostor. Cuando la variación dentro de la clase es grande, dos muestras del mismo rasgo biométrico de un individuo pueden no reconocerse como una coincidencia, lo que lleva a un falso error de rechazo.
- FAR es la probabilidad de que un impostor sea reconocido como un individuo genuino. Una coincidencia falsa ocurre cuando dos muestras de diferentes individuos se reconocen incorrectamente como una coincidencia, posiblemente debido a una gran similitud entre clases.

Existe una compensación entre FAR y FRR en cada sistema biométrico. De hecho, tanto FAR como FRR son funciones del umbral del sistema. Si se reduce el umbral para que el sistema sea más tolerante a las variaciones de entrada y al ruido, entonces FAR aumenta. Por otro lado, si se eleva el umbral para hacer que el sistema sea más seguro, FRR aumenta en consecuencia.

5.2.8 Características biométricas

A continuación se detallan en la tabla 3 las características biométricas.

Tabla 3: Características biométricas.

Característica	Biometría
Universalidad:	cada persona debe poseer el rasgo biométrico que se está utilizando. Por ejemplo, todos tienen una cara, pero no es el caso con GAIT biométrico (para usuarios de sillas de ruedas).
Singularidad:	no deben existir dos personas iguales en términos del rasgo biométrico utilizado, es decir, todos deben ser únicos en términos del rasgo biométrico utilizado.
Permanencia:	el rasgo biométrico de un individuo debe ser lo suficientemente invariable durante un período de tiempo con respecto al algoritmo de correspondencia. Un rasgo que cambia significativamente con el tiempo no es un biométrico útil.
Rendimiento:	el rasgo biométrico debe ser invariable con el tiempo, es decir, no debe cambiar con el tiempo.
Medibilidad:	debería ser posible adquirir y digitalizar el rasgo biométrico utilizando dispositivos adecuados que no causen molestias indebidas al individuo. Además, los datos sin procesar adquiridos deben poder procesarse para extraer conjuntos de características representativos.
Burla:	se refiere a la facilidad con que se puede imitar el rasgo de un individuo usando artefactos (por ejemplo, dedos falsos), en el caso de rasgos físicos, y mimetismo, en el caso de rasgos de comportamiento.
Recopilar:	el rasgo biométrico debe ser fácilmente medible.
Rendimiento:	el procesamiento del rasgo biométrico debe ser preciso y rápido.
Seguro:	debe ser seguro y no se puede copiar.
Aceptabilidad:	las personas deben estar dispuestas a aceptar el sistema biométrico.

Fuente: El Autor.

5.2.9 Autenticación basada en biometría

Los sistemas biométricos se dividen en diversos tipos como son los fisiológicos y de comportamientos entre los cuales encontramos patrón de venas, huellas digitales, geometría de la mano, ADN, patrón de voz, patrón de iris, dinámica de firma y detección de rostros.

Figura 11. Tipos de Biometría.

BIOMETRÍA

Fisiológica

Reconocimiento del Rostro

Reconocimiento de la Retina e Iris

Reconocimiento por Voz

Reconocimiento de la Huellas Dactilar

Reconocimiento de la Palma de la Mano

Reconocimiento de Vasculat

Reconocimiento del Oido

Comportamiento

Dinamica de Tecleo

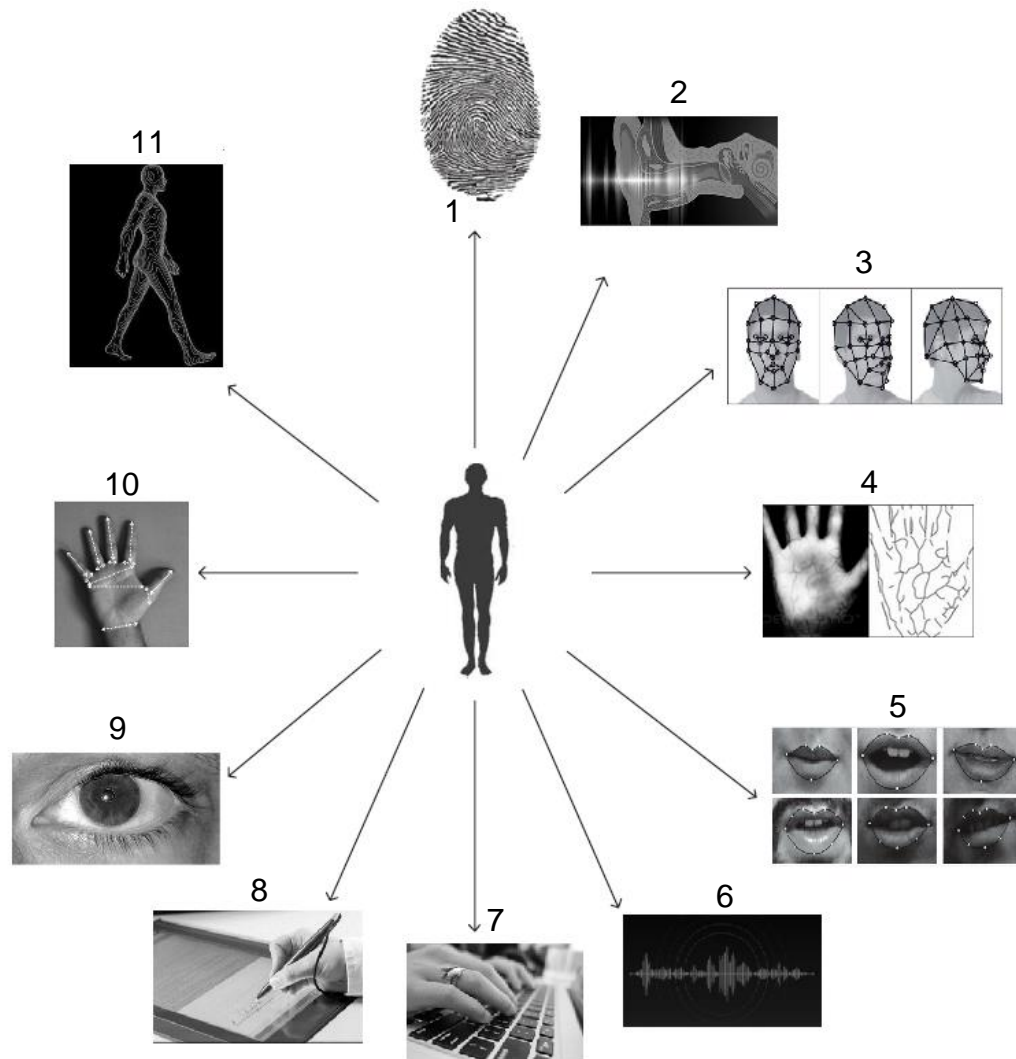
Dinamica de Firma

Estilo de Marcha

Movimientos del Labio

Fuente: El Autor.

Figura 12. Características de Biométricas



Fuente: El Autor

- 1.Reconocimiento de la Huella Dactilar
- 2.Reconocimiento del oído
- 3.Reconocimiento Rostro
- 4.Reconocimiento Vascular
- 5.Movimiento de los labios
- 6.Reconocimiento por Voz
- 7.Dinámica del Tecleo
- 8.Reconocimiento de Firma
- 9.Reconocimiento de la Retina e Iris
- 10.Reconocimiento de la Palma de la Mano
- 11.Estilo de Marcha

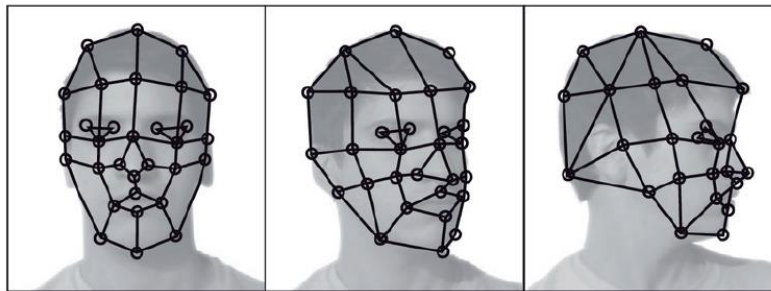
5.2.10 Tipos De Biometría Fisiológicos

Reconocimiento Facial

Es un método para identificar o verificar la identidad de un individuo que usa el rostro. "La cara es un mecanismo no intrusivo de reconocimiento que no exige contacto con el sensor y quizá es, junto con la voz, el método más natural utilizado por las personas para el reconocimiento"⁴⁴. Sin embargo este procedimiento intenta identificar un individuo en función de las características faciales (cuenca del ojo, posición, espacio entre pómulos, barbilla etc. (Figura 1) " así como sus relaciones espaciales, o bien en un análisis global de la misma, representándola como combinación de un conjunto de caras de referencia llamadas canónicas (eigenfaces)"⁴⁵. Los sistemas de reconocimiento facial se pueden usar para identificar personas en fotos, videos o en tiempo real.

Los algoritmos de reconocimiento facial pueden clasificarse en dos grandes categorías según los esquemas de extracción de características para la representación facial: métodos basados en características y métodos basados en apariencia. Las propiedades y las relaciones geométricas, como las áreas, distancias y ángulos entre los puntos de rasgos faciales son utilizado como descriptores para el reconocimiento facial. Por otro lado, los métodos basados en la apariencia consideran las propiedades globales del patrón de intensidad de la imagen de la cara⁴⁶

Figura 13. Reconocimiento Facial



Fuente: Hacking desde Cero - Seguridad Física y Biometría.⁴⁷

⁴⁴ García Ortega, Javier, Alonso Fernández, Fernando. Belmonte Coomonte, Rafael. Biometría y Seguridad # Ed 1. Madrid, Ed: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones, 2008 33 p. ISBN: 978-84-7402-350-3.

⁴⁵ García Ortega, Javier, Alonso Fernández, Fernando. Belmonte Coomonte, Rafael. Biometría y Seguridad # Ed 1. Madrid, Ed: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones, 2008 33 p. ISBN: 978-84-7402-350-3.

⁴⁶ Woodward, John D. Jr. Orlans Nicholas M. Higgins Peter T. Biometrics # ed 1. Washington, D.C: MCGRAW-HILL, 2004 45 p. ISBN: 978-007222272.

⁴⁷ USERS. Hacking desde Cero - Seguridad Física y Biometría En: USERS. 2011. vol. 1. no. 192, p. 69.

Reconocimiento del Retina e iris

En seguridad, el reconocimiento del iris y el escaneo retiniano son tecnologías biométricas de identificación del "ojo", basadas en las características fisiológicas únicas del ojo para identificar a un individuo. Aunque ambos usan alguna parte del ojo para la identificación, estos métodos biométricos tienen un rendimiento muy diferente. "El reconocimiento de iris se ha definido como un método automatizado de identificación biométrica que utiliza técnicas matemáticas de reconocimiento de patrones en imágenes de video de los ojos de un individuo "⁴⁸.

El método automatizado de reconocimiento del iris es relativamente joven, existiendo en patente solo desde 1994. El Iris biométrico es más confiable y preciso como en comparación con otros rasgos biométricos como la huella digital. El rendimiento de estos sistemas que utilizan esta modalidad es prometedor. El reconocimiento se realiza través de una cámara de alta resolución con una sutil iluminación infrarroja que captura imágenes de la estructura del iris. Estas imágenes se convierten en plantillas digitales y se almacenan en una base de datos en el lector.

Estas plantillas biométricas proporcionan una representación matemática del iris, que coincide con una identificación positiva e inequívoca de una persona. Los sistemas de reconocimiento de iris utilizan texturas de iris como identificadores únicos, El iris es un músculo dentro del ojo que regula el tamaño de la pupila, controlando la cantidad de luz que ingresa al ojo. Es la porción coloreada del ojo con coloración basada en la cantidad de pigmento de melatonina dentro del músculo.

El reconocimiento de retina es una técnica biométrica que utiliza patrones únicos en la retina de una persona para su identificación. La retina es la capa de vasos sanguíneos situada en la parte posterior de un ojo. El ojo se coloca frente al sistema a una distancia de captura que varía de 8 cm a un metro. La persona debe mirar una serie de marcadores, vistos a través del ocular, y alinearlos. El ojo está ópticamente enfocado para que el escáner capture el patrón de retina. La retina se escanea con radiación de infrarrojo cercano (NIR 890 nm) y se captura el patrón único de los vasos sanguíneos. El reconocimiento de retina hace uso de la individualidad de los patrones de los vasos sanguíneos. Se ha desarrollado comercialmente desde mediados de la década de 1970. Sandia Laboratory informó una tasa de rechazo falso inferior al 1,0%.⁴⁹

⁴⁸ Mayhew Stephen, Iris Recognition Used to Secure Borders [En Línea]. Ciudad Toronto: Autores: biometricupdate 2020; Disponible en: <https://www.biometricupdate.com/201802/history-of-biometrics-2>

⁴⁹ SpringerLink, Encyclopedia of Biometrics - Retina Recognition [En Línea]. Ciudad: . Autores: Yoichi Seto 2018; Disponible en: https://link.springer.com/referenceworkentry/10.1007%2F978-0-387-73003-5_132

Figura 14. Reconocimiento del Retina e iris



Fuente. Hacking desde Cero - Seguridad Física y Biometría En ⁵⁰

Reconocimiento de Voz

La voz, como muchas otras características que se utilizan para los métodos biométricos, La voz humana es tan única como una huella digital. la voz combina directamente características biológicas y de comportamiento. el sonido que hace un individuo cuando habla se basa en aspectos físicos del cuerpo (boca, nariz, labios, cuerdas vocales, etc.) y puede verse afectado por edad, estado emocional, idioma nativo y condiciones médicas. El reconocimiento por el habla es considerado uno de los más naturales, ya que también es utilizados por el ser humano para identificar a otros. Su estudio data de mediados de los años 60, cuando se estableció que los patrones y las frecuencias con los que cada persona dicen una palabra son únicos.⁵¹ La calidad del dispositivo de grabación y el ruido ambiental también influyen en el reconocimiento. La voz en biometría o "impresión de voz" se presenta como un modelo numérico del sonido. la tecnología de biometría de voz se utiliza con fines de identificación de locutores en diversas industrias, desde los centros de llamadas de los bancos hasta las agencias de investigación de delitos, para identificar a los hablantes de manera confiable en función de su voz.

El rango de posibles aplicaciones La biometría de la voz es más amplia que para otros rasgos biométricos habituales. Podemos distinguir tres tipos principales de aplicaciones que aprovechan la Información biométrica presente en la señal de voz:

- Autenticación de voz (control de acceso, generalmente remota por teléfono) y reconocimiento de fondo (verificación de voz natural)

⁵⁰ USERS. Hacking desde Cero - Seguridad Física y Biometría En: USERS. 2011. vol. 1. no. 192, p. 69.

⁵¹ USERS. Hacking desde Cero - Seguridad Física y Biometría En: USERS. 2011. vol. 1. no. 68, p.

- Detección de altavoces (por ejemplo, detección de listas negras en centros de llamadas o escuchas telefónicas y vigilancia), también conocida como detección de altavoces.
- Reconocimiento forense del hablante (uso de la voz como evidencia en los tribunales de justicia o como inteligencia en investigaciones policiales)⁵²

Figura 15. Reconocimiento por Voz



Fuente: El Autor

Huellas dactilares

La identificación de huellas digitales también se conoce como La dactiloscopia o también la identificación manual es el proceso de comparando dos ejemplos de impresión de piel de cresta de fricción de dedos humanos, palma o dedos de los pies.

Los sistemas de autenticación biométrica basados en huellas digitales se convirtieron en una de las técnicas de autenticación más realizadas, populares y exitosas entre otros métodos de seguridad biométrica para los procesos de identificación y verificación de la identidad de uno. Hoy en día, las huellas digitales se consideran una de las tecnologías biométricas más antiguas.

La huella dactilar se compone de un patrón de crestas y valles situadas en la superficie del dedo, el cual se forma durante los primeros meses de desarrollo fetal y permanece hasta la descomposición tras la muerte. Asimismo, la sudoración, la secreción sebácea y la suciedad de la piel hacen que el contacto del dedo con casi cualquier superficie (metal, cristal, plástico, madera, etc.) produzca en la misma una huella latente que puede ser posteriormente capturada.⁵³

⁵² Anil K. Jain. Patrick Flynn. Arun A. Ross. Handbook of Biometrics # ed 1. New York: ed. Springer Science+Business Media, LLC, 2007 151 p. ISBN: 978-0-387-71041-9.

⁵³ Garcia Ortega, Javier, Alonso Fernandez, Fernando. Belmonte Coomonte, Rafael. Briometria y Seguridad # ed 1. Madrid, ed: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones, 2008 31 p. ISBN: 978-84-7402-350-3.

los sistemas dependen de la capacidad del dispositivo biométrico para distinguir impresiones de crestas y valles hechos por el dedo de un individuo. "Para captar la huella se utilizan sensores como los ópticos, que toman una imagen común de la huella estos son los más usados. También hay capacitivos, que determinan el calor de cada punto basados en la capacidad eléctrica. Otros utilizan ultrasonido o prisma para detectar cambios en la reflectancia de la luz"⁵⁴

Figura 16. Reconocimiento de la Huella Dactilar



Fuente: El Autor

Reconocimiento de la Palma de la Mano

El reconocimiento mediante geometría de la mano se basa en una serie de medidas tales como la forma de la mano, el tamaño de la palma y la longitud y anchura de los dedos, las distancia entre los nudillos, tal como puede observarse en la Figura 4.⁵⁵. Este método se basa en el hecho de que la forma de la mano de una persona difiere de la forma de la mano de otra persona y no cambia después de cierta edad. Muchos sistemas y aplicaciones de seguridad dependen del reconocimiento de la geometría de la mano como una técnica automatizada para la identificación / verificación de sus usuarios legítimos. Este método de autenticación biométrica comenzó a tomar una gran popularidad en varios sectores de seguridad. Fue instalado temprano y utilizado como método biométrico desde finales de los años 60. Uno de los despliegues notables de los sistemas de reconocimiento de manos tuvo lugar en los Juegos Olímpicos de 1996, en los que el acceso físico a la Villa Olímpica fue controlado y protegido mediante sistemas de reconocimiento de geometría de manos. La autenticación biométrica basada en identificar a una persona por la forma de su mano. En su forma básica, se basa en tomar una fotografía de la mano del usuario mientras se coloca sobre una superficie, y después de una detección de contorno, encontrar puntos singulares y tomar medidas entre

⁵⁴ USERS. Hacking desde Cero - Seguridad Física y Biometría En: USERS. 2011. vol. 1. no. 66, p.

⁵⁵ Garcia Ortega, Javier, Alonso Fernandez, Fernando. Belmote Coomonte, Rafael. Briometria y Seguridad # Ed 1. Madrid, Ed: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones, 2008 31 p. ISBN: 978-84-7402-350-3

ellos.⁵⁶ La biometría de la geometría de la mano es una de las facetas más exitosas de la industria global de tecnologías biométricas. La integración funcional, el uso eficiente y los beneficios de seguridad son características clave que impulsan el crecimiento del mercado biométrico de geometría de la mano.

Figura 17. Reconocimiento de la Palma de la Mano



Fuente.

Reconocimiento Vascular

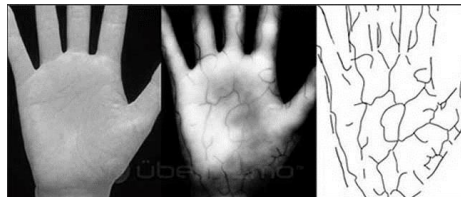
La biometría vascular es una forma relativamente nueva de autenticación biométrica. Identifica a un individuo usando el patrón de venas dentro de los dedos o palmas. Los escáneres vasculares, como un escáner de venas de los dedos o un escáner de venas de la palma de la mano, utilizan luces infrarrojas cercanas combinadas con una cámara especial para capturar patrones de venas. La imagen se convierte en una clave biométrica cifrada o representación matemática y se almacena como una plantilla. Durante la autenticación, la imagen de la vena del dedo se captura, se convierte nuevamente y se compara con la plantilla almacenada del usuario. "Los investigadores han determinado que el patrón vascular del cuerpo humano es exclusivo de un individuo específico y no cambia a medida que las personas envejecen."⁵⁷ La tecnología de las venas de los dedos es similar en principio con la tecnología de huellas digitales. Ambas tecnologías inscriben sujetos y almacenan los patrones de huellas dactilares / venas como plantillas biométricas en la base de datos. Esta base de datos se utiliza para autenticar sujetos que se presentan en los puntos de autenticación.

⁵⁶ SpringerLink, Encyclopedia of Biometrics - Retina Recognition [En Línea]. Ciudad: . Autores: Raul Sanchez-Reillo 2018; Disponible en: https://link.springer.com/referenceworkentry/10.1007%2F978-0-387-73003-5_2451

⁵⁷ Stephen Mayhew, Explainer: Vascular Pattern Recognition [En Línea]. Ciudad Toronto: Autores: biometricupdate 2019; Disponible en: <https://www.biometricupdate.com/201909/biometric-ear-canal-geometry-recognition-developed-by-university-of-buffalo-researchers>

El potencial para el uso de la tecnología se puede rastrear a un trabajo de investigación preparado en 1992 por el Dr. K. Shimizu, en el que discutió la imagen óptica transc corporal y las posibles aplicaciones de escaneo óptico CT. El primer artículo sobre el uso de patrones vasculares para el reconocimiento biométrico se publicó en 2000. Ese documento describió la tecnología que utilizaba vasos sanguíneos subcutáneos en el dorso de la mano, que fue el primero en convertirse en un sistema de reconocimiento de patrones vasculares disponible comercialmente. La investigación adicional mejoró esa tecnología e inspiró la investigación adicional y la comercialización de sistemas basados en los dedos y la palma.⁵⁸

Figura 18. Reconocimiento Vascular.



Fuente. handresearch, Fujitsu gives Biometrics a Hand.⁵⁹

Reconocimiento del oído

Cada vez más, la seguridad biométrica, utiliza las características de nuestros cuerpos para verificar quiénes somos, se está volviendo más común. Otro mecanismo de autenticación es por medio de un individual en función de la forma de la oreja y la estructura del tejido cartílago del pinna.

Asimismo, "La forma de la oreja así como su estructura de cartílagos es un rasgo que permite distinguir entre personas. No es un rasgo muy distintivo, pero su captura es bastante sencilla y no sufre los problemas de iluminación o del fondo que tiene el reconocimiento de cara, puesto que la propia cabeza alrededor de la oreja actúa como fondo, permitiendo detectarla de un modo fiable."⁶⁰ Las orejas se caracterizan por una estructura estable que se conserva desde el nacimiento hasta la vejez.

Investigadores de la Universidad de Buffalo están desarrollando un sistema biométrico de reconocimiento de geometría del canal auditivo para autenticar a los

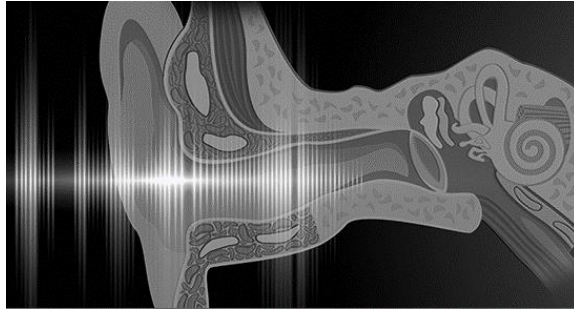
⁵⁸ Stephen Mayhew, Explainer: Vascular Pattern Recognition [En Línea]. Ciudad Toronto: Autores: biometricupdate 2019; Disponible en: <https://www.biometricupdate.com/201909/biometric-ear-canal-geometry-recognition-developed-by-university-of-buffalo-researchers>

⁵⁹ handresearch, Fujitsu gives Biometrics a Hand [En Línea]. Ciudad: . Autores: Robert Vamosi 2008; Disponible en: <http://www.handresearch.com/news/fujitsu-gives-biometrics-a-hand.htm>

⁶⁰ Garcia Ortega, Javier, Alonso Fernandez, Fernando. Belmonte Coomonte, Rafael. Biometría y Seguridad # Ed 1. Madrid, Ed: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones, 2008 38 p. ISBN: 978-84-7402-350-3

usuarios de teléfonos inteligentes con audífonos⁶¹ La tecnología puede identificar una oreja una y otra vez con una precisión del 99.6 por ciento. Funciona al desatar un algoritmo de producción de rayos en una imagen para buscar características curvas. Cuando un rayo encuentra uno, el software dibuja sobre la pieza y repite el análisis. En unos pocos cientos o miles de ciclos, pinta limpiamente la oreja más que cualquier otra estructura de la cara.

Figura 19. Reconocimiento del oído.



Fuente. Ear canal biometrics shows promise as authenticator.⁶²

5.2.11 Tipos De Biometría Conductual

La biometría del comportamiento es aquella que mide los patrones de comportamiento en oposición a (o además de) las características físicas. Estos son solo algunos ejemplos de biometría conductual.

Dinámica de tecleo

La dinámica del golpe de teclado es un rasgo biométrico que, según algunas hipótesis, puede ser distintivo de los individuos. De hecho, existe una larga tradición de reconocer a los operadores de código Morse por sus "puños", los patrones distintivos que las personas utilizan para crear mensajes. Sin embargo, la dinámica de la pulsación de teclas se ve fuertemente afectada por el contexto, como el estado emocional de la persona, su postura, el tipo de teclado, etc.

Es posible pensar que cada persona escribe con un teclado de manera diferente, mostrando diferencias en el tiempo transcurrido entre cada pulsación o el tiempo

⁶¹ Chris Burt, Biometric ear canal geometry recognition developed by University of Buffalo researchers [En Línea]. Ciudad Toronto: Autores: biometricupdate 2019; Disponible en: <https://www.biometricupdate.com/201909/biometric-ear-canal-geometry-recognition-developed-by-university-of-buffalo-researchers>

⁶² SecureIDNews, Ear canal biometrics shows promise as authenticator, patent filed [En Línea]. Ciudad: Georgia. Autores: AVISIAN Staff 2019; Disponible en: <https://www.secureidnews.com/news-item/ear-canal-biometrics-shows-promise-as-authenticator-patent-filed/>

que se tiene pulsada cada tecla. No es un rasgo de muy alta capacidad discriminativa y puede ser variable al tratarse de una característica de comportamiento. Por el contrario, puede obtenerse de un modo no intrusivo (simplemente monitorizando al usuario) y al poder observarse durante un periodo de tiempo más o menos largo, permite verificar la identidad del usuario a lo largo de todo ese tiempo. Por ejemplo, si en un momento dado se observan cambios importantes en la dinámica de tecleo, puede considerarse que el usuario no es el mismo y a continuación, bloquear el sistema.⁶³

Figura 20. Dinámica del Tecleo.



Fuente. AI-based typing biometrics might be authentication's next big thing.⁶⁴

Reconocimiento de Firma

La autenticación de un individuo mediante el análisis del estilo de escritura a mano, en particular la firma "El reconocimiento por firma es poco problemático y bien aceptado, dado que estamos muy habituados a usarla como método de reconocimiento. El proceso de análisis se realiza en dos áreas; la firma en si y el modo en el que se lleva a cabo. Los datos tomados son la velocidad, la precisión, la dirección, el largo del trazo y las áreas donde se levanta el lápiz "⁶⁵

La firma de una persona, así como la manera en que realiza dicha firma, es una propiedad característica de cada individuo. La firma es un mecanismo de validación de identidad usado desde hace siglos en entornos legales, gubernamentales y en transacciones comerciales. Es por ello que su aceptación como mecanismo de reconocimiento es muy alta. Por el contrario, la firma es un rasgo de comportamiento que va cambiando con el tiempo, que depende del estado físico y emocional, y que precisa que el individuo coopere y realice el acto

⁶³ Garcia Ortega, Javier, Alonso Fernandez, Fernando. Belmonte Coomonte, Rafael. Biometria y Seguridad # ed 1. Madrid, ed: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones, 2008 38 p. ISBN: 978-84-7402-350-3

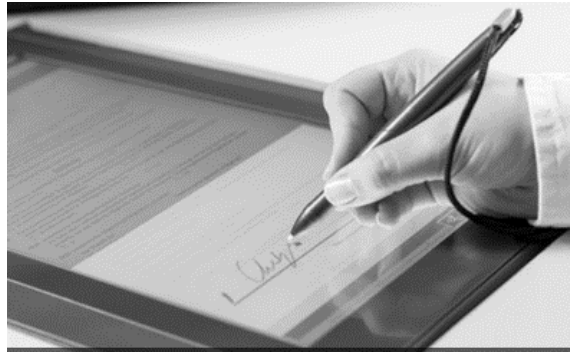
⁶⁴ csoonline, AI-based typing biometrics might be authentication's next big thing [En Línea]. Ciudad: Georgia. Autores: Lucian Constantin Staff 2017; Disponible en: <https://www.secureidnews.com/news-item/ear-canal-biometrics-shows-promise-as-authenticator-patent-filed/>

⁶⁵ USERS. Hacking desde Cero - Seguridad Física y Biometría En: USERS. 2011. vol. 1. no. 66, p.

de firmar. Incluso varias firmas hechas en un corto espacio de tiempo pueden diferir sustancialmente. Asimismo, la firma es susceptible de ser imitada⁶⁶

El inconveniente principal es que nunca se firma dos veces iguales, por lo que debe ajustarse los patrones.⁶⁷

Figura 21. Reconocimiento de Firma.



Fuente. Biometrics ⁶⁸

Estilo de Marcha

El reconocimiento de la marcha es el proceso en el que las características del movimiento humano, Se define como la identificación de una persona a través del patrón producido al caminar. La marcha tiene ventajas particulares sobre otros datos biométricos: se puede usar a distancia, no utiliza habilidades adicionales por parte del sujeto y se puede realizar sin la conciencia del sujeto o su participación. No se supone que la marcha sea muy distintiva, pero es suficientemente discriminatoria para permitir la verificación en algunas aplicaciones de baja seguridad.

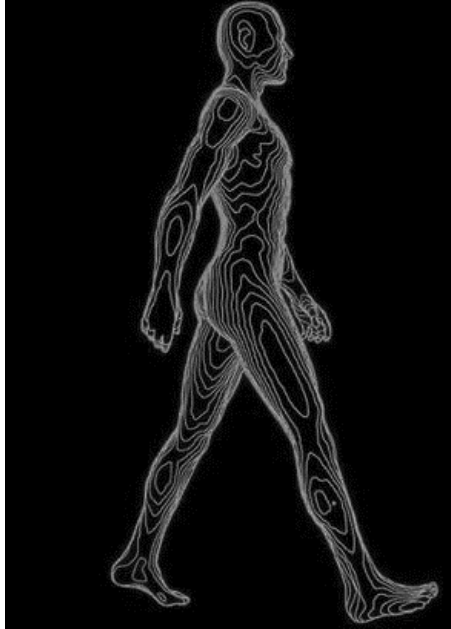
El modo de andar es una característica peculiar de cada persona. A pesar de que no es muy distintivo, es muy fácil de capturar (basta una cámara de vídeo) y no es necesaria la cooperación del usuario. Pensemos que en sistemas de control de acceso en los que existan cámaras ya instaladas, será un rasgo adicional fácilmente obtenible. No obstante, al ser una característica de comportamiento, está sujeta a variaciones con el tiempo debido a cambios en el peso, vestimenta, lesiones, enfermedades, estados de embriaguez, etc.

⁶⁶ Garcia Ortega, Javier, Alonso Fernandez, Fernando. Belmonte Coomonte, Rafael. Biometria y Seguridad # ed 1. Madrid, ed: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones, 2008 38 p. ISBN: 978-84-7402-350-3

⁶⁷ USERS. Hacking desde Cero - Seguridad Física y Biometría En: USERS. 2011. vol. 1. no. 66, p.

⁶⁸ biomed4n6, Biometrics [En Línea]. Ciudad: . Autores: biomed4n6 2018; Disponible en: <http://biomed4n6.uniroma3.it/research/biometrics.html>

Figura 22. Estilo de Marcha



Fuente. Gait biometrics shows promise⁶⁹

Movimiento de los labios

En la identificación por medio de movimientos de labios, una persona dice, en general al reconocimiento, palabras ante establecidas, en que el movimiento de la boca se graba con una cámara como una consecuencia de película. Las características que se usan para la identificación son el ancho de boca y la apertura de boca en sonidos determinados. Para el aumento de la exactitud procesal el color de labios puede ser usado como una característica más.

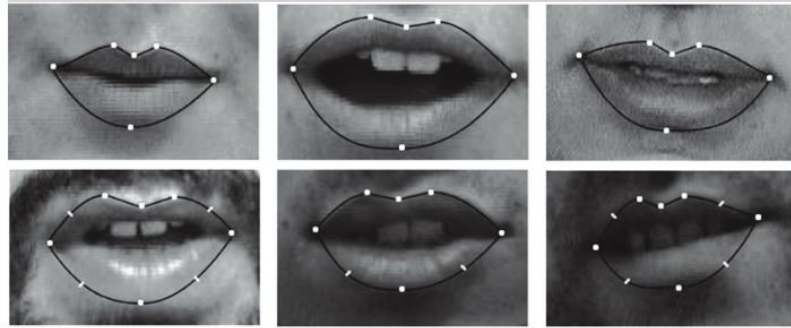
El movimiento de los labios es una característica de comportamiento que analiza los movimientos a medida que el individuo va hablando. Puede combinarse muy fácilmente con la voz y/o con una secuencia de imágenes (vídeo) de la cara.⁷⁰ Esta triple combinación da lugar a un sistema muy difícil de vulnerar y que solamente necesita una cámara de vídeo con micrófono que capture al usuario hablando. Al igual que los sistemas de voz, puede trabajar en modo dependiente de texto o en modo independiente de texto. Asimismo, para la captura de los labios, como para la cara, pueden usarse cámaras con luz visible o con luz infrarroja.⁷¹

⁶⁹ Homeland Security News Wire, Gait biometrics shows promise [En Línea]. Ciudad: New York. Autores: Homeland Security News Wire 2011; Disponible en: <http://www.homelandsecuritynewswire.com/gait-biometrics-shows-promise>

⁷⁰ (<http://catedraisdefe.etsit.upm.es/webNueva/index.html>, 2020)

⁷¹ Garcia Ortega, Javier, Alonso Fernandez, Fernando. Belmonte Coomonte, Rafael. Briometria y Seguridad # Ed 1. Madrid, Ed: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones, 2008 38 p. ISBN: 978-84-7402-350-3

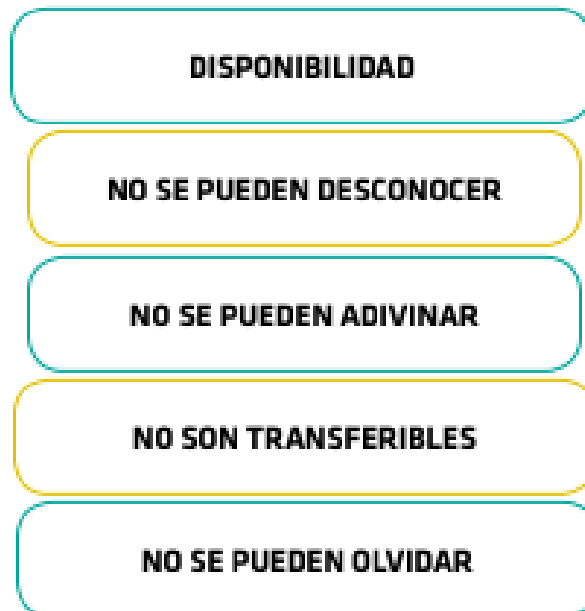
Figura 23. Movimientos de los Labios



Fuente. Multimodal Person Recognition for Human-Vehicle Interaction. Multimedia ⁷²

5.2.12 Ventajas de la Biometría.

Figura 6. Ventajas de Biometría.



Fuente: El Autor.

⁷² Erzin, Engin & Yemez, Y. & Tekalp, A. & Ercil, Aytul & Erdogan, Hakan & Abut, H.. (2006). Multimodal Person Recognition for Human-Vehicle Interaction. Multimedia, IEEE. 13(2). 18 - 31. 10.1109/MMUL.2006.37.

5.2.13 Desventajas de la Biometría.

Al igual que con cualquier nuevo sistema o tecnología, siempre habrá ventajas y desventajas, y ambas partes deben ser examinadas en detalle antes de que una empresa o individuo continúe implementando.

Los inconvenientes que los sistemas de autenticación biométrica tienen que ver con la privacidad de las personas, los métodos de identificación tradicionales como las contraseñas, PIN, patrones, llaves y tarjetas, entre otros se pueden cambiar, al capturar un rasgo físico de un individuo como una huella dactilar esta no se puede modificar, por lo que plantea un problema de privacidad a largo plazo.

De igual forma los rechazos y las aceptaciones falsas aún pueden ocurrir en algunas tecnologías, los sistemas biométricos son más difíciles de adaptar para las personas mayores o con discapacidades. Asimismo, Si un usuario tiene lesiones pueden hacer que una autenticación biométrica no funcione correctamente: Ejemplo (Quemadura, Cortadas en un dedo podría dificultar el registro y la lectura en el lector biométrico).

También se presenta inconvenientes cuando las personas sienten temor por tocar un dispositivo que otra persona ya toco, lo que podría provocar la propagación de enfermedades, asimismo la Superintendencia de Industria y Comercio del territorio nacional emitió un comunicado CIRCULAR EXTERNA No. 002 (24 DE MARZO 2020) Mediante el Decreto 417 del 17 de marzo de 2020 se declaró el Estado de Emergencia Económica, Social y Ecológica para conjurar la crisis e impedir la extensión de los efectos del virus COVID-19 (Coronavirus). Asimismo, la Resolución 385 del 12 de marzo de 2020 del Ministerio de Salud y Protección Social decretó la emergencia sanitaria.⁷³

Huella Dactilar:

Desventajas: aunque el sistema de reconocimiento de huellas digitales tiene varias ventajas, este sistema tiene algunas desventajas. Este sistema biométrico tiene cierta complejidad en la obtención de imágenes de alta calidad de imágenes de patrones de dedos. Debido a la suciedad, cortes, rasgaduras y problemas de desgaste que pueden afectar fácilmente las crestas y las minucias de la yema del dedo.

Facial:

Desventajas: varios factores afectan el rendimiento general del sistema biométrico de reconocimiento facial. Por ejemplo, la calidad o resolución de las fotos recopiladas para cada individuo, las condiciones de luz, los ángulos de rotación de

⁷³ (SUPERINTENDENTE DE INDUSTRIA Y COMERCIO , 2020)

la cara, etc. Además, las diferentes expresiones faciales plantean algunos desafíos para el reconocimiento automático de la identidad de las personas, como expresiones tristes, felices, enojadas y otras.

Retina:

Desventajas: varios factores afectan el rendimiento y puede ser incomodidad para el usuario debido a los grandes esfuerzos de los contribuyentes para capturar sus vasos retinianos. Sin embargo, la biometría basada en el escaneo retiniano tiene algunos factores médicos que pueden afectar la precisión del proceso de autenticación, como la presión arterial alta. Además, diferentes documentos abordan otras condiciones que pueden disminuir el rendimiento del escaneo retiniano, como usar anteojos, lentes, etc.

Palma de la Mano

Desventajas: Requiere un dispositivo de hardware especial para escanear la geometría de la mano. Dicho escáner debe ser tridimensional para obtener información completa de la palma. En contraste con otros dispositivos que toman solo unos pocos dedos de información. Por lo tanto, este método se considera un costoso sistema de autenticación biométrica. Además, existen algunas limitaciones que pueden afectar la extracción de información de la palma, como el uso de algunas joyas, etc. Otro inconveniente del escaneo manual es el gran espacio que se requiere para almacenar la información escaneada de la geometría de la palma.

Oído

Desventajas: al igual que otros esquemas de reconocimiento biométrico, la autenticación biométrica basada en el oído tiene sus propios inconvenientes. Este método aún no ha alcanzado un nivel notable de seguridad. Una de las desventajas del reconocimiento del oído son las características distintivas simples del oído que no pueden proporcionar un fuerte establecimiento de la identidad de un individuo.

5.3. MARCO LEGAL

5.3.1 Entidades

- **ISO:** La Organización Internacional de Normalización (ISO), junto con la Comisión Electrotécnica Internacional (IEC), ha creado conjuntamente un comité llamado Comité Técnico Conjunto 1 (JTC), responsable de la creación de estándares de tecnología de la información. En 2002, se creó un subcomité SC 37 sobre biometría dentro del JTC 1 para desarrollar estándares biométricos internacionales.

SC 37 ha organizado su trabajo en seis grupos de trabajo (WG) que reúnen a expertos de dominio de todos los organismos nacionales participantes:

- WG 1: Vocabulario y definiciones biométricos armonizados;
- WG 2: Interfaces técnicas biométricas;
- WG 3: Formatos de intercambio de datos biométricos;
- WG 4: Arquitectura y perfiles funcionales biométricos;
- WG 5: Pruebas biométricas e informes;
- WG 6: Aspectos cruzados jurisdiccionales y sociales.

El SC 37 se vincula con estos subcomités para controlar que el trabajo relevante se puede controlar y se evite la replicación.

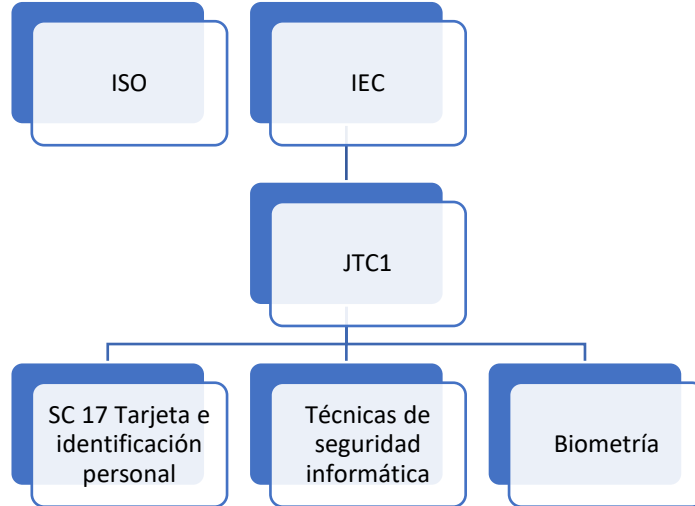
TC 68 - Servicios financieros;
SC 17: tarjetas inteligentes;
SC 27: seguridad de TI.

- **Consortio BioAPI:** El Consorcio BioAPI es un grupo de más de 90 organizaciones cuyo objetivo es fomentar y promover el crecimiento de la tecnología biométrica mediante el desarrollo de una interfaz de programación de aplicaciones (API) en toda la industria. La API del consorcio define como una aplicación de software interactúa con un dispositivo de verificación biométrica; es compatible con diferentes sistemas operativos, aplicaciones de proveedores y tipos de tecnologías biométricas que incluyen reconocimiento de voz y facial, escaneos de iris y retina, verificación de firma, geometría de lóbulos de manos y oídos y análisis de huellas digitales. El marco BioAPI desarrollado por este grupo ha pasado de ser un estándar informal a un estándar publicado por SC 37
- **NIST:** El Instituto Nacional de Estándares y Tecnología. El primer estándar biométrico fue creado por el Laboratorio de Tecnología de la Información

(ITL) de NIST en 1986 para facilitar el intercambio de imágenes de huellas digitales entre las agencias de aplicación de la ley y desde entonces ha desempeñado un papel importante en el desarrollo de estándares internacionales y de EE. UU.

- **OASIS:** La Organización para el Avance de los Estándares de Información Estructurada. La experiencia y la aceptación de OASIS como organización para crear estándares relacionados con la Web lo han convertido en un colaborador natural en la creación de estándares biométricos para arquitecturas web.
- **ITU-U : INTERNATINAL TELECOMMUNICATION UNION:** incursionó en las normas biométricas en 2001 como parte de su trabajo en seguridad de las telecomunicaciones. El primer estándar, X.1081, definió un marco multimodal que se puede utilizar para clasificar, identificar y abordar los aspectos de seguridad de la biometría en un sistema telebiométrico
- **M1** es el Grupo de Asesoramiento Técnico (TAG) de los Estados Unidos para el SC 37. Fue establecido en junio de 2002 y es responsable de formular las posiciones de los EE. UU. En el SC 37 donde tiene el voto de los EE. UU. El personal de sus organizaciones miembros representa estos puestos en SC 37. Es notable porque es una organización de desarrollo de normas por derecho propio: sus normas se publican en los EE. UU. Como normas INCITS 2, pero se pueden comprar en todo el mundo. El trabajo de M1 a menudo se ha contribuido al SC 37 como documentos base para sus actividades de desarrollo.

Figura 25: Estandarización en biometría.



Fuente: El Autor

Figura 26: Agencias especializadas de la ONU



Fuente: El Autor

Figura 27: consorcios internacionales



Fuente: El Autor

5.3.2 Estándares Internacionales

Tabla 4: Estándares ITU-T

Estándares ITU-T	
Nombre	Descripción
ITU-T X.1081	modelo multimodal que puede usarse como marco para identificar y especificar aspectos de seguridad de la tele biometría
ITU-T X.1084	Marco general para protocolos de autenticación de telebiometría
ITU-T X.1085	Pautas específicas para protocolos de autenticación de telebiometría
ITU-T X.1086	Pautas para contramedidas para mejorar la seguridad y la privacidad en telebiometría
ITU-T X.1087	Directrices para preservar la confidencialidad e integridad de los datos biométricos.
ITU-T X.1088	Marco para la generación y protección de claves digitales biométricas
ITU-T X.1089	Marco para implementar un sistema biométrico con emisión de certificados, gestión, uso y revocación

Fuente: El Autor

Tabla 5: Pruebas de rendimiento biométrico y estándares de informes

Pruebas de rendimiento biométrico y estándares de informes		
Nombre	Publicada	Descripción
19795-1:	2006	Parte 1: Principios y marco
19795-2:	2007	Parte 2: Pruebas de metodologías para tecnología y evaluación de escenarios
TR 19795-3:	2007	Parte 3: Pruebas específicas de modalidades
TR 19795-4:	2008	Parte 4: Pruebas de rendimiento de interoperabilidad
TR 19795-5:	2009	Parte 5: Escenario de control de acceso y esquema de calificación
TR 19795-5:	2011	Parte 7: Prueba de algoritmos de comparación biométrica en tarjeta

Fuente: El Autor

Tabla 6: Lista de estándares de calidad de muestra e informes técnicos

Lista de estándares de calidad de muestra e informes técnicos		
Nombre	Publicada	Descripción
ISO/IEC 29794-1:	2009	Parte 1: Marco de calidad de la muestra biométrica
ISO/IEC 29794-4:	2010	Parte 4: Datos de imagen del dedo (Informes técnicos)
ISO/IEC 29794-5:	2010	Parte 5: Datos de imagen facial (Informes técnicos)
ISO/IEC 29794-6		Parte 6: Imagen de iris (en curso)

Fuente: El Autor

Tabla 7: Estándares de prueba de conformidad

Estándares de prueba de conformidad		
Pruebas de conformidad para la interfaz de programación de aplicaciones biométricas (BioAPI)		
Nombre	Publicada	Descripción
ISO/IEC 24709-1:	2007	Parte 1: Marco de calidad de la muestra biométrica
ISO/IEC 24709-2:	2007	Parte 2: Afirmaciones de prueba para proveedores de servicios de biometría BioAPI
ISO/IEC 24709-1:	2011	Parte 3: Afirmaciones de prueba para el marco biométrico de BioAPI
Metodología de prueba de conformidad para formatos de intercambio de datos definidos en ISO / IEC 19794		
ISO/IEC 29109-1:	2009	Parte 1: Metodología de prueba de conformidad generalizada
ISO/IEC 29109-2:	2010	Parte 2: Datos de minucias de dedo
ISO/IEC 29109-4:	2010	Parte 4: Datos de imagen del dedo
ISO/IEC 29109-5:	2011	Parte 5: Datos de imagen facial
ISO/IEC 29109-10:	2010	Parte 10: Datos de silueta de geometría de mano

Fuente: El Autor

Tabla 8: Interfaces técnicas

		Interfaces técnicas
Nombre	Publicada	Descripción
19784-1:	2006	Interfaces de programación de aplicaciones biométricas - Parte 1 Especificación BioAPI
19784-1: - Amd 1:	2007	Especificación BioGui
19784-1: - Amd 1:	2009	Marco - BioApi gratuito
19784-1: - Amd 1:	2010	Soporte para el intercambio de certificados y aserciones de seguridad y otros aspectos de seguridad
19784-2:	2007	Interfaces de programación de aplicaciones biométricas - Parte 2: Interfaces de proveedor de funciones de archivo Biométrico
19784-4:	2011	Interfaces de programación de aplicaciones biométricas - Parte 2: Interfaces del proveedor de funciones del sensor biométrico
19785-1:	2006	Marco común de formatos de intercambio biométrico - Parte 1: Especificación del elemento de datos
19785-2:	2006	Marco de formatos comunes de intercambio biométrico - Parte 2: Procedimientos para la operación de la Autoridad de registro biométrico
19785-3:	2007	Marco común de formatos de intercambio biométrico - Parte 3: Especificaciones de formatos de usuario
19785-4:	2010	Marco común de formatos de intercambio biométrico - Parte 4: Especificaciones de formatos de bloque de seguridad
24708:	2008	Protocolo de interconexión BioAPI

Fuente: El Autor

Tabla 9: Estandarización de interfaz

Estandarización de interfaz	
ISO/IEC 19784 BioAPI	ISO / IEC 19784 es un estándar multiparte que define interfaces de programación de aplicaciones para productos biométricos. Sus estructuras de datos y llamadas a funciones permiten que los componentes de un sistema biométrico sean proporcionados por diferentes proveedores en apoyo de un modelo de autenticación de alto nivel e independiente de la modalidad
ISO/IEC 24709 BioAPI Conformance Testing	Este conjunto de estándares se encuentra actualmente en desarrollo. Los documentos establecen procedimientos para probar la conformidad de las implementaciones de ISO / IEC 19784-x BioAPI.
ISO/IEC 19785 CBEFF	El estándar del Marco Común de Formatos de Intercambio Biométrico (CBEFF) establece un medio para definir estructuras estándar para registros de información biométrica (BIR)
ISO/IEC 24741 Biometrics Tutorial	Este proyecto está desarrollando un informe técnico (es decir, un documento redactado de manera similar pero sin los requisitos normativos de un estándar) que cubrirá las propiedades de un biométrico, la historia de la biométrica, las principales modalidades y tecnologías, una vista funcional de los sistemas a nivel de componente, descripciones de los procesos de inscripción, verificación e identificación, y material adicional sobre estándares, aplicaciones, pruebas y privacidad
ISO/IEC 24742 Multimodal and Other Biometric Fusion	Este informe técnico articula los conceptos propios de la fusión en biometría. Describe los diversos niveles de fusión (muestra, característica, puntaje, rango y decisión) e incluye material sobre correlación, normalización de puntaje, datos de caracterización.

Fuente: El Autor

Tabla 10: Estándares de formato de datos

Estándares de formato de datos			
<p>La estandarización de las estructuras de datos para el uso interoperable de datos biométricos entre organizaciones es en muchos aspectos, la parte más grande e importante de los esfuerzos de estandarización biométrica. El objetivo es el mismo en ambos casos: intercambio de datos perfecto, correcto y efectivo entre los productos de múltiples proveedores. El Grupo de trabajo 3 del SC 37 desarrolla estándares de formato de intercambio de datos biométricos</p>			
ISO/IEC	Publicada	Título de la norma	Descripción
19794-1	2007	Marco de referencia	Sirve como marco para las partes posteriores del conjunto de estándares de formato de intercambio de datos biométricos de 19794. Establece el propósito y el papel de esos estándares, define términos básicos como tipo y plantilla biométricos, y aborda los aspectos comunes asociados con la adquisición, procesamiento y uso de muestras
19794-2	2005	Datos de minucias de los dedos	Define un contenedor BDB para puntos de minucias. Como se muestra en la Figura 24.3, se permiten tres codificaciones, un formato de "registro" predeterminado y dos formatos de "tarjeta" para tarjetas inteligentes (por ejemplo, ISO / IEC 7816-11) y otras credenciales.
19794-3	2006	Datos espectrales del patrón de dedo	Codifica datos de crestas de huellas digitales mediante la aplicación de una descomposición espectral a cada celda de una matriz. Las celdas pueden superponerse y ser rectangulares.
19794-4	2006	Datos de imagen de dedo	Define un contenedor para imágenes ráster 2D de dedos y palmas en escala de grises
19794-5	2005	Datos de imagen facial	Define una estructura de datos para el almacenamiento de imágenes faciales. El registro incluye campos para expresión, color de ojos, color de cabello y género. Opcionalmente permite la inclusión de puntos de características ISO / IEC 14496-2 MPEG 4.
	Norma	Condiciones para tomar fotografías para datos de imágenes faciales	

	Norma	Formato de intercambio de datos de imagen de cara tridimensional	
19794-6	2005	Datos de imagen de iris	Define una estructura de datos para el almacenamiento de una imagen ráster 2D rectilínea convencional de un ojo o una representación de coordenadas polares de los datos del iris 4.
19794-7	2007	Firma / firma de datos de series de tiempo	Define un contenedor para registrar los datos capturados cuando una persona escribe una firma o un signo personal en una tableta digitalizadora o con un sistema avanzado de pluma
19794-8	2006	Datos esqueléticos del patrón de dedo	Define un contenedor para la estructura esquelética de las crestas de una huella digital y sus puntos minuciosos
19794-9	2007	Datos de imagen vascular	Establece un formato de registro simple para imágenes ráster 2D convencionales de la parte frontal y posterior de los dedos o las manos.
19794-10	2007	Datos de silueta de geometría de mano	Establece un contenedor para la información de silueta extraída de imágenes de manos. Los datos están representados por una codificación en cadena de Freeman del contorno de la silueta de la mano binaria vista desde arriba y desde el costado
19794-11	2013	Firma procesada / Firma dinámicos / Datos	Especifica un formato de intercambio de datos para datos de comportamiento de firma / signo procesados extraídos de una serie de tiempo, capturados utilizando dispositivos como tabletas digitalizadoras, dispositivos informáticos basados en bolígrafo o bolígrafo avanzado sistemas
19794-12	WD	Datos de identidad facial	
19794-13	2018	Datos de reconocimiento de altavoz de de	Especifica un formato de intercambio de datos que se puede utilizar para almacenar, grabar y transmitir datos de voz humana (voz) acústica digitalizados que se supone que provienen de un solo altavoz grabado en una sola sesión

Fuente: El Autor

Tabla 11: Pruebas de rendimiento

Pruebas de rendimiento			
ISO/IEC	Publicada	Título de la norma	Descripción
19795-1	2006	Principios y marco	El estándar proporciona una gran cantidad de material sobre pruebas biométricas e informes. Es una evolución de un documento seminal de mejores prácticas de evaluación biométrica [10]
19795-2	2007	Evaluación de tecnología y escenarios	El estándar regula dos tipos de pruebas biométricas en su mayoría distintas: pruebas de tecnología (con cuerpos de prueba fuera de línea) de la capacidad algorítmica central de los componentes y pruebas de escenario (con una población viva) de productos destinados a ser predictivos de la operación desplegada.
19795-3	2007	Prueba específica de modalidad	Este informe técnico está en desarrollo para cubrir aspectos específicos de la modalidad de pruebas biométricas
19795-4	2008	Pruebas de rendimiento de interoperabilidad	Este estándar está en desarrollo para abordar la evaluación de interoperabilidad de componentes biométricos modulares
19795-5	2011	Rendimiento del control de acceso biométrico Sistemas	Esta norma está en desarrollo para establecer un procedimiento definitivo para la prueba de productos de control de acceso biométrico
19795-6	2012	Rendimiento de los sistemas operacionales	Esta norma está en desarrollo para abordar la evaluación de los sistemas de campo. Su objetivo es proporcionar una estimación instantánea del rendimiento. Enumerará aspectos que son específicos de las operaciones en vivo

Fuente: El Autor

Tabla 12: Perfiles biométricos para interoperabilidad e intercambio de datos

Perfiles biométricos para interoperabilidad e intercambio de datos		
ISO/IEC	Publicada	Descripción
24712-1	2007	Parte 1: Descripción general del sistema y los perfiles biométricos
24712-2	2008	Parte 2: Control de acceso físico para empleados en aeropuertos
24712-3		Parte 3: Verificación e identificación biométrica de la gente de mar

Fuente: El Autor

Tabla 13: Perfiles

Perfiles			
los perfiles de aplicación son estándares que adaptan uno o más estándares subyacentes para una actividad u operación específica.			
ISO/IEC	Publicada	Título de la norma	Descripción
24713-1	2008	Arquitectura de referencia del sistema biométrico	El estándar enumera los componentes funcionales de los sistemas biométricos genéricos e identifica la naturaleza de cada uno.
24713-2	2008	Control de acceso físico para empleados en aeropuertos	El estándar describe una función basada en tokens para la biometría en entornos aeroportuarios
24713-3	2009	Verificación biométrica e identificación de la gente de mar	Esta norma se está desarrollando esencialmente como una codificación de los requisitos biométricos del Convenio núm. 185 (2003) de la Organización Internacional del Trabajo que establece especificaciones para un documento de identidad que debe emitirse a la gente de mar de las naciones ratificantes
NIST SP 800-76	2004	Verificación de identidad personal	la Directiva Presidencial de Seguridad Nacional 12 ordenó a la rama ejecutiva del gobierno de los EE. UU. Que estableciera un mecanismo de acreditación altamente seguro y un token de identificación universalmente interoperable empleados y contratistas

Fuente: El Autor

Tabla 14: Normas de seguridad

Normas de seguridad			
ISO/IEC	Publicada	Título de la norma	Descripción
19792	2009	Evaluación de seguridad de biometría	Este estándar está en desarrollo en SC 27. Considera los ataques activos y es distinto de los estándares de prueba de SC 37 para los que los ataques activos están fuera de alcance
24761	2009	Contexto de autenticación para biometría	Este estándar está en desarrollo en SC 27 para permitir que las organizaciones que reciben los resultados de las autenticaciones biométricas de los usuarios a través de una red abierta puedan determinar si las circunstancias de la autenticación remota satisfacen sus requisitos
24745	2011	Protección biométrica de plantillas	Este estándar está en desarrollo en SC 27 para guiar la protección de plantillas biométricas con respecto a la confidencialidad, integridad y disponibilidad.
19092-1	2009	Servicios financieros - Biometría - Parte 1: Marco de seguridad	Establece un marco de seguridad para la autenticación biométrica de individuos en el ámbito de los servicios financieros. Requiere protección de integridad (firma digital, por ejemplo) para datos biométricos y resultados de autenticación cuando se transmiten entre componentes.

Fuente: El Autor

5.3.3 Normatividad para Acceder a Datos biométricos en Colombia

Tabla 15: Normatividad para Acceder a Datos biométricos en Colombia

Normatividad		Publicada	Título de la norma	Descripción	Dato
LEY	1450	2011	Artículo 227 PARÁGRAFO 2º:	Las entidades que desarrollen actividades financiera, bursátil, aseguradora y cualquier otra relacionada con el manejo, aprovechamiento e inversión de los recursos de captación del público. ⁷⁴ Las administradoras del sistema de seguridad social integral en pensiones, salud y riesgos laborales Las entidades públicas o particulares con funciones públicas que quieran verificar la plena identidad del ciudadano ⁷⁵	Datos biométricos de los afiliados al sistema general de seguridad social, salud y pensiones y en general, los que administra la RNEC
LEY	1581	2012	ARTÍCULO 10. CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN.	Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial sin necesidad de requerir autorización del titular del dato ⁷⁶	No se restringe el tipo de dato al que pueden acceder
Decreto	019	2012	ARTÍCULO 18.	En los trámites y actuaciones que se cumplan ante las entidades públicas y los particulares que ejerzan funciones	Datos biométricos

⁷⁵ (www.seguroscolpatria.com, 2020)

			VERIFICACIÓN DE LA HUELLA DACTILAR POR MEDIOS ELECTRÓNICOS.	administrativas; el Instituto Nacional Penitenciario y Carcelario INPEC ⁷⁷	
LEY	1753	2015	ARTÍCULO 159. OBLIGATORIEDAD DE SUMINISTRO DE INFORMACIÓN.	Las entidades que desarrollen actividades financiera, bursátil, aseguradora y cualquier otra relacionada con el manejo, aprovechamiento e inversión de los recursos de captación del público. Las administradoras del sistema de seguridad social integral en pensiones, salud y riesgos laborales Las entidades públicas o particulares con funciones públicas que quieran verificar la plena identidad de los ciudadanos ⁷⁸	Datos biométricos de los afiliados al sistema general de seguridad social, salud y pensiones y en general, los que administra la RNEC
Resolución	5633	2016	ARTÍCULO 14. SOLICITUD DE ACCESO Y CONSULTA A LA BASE DE DATOS PARA EL PROCESO DE	Las entidades interesadas en acceder y consultar los datos y la base de datos con la información biográfica y biométrica que produce y administra la Registraduría Nacional del Estado Civil	Datos biométricos

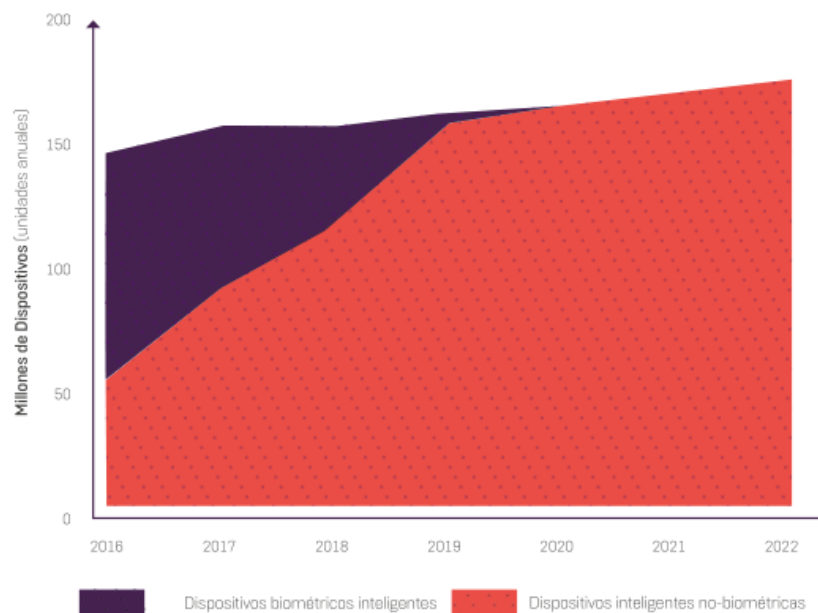
			AUTENTICACIÓN BIOMÉTRICA.⁷⁹		
Decreto 1413	1413	2017	ARTÍCULO Actores Involucrado 2.2.17.2.2.4 – Artículo 2.2.17.3.1 uso de los servicios ciudadanos digitales⁸⁰	Entidades públicas y particulares que ejercen función pública	Datos biométricos

Fuente: El Autor

5.4. MARCO TECNOLÓGICO

Los sistemas biométricos es una industria en constante evolución. De esta manera, esta tecnología ha sido valorada en los últimos años en el mercado mundial, esta tecnología se destaca por proporcionar un alto nivel de seguridad en los sectores privado, público y comercial. Las organizaciones y los usuarios de todo el mundo ahora están tratando de aprovechar sus beneficios con el fin para aliviar los problemas de privacidad y seguridad de datos. Además, se ha popularizado por los fabricantes de telefonía móvil en la última década que ha agregado millones de tecnologías increíblemente potentes y disruptivas. En los próximos años, el 64% de los teléfonos inteligentes contarán con funciones de reconocimiento facial en comparación con el 5% de los teléfonos inteligentes que lo tuvieron en 2017.

Figura 28: Número de dispositivos móviles biométricos vs no-biométricos



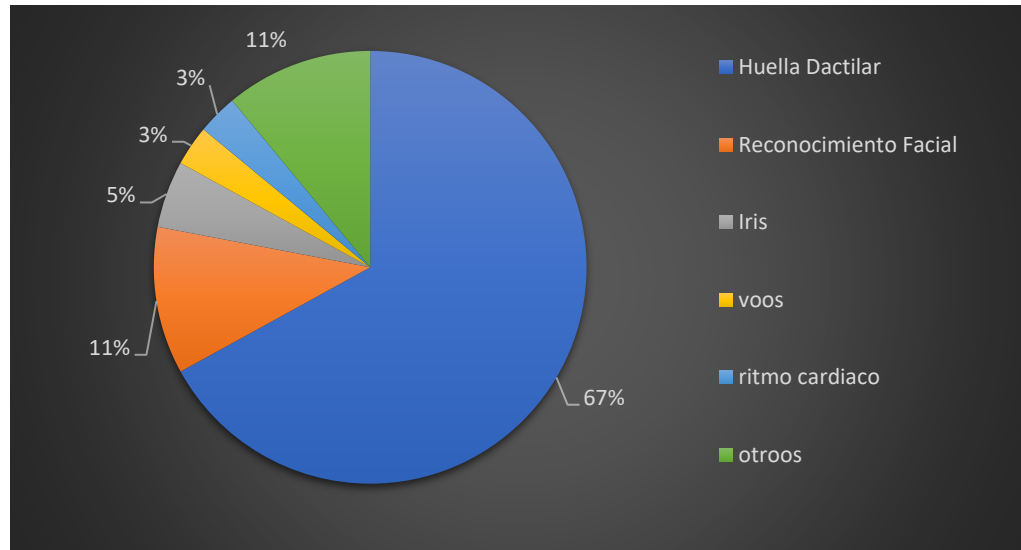
Fuente: FINTECHGRACIÓN: Libro Version Extendida: Biometría, 2020. ⁸¹

4.1 Cuotas del Mercado

Las cuotas de mercado para los diversos sistemas biométricos que se muestran arriba son una combinación de sistemas biométricos separados y sistemas biométricos del servidor del cliente, ya que la mayoría de los sistemas biométricos pertenecen a una de estas dos categorías. Hoy en día el reconocimiento de las **Huellas Dactilares** es el identificador biométrico más utilizado en el mercado, pero se estima que otro tipo de biometría dominará en el 2020

⁸¹ (www.fintechgracion.com, 2020)

Figura 29. Uso tipos de autenticación biométrica.



Fuente: FINTECHGRACIÓN: Libro Version Extendida: Biometría. Universidad Politécnica de Madrid. 2020. ⁸²

Figura 30. Dispositivos biométricos y sensores Participación en el mercado de ingresos por tipo. Incluyendo los mercados de consumo, empresa, banca, servicios financieros, salud, gobierno y seguridad.

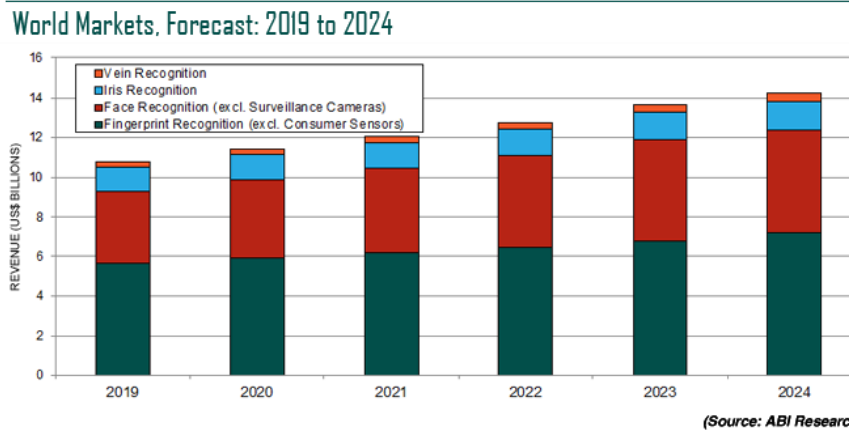
Producto	Reconocimiento Facial	Norte America	U.S	
	Geometría de la mano		Canada	
	Voz			
	Firma			
	Iris		Europa	Alemania
	AFIS		Francia	
	Otros		Rusia	
	No AFIS		Reino Unido	
				Asia
Aplicacion	Gubernamental	Japon		
	Defensa	India		
	Entidades Financieras	Korea del Sur		
	Consumo Electronico	LATAM	Brasil	
	Salud		Mexico	
	Transporte / Logistica			
	Otros	MEA - Oriente Medio y África		

Fuente: gminsights, industry-analysis: Productos, aplicaciones, Regiones biométricas. ⁸³

⁸² (IBID, 2020)

⁸³ (www.gminsights.com, 2020)

Figura 31. Ingresos totales de dispositivos biométricos por mercado final.
Total Biometric Device Revenue by Modality





Fuente: ABI Research: Tecnología y aplicaciones biométricas.⁸⁴



4.2 Compañías desarrolladoras de sistemas Biométricos

Hay una gran cantidad de empresas innovadoras responsables del desarrollo de diversas soluciones de hardware y software para sistemas biométricos. Estas empresas trabajan para diferentes entidades gubernamentales y civiles para mejorar la gestión de identidad, mejorar la seguridad lógica y física y aumentar la eficiencia operativa. A continuación, en la tabla se realiza un resumen de las principales compañías desarrolladora de sistemas Biométricos.




Tabla 16: Compañías desarrolladora sistemas Biométricos

Logo	Compañía	Descripción	Sitio WEB
	EyeLock	EyeLock proporciona soluciones biométricas basadas en iris que establecen los estándares de la industria mientras brindan los beneficios sin contacto, convenientes y de alta seguridad para todos los negocios verticales.	https://www.eyelock.com/
	Cognitec Systems	Cognitec Systems se fundó en 2002 y actualmente se dedica a ofrecer soluciones de software y hardware a sus clientes en el campo de la biometría, Cognitec desarrolla	https://www.cognitec.com/

⁸⁴ (abiresearch.com, 2020)

		aplicaciones de reconocimiento facial líderes en el mercado para clientes empresariales y gubernamentales de todo el mundo.	
	Aware	proveedor de software de identificación biométrica y autenticación desde 1992. Dentro de su productos se encuentran SDK, API y aplicaciones para registro y correspondencia de huellas digitales, rostro, iris y voz; detección de vida móvil y autenticación.	https://www.aware.com/
	NEXT Biometrics	proporciona tecnología de sensor de huellas dactilares segura y fácil de usar para la autenticación en los mercados de tarjetas inteligentes, identificación gubernamental y control de acceso y portátiles. la compañía desarrolla productos de huellas dactilares rentables y de alta seguridad.	https://www.nextbiometrics.com/
	JENETRIC	son expertos en tecnología de captura de huellas digitales que combina las más altas exigencias de calidad de imagen, velocidad de captura y facilidad de uso.	https://www.jenetric.com/home.html
	BioRugged	tiene una gama de terminales empresariales, resistentes con biometría, impresión térmica y otras capacidades periféricas. Estos dispositivos son de alta calidad y asequibles, lo que los hace ideales para mercados sensibles a los costos.	http://www.biorugged.com/
	Infinity Optics Solutions	desarrolla una solución biométrica criptográfica que permite un despliegue biométrico seguro y protegido	http://www.infinityoptics.com.sg/

		en aplicaciones de identidad digital utilizando una verdadera tecnología biométrica de hash generada a partir de huellas dactilares, rostro 2D / 3D, escaneos de palma, iris y voz. La compañía también diseña sistemas biométricos avanzados de reconocimiento de iris de profundidad de campo.	
	BIO-key	Es pionero e innovador en uno, somos reconocidos como desarrolladores líderes de autenticación biométrica de huellas dactilares y soluciones de seguridad.	https://www.bio-key.com/
	Unioncommunity	Es una compañía que ofrece varias soluciones biométricas como control de acceso, gestión de asistencia de tiempo, detección de imágenes y más. Las marcas incluyen Virdi y Nitgen.	https://www.virditec.com/h.com/
	IrisGuard	La tecnología EyePay de IrisGuard es una innovadora plataforma Secure Financial Delivery que utiliza tecnología de reconocimiento de iris de extremo a extremo.	https://www.irisguard.com/
	Iris ID	Desde 1997, ha sido el desarrollador clave y el impulsor de la comercialización de la tecnología de reconocimiento de iris. IrisAccess, ahora en una sexta generación, es la plataforma de reconocimiento de iris más implementada del mundo.	https://www.irisid.com/
	Jumio	Es el líder mundial en verificación y autenticación de identidad basada en biometría que ayuda a las empresas en línea a saber que sus clientes	https://www.jumio.com/

		son quienes dicen ser, ayudándoles a proteger sus ecosistemas (contra el fraude y la adquisición de cuentas), cumplir con los mandatos de cumplimiento y mejorar las tasas de conversión de incorporación .	
	FaceTec	fabrica Zoom con TrueLiveness, un autenticador biométrico de rostro móvil ultra seguro, fácil de usar y de gestión que verifica de forma única la vida.	https://www.facetec.com/
	HID Global	HID ofrece una amplia gama de software y hardware biométricos que pueden combinarse con soluciones de autenticación y administración de identidad física y móvil para una variedad de casos y entornos de uso de defensa, aplicación de la ley y gobierno. Nuestras soluciones y dispositivos biométricos ayudan a las organizaciones públicas y privadas a identificar y autenticar rápidamente a los empleados y ciudadanos utilizando iris, huellas digitales, así como identificaciones y credenciales móviles o físicas.	https://www.hidglobal.com/
	Suprema	Suprema ID proporciona soluciones de identidad biométrica de extremo a extremo que ofrece un rendimiento líder en la industria, confiabilidad e integración más simple, incluyendo autenticación, inscripción y lectores de pasaportes electrónicos.	https://www.suprema-id.com/en/contents/index.php

Fuente: El Autor

4.3 Sensores biométricos

Un sensor biométrico es cualquier componente capaz de adquirir una muestra biométrica digital. La mayoría de los componentes del sensor están alojados en un componente de hardware dedicado, para autenticar, identificar y verificar a un individuo, es necesario capturar sus características fisiológicas y de comportamiento. Esto requiere de un hardware especializado como son sensores, escaneadores o lectores biométricos, estos mecanismos son la parte de una solución biométrica con la que un usuario interactúa. Hay muchos tipos de lectores biométrica y sensores biométricos correspondientes que se utilizan hoy en día. Ya sea que se trate de cámaras de alta resolución para capturar biometría facial, cámaras infrarrojas para escanear iris, dispositivos de ultrasonido para representar múltiples capas de una huella digital o dispositivos de imágenes subdérmicas para mapear las venas de la palma y los dedos, los sensores y detectores son importantes de un ecosistema biométrico completo.

4.4 Tipos Sensores de Captura

La generación actual de sistemas biométricos está disponible con sensores que aprovechan diferentes técnicas, como capacitancia, térmica, etc. Los sistemas actuales de reconocimiento biométrico son considerablemente más rápidos que las generaciones anteriores. Tienen SDK disponible para PC y vienen con soporte para cifrado

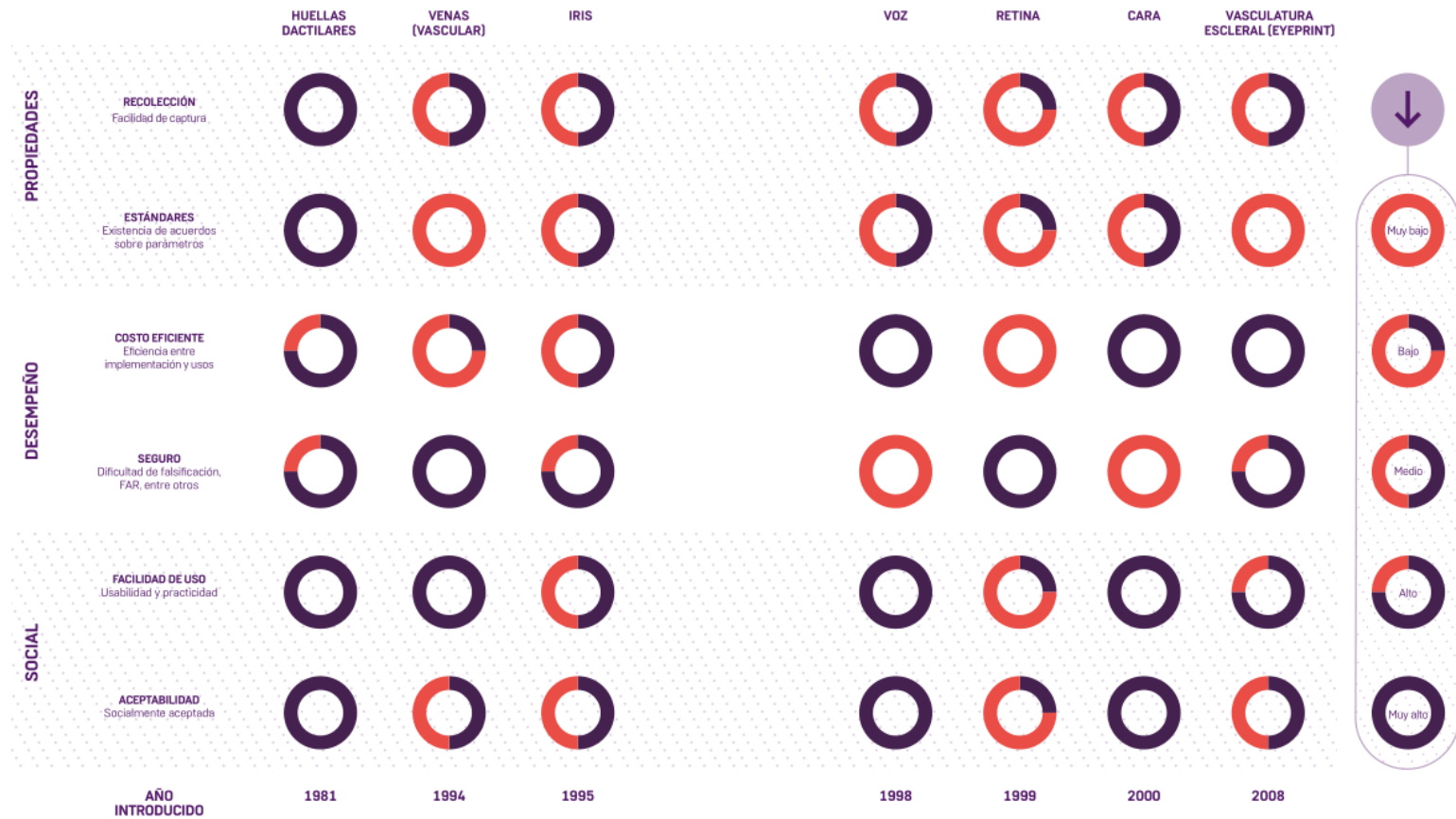
Tabla 17. Sensores para la captura.

CARACTERÍSTICAS DE BIOMÉTRICAS	SENSOR
HUELLA	capacitiva, óptica, térmica, acústica, sensible a la presión
FIRMA	Table
ROSTRO	Cámara
IRIS	Cámara
RETINA	Cámara
PALMA DE MANO	Cámara
VASCULAR	Cámara Infrarroja
OÍDO	Cámara
VOZ	Micrófono
DINÁMICA DE TECLEO	Teclado
MOVIMIENTO DE LOS LABIOS	Cámara

Fuente: El Autor.

A continuación, se figura se realiza un resume las Características y factores sociales de distintas modalidades biométricas

Figura 32. Características y factores sociales de distintas modalidades biométricas.



Fuente: FINTECHGRACIÓN: Fintechgracion Libro Version Extendida (2019).⁸⁵

⁸⁵ (www.fintechgracion.com, 2020)

4.5 Aplicaciones Horizontales y verticales

La Industria de Biométrica ofrece varias tecnologías. cada tecnología es considerada como un segmento de mercado diferente. A continuación, en la tabla 19.

Tabla 19: Aplicaciones Horizontales y verticales

Tecnología	Aplicación Horizontales	Principales Mercados Verticales
AFIS / Lifescan	Controles de vigilancia	Servicios Policiales y Militares
Reconocimiento de Cara	Identificación sin contacto	Farmacéuticas, Hospitales, Industria Pesada y Obras
Geometría de la Mano	Identificación Criminal	Hospitales y Sector Salud
Reconocimiento del Iris (Ojo)	Acceso a Sistemas	Industria Manufacturera
Reconocimiento de Voz	Acceso a Instalaciones	Viajes y Turismo
Escritura y Firma	Vigilancia	

Fuente: El Autor

4.6 Comparativa de los sistemas biométricos

A continuación, en la tabla 18 se realiza una comparativa de los diversos sistemas biométricos .

Tabla 18: Comparativa de sistemas biométricos:

	Ojo (Iris)	Ojo (Retina)	Huella Dactilar	Vascular dedo	Vascular Mano	Geometría de la Mano	Escritura y Firma	Voz	Cara 2D	Cara 2D
Fiabilidad	Muy Alta	Muy Alta	Muy Alta	Muy Alta	Muy Alta	Alta	Media	Alta	Media	Alta
Facilidad de Uso	Media	Baja	Alta	Muy Alta	Muy Alta	Alta	Alta	Alta	Alta	Alta
Prevención de Ataques	Muy Alta	Muy Alta	Alta	Muy Alta	Muy Alta	Alta	Media	Media	Media	Alta
Aceptación	Media	Baja	Alta	Alta	Alta	Alta	Muy Alta	Alta	Muy Alta	Muy Alta
Estabilidad	Alta	Alta	Alta	Alta	Alta	Media	Baja	Media	Media	Alta

Fuente: El Autor

4.7 Aplicaciones de la biometría.

La mayoría de las aplicaciones biométricas se dividen en una de nueve categorías generales, A continuación, en la tabla 20 se detallan las aplicaciones biométricas.

Tabla 20: Aplicaciones de la biometría.

Sectores	Descripción
Servicios financieros:	por ejemplo, cajeros automáticos y transacciones bancarias
Inmigración y control fronterizo	por ejemplo, Aeropuertos, emisión de pasaportes y visas
Servicios sociales	por ejemplo, Programas sociales
Atención médica	por ejemplo, Medidas de seguridad para la privacidad de médicos registros
Control de acceso físico	por ejemplo, institucional, gubernamental y residencial
Tiempo y asistencia	por ejemplo, reemplazo de tarjeta perforada de tiempo).
Seguridad informática	por ejemplo, acceso a la computadora personal, red acceso, uso de Internet, comercio electrónico, correo electrónico, encriptación
Telecomunicaciones	por ejemplo, teléfonos móviles
Aplicación de la ley	por ejemplo, investigación criminal, identificación nacional, licencia de conducir, instituciones correccionales / cárceles, confinamiento en el hogar, arma inteligente

Fuente: El Autor.

4.8 Sensores de Reconocimiento de Huella

A continuación, en la tabla 21 se exponen diversos lectores biométricos de reconocimientos de huella dactilares.

Tabla 21: Lectores biométricos de reconocimientos de huellas dactilares.

Lector	Nombre	Descripción
	M2-S™ Fingerprint Scanner	<p>El escáner de huellas digitales M2-S fue diseñado para usarse con la metodología de integración Bio-Plugin™ de M2SYS y también es compatible con muchos SDK de huellas digitales estándar. El diseño robusto y ergonómico del lector fuerza la colocación perfecta de los dedos con cada escaneo para producir una imagen optimizada con el área de superficie máxima capturada.</p>
	WEB	
	https://www.m2sys.com/m2-s-fingerprint-scanner/	
Lector	Nombre	Descripción
	DigitalPersona U.are.U 5160	<p>El lector de huellas dactilares U.are.U 5160 de estilo táctil es un sensor óptico de huellas dactilares certificado FIPS 201 PIV diseñado para servir como periférico USB. Esta potente y robusta máquina de verificación e identidad de huellas dactilares es ideal para grandes implementaciones en votación, derechos, atención médica, finanzas y educación.</p>
	WEB	
	https://www.neurotechnology.com/fingerprint-scanner-digitalpersona-u-are-u-5100-5160.html	

Fuente: El Autor

4.9 Sensores de Reconocimiento de la Firma

Los sistemas biométricos analizan el acto de escribir comprobando la presión utilizada y la velocidad, el ritmo de escritura y no solo observando la forma en que se forman las palabras, sino que también registra la secuencia en la que se escriben las letras. Los sensores del sistema incluyen una superficie de escritura sensible al tacto o un bolígrafo que contiene sensores que detectan el ángulo, la presión y la dirección. A continuación, en la tabla 22 se exponen diversos lectores biométricos de Firma.

Tabla 22: Lectores biométricos de reconocimientos de Firma.

Lector	Nombre	Descripción
	Topaz T-s460-hsb-r USB Electronic Signature	SigLite® 1x5 es la libreta de firma electrónica sensible a la presión y de bajo costo de Topaz. Cuenta con todas las técnicas de captura forense y biométrica de alta calidad de una tableta SignatureGem® pero con un panel táctil y un lápiz óptico de bajo costo en lugar del lápiz y el sensor electromagnéticos activos.
	WEB	
	https://www.topazsystems.com/siglite1x5.html	
Lector	Nombre	Descripción
	Secure Sign II	Secure Sign II combina un panel táctil con un área de firma. Juntos hacen un asunto claro e intuitivo del proceso de firma electrónica. Los clientes saben y ven con precisión qué documento firman porque toda la acción ocurre en un panel. La firma biométrica evaluada de manera sofisticada proporciona una identificación detallada y precisa de una persona.
	WEB	
	https://www.elcom.eu/en/produkty/podpisove-riesenia/secure-sign2/	

Fuente: El Autor

4.10 Lector de Venas del Dedo

La tecnología de reconocimiento de venas de los dedos es un método de autenticación biométrica que utiliza técnicas de reconocimiento de patrones basadas en imágenes de huellas digitales humanas y patrones de venas de los dedos debajo de la superficie de la piel. Un dispositivo especializado utiliza luz de infrarrojo cercano para capturar un perfil único de huella digital y patrón de vena de dedo, que luego se combina con un perfil registrado previamente para verificar la identidad individual. A continuación, en la tabla 23 se exponen diversos lectores biométricos de reconocimientos vascular.

Tabla 23: Lectores biométricos de reconocimientos vascular.



Lector	Nombre	Descripción
	Hitachi H-1 Lector de venas del dedo PC-KCA100	La tecnología de la vena del dedo es una solución biométrica segura, confiable y no invasiva que proporciona autenticación de identidad rápida y altamente precisa para acceder a datos o áreas seguras.
	WEB	
	http://www.hitachi.co.jp/products/it/veinid/global/products/embedded_devices_u.html	
Lector	Nombre	Descripción
	Escáner de venas de dedo Futronic VS80 USB2.0	Está diseñado para capturar las mejores imágenes de venas de dedo para esta aplicación. Se usa una fuente de luz infrarroja en el VS80 que funciona junto con un sensor de imagen CMOS de alta calidad para proporcionar una imagen clara y de alto contraste de la vena del dedo para la coincidencia. El VS80 fue diseñado para filtrar el "ruido de fondo" en las imágenes de las venas de los dedos, lo que permite una mayor precisión y un mayor nivel de seguridad.
	WEB	
	https://www.futronic-tech.com/pro-detail.php?pro_id=1531	

Fuente: El Autor

4.11 Lector de Reconocimiento del Iris

El reconocimiento del iris o el escaneo del iris es el proceso de usar luz visible e infrarroja cercana para tomar una fotografía de alto contraste del iris de una persona. Es una forma de tecnología biométrica en la misma categoría que el reconocimiento facial y las huellas digitales. A continuación, en la tabla 24 se exponen diversos lectores biométricos de reconocimientos del Iris.

Tabla 24: lectores biométricos de reconocimientos del Iris.

Lector	Nombre	Descripción
	UltraMatch S2000	Adoptando el algoritmo BioNANO, el sistema proporciona el reconocimiento de iris más preciso, estable y rápido al mismo tiempo que ofrece seguridad de alto nivel en el registro biométrico, la identificación individual y el control de acceso ⁸⁶ . Utiliza el algoritmo BioNano V10 con el procesador TI Stellaris® 32-Bit de alta velocidad y activación por infrarrojos. Los métodos de identificación son por reconocimiento de iris o lectura de tarjeta de proximidad.
	WEB	
	https://www.anviz.com/product/s2000-iris-recognition.html	
Lector	Nombre	Descripción
	EyeSwipe - Nano TS	Es una solución biométrica del Iris avanzada para puntos de acceso, proporcionando la captura del iris en tiempo real tanto a distancia como en movimiento. Ha sido diseñado para satisfacer las necesidades de un acceso o un entorno de rápido rendimiento y cuenta con un amplio rango de captura para un mejor uso a altas velocidades ⁸⁷
	WEB	
	http://eyelock.nobelsecurity.systems/eyeswip-e-nano-ts/	

Fuente: El Autor



⁸⁶ (<https://www.lsb.es>, s.f.)

⁸⁷ (<https://sierra.sg/>, s.f.)

4.12 Lector de Reconocimiento Facial

El escáner facial es el sistema de reconocimiento de generación futura que proporciona un proceso de verificación humana increíblemente versátil. El sistema de reconocimiento facial captura imágenes fijas o imágenes de video en vivo para identificar a un individuo a cierta distancia, ya que no implica ninguna interacción física con la persona. Las imágenes capturadas serán en forma de puntos nodales que se comparan con los puntos nodales existentes presentes en el sistema para identificar a un individuo previamente registrado. A continuación, en la tabla 25 se exponen diversos lectores biométricos de reconocimientos Facial.

Tabla 25: Lectores biométricos de reconocimientos Facial.



Lector	Nombre	Descripción
	FR01W: Lector de reconocimiento facial	<p>El FR01W es un terminal de reconocimiento facial de doble cámara diseñado para proporcionar un reconocimiento rápido, preciso y sin interrupciones al ritmo normal de marcha sin ralentizar al individuo. FR01W también tiene un lector RFID incorporado, compatible con 13.56MHz y una salida Wiegand universal que permite la conexión a sistemas de control de acceso de terceros</p>
	<p>WEB</p> <p>http://genieaccess.com/product/fr01w-facial-recognition-reader/</p>	
Lector	Nombre	Descripción
	FacePass 7 Smart Face Recognition System	<p>Anviz FacePass 7 es un lector de tarjetas y reconocimiento facial para control de acceso y uso en interiores. El control de acceso se lleva a cabo mediante un escáner facial y / o una tarjeta o etiqueta de proximidad RFID. El Anviz FacePass 7 es ideal para usar en la atención médica, la industria alimentaria, los laboratorios y otras instalaciones donde no se desea el control de acceso con las manos, se usan guantes o no se desea el contacto.</p>
	<p>WEB</p> <p>https://www.anviz.com/product/facepass7-face-recognition.html</p>	

Fuente: El Autor

4.13 Lector de Reconocimiento Geometría Mano

Los dispositivos de geometría de mano son dispositivos biométricos especialmente diseñados para capturar las características geométricas (por ejemplo, la longitud, el ancho, el grosor y la curvatura de los dedos, el tamaño de la palma y las distancias entre las articulaciones) de una mano humana para la verificación de identidad basada en la geometría de la mano. Un dispositivo típico de geometría de la mano graba imágenes de las partes laterales y dorsales de la mano con una cámara de dispositivo acoplado a carga (CCD) que está montada sobre una superficie plana sobre la cual la persona que se presenta al dispositivo coloca su mano. El conjunto de características geométricas extraídas de estas imágenes se compara con una plantilla pregrabada almacenada en la base de datos del dispositivo. A continuación, en la tabla 25 se exponen diversos lectores biométricos de reconocimientos de la Geometría de la Palma.

Tabla 26: Lectores biométricos de reconocimiento de la Geometría de la Palma.

Lector	Nombre	Descripción
	HandKey II Biometric Terminal	La geometría de reconocimiento de manos usa la forma de la mano para identificar / verificar a la persona. Tanto el HK-2 como el HK-CR (ambos modelos solo para uso en interiores) utilizan tecnología de geometría de mano probada en el campo que mapea y verifica el tamaño y la forma de la mano de una persona en menos de un segundo.
	WEB https://www.security.honeywell.com/uk/product-repository/handkey	
Lector	Nombre	Descripción
	GT400 Biometric Hand Geometry Reader	Una de las soluciones más eficientes para la gestión de la fuerza laboral es el AMG HandPunch GT400. Con este sistema de reloj biométrico, puede mejorar la precisión del mantenimiento de registros, aumentar la productividad de los empleados, mitigar los riesgos y proporcionar tranquilidad para usted y su personal.
	WEB https://www.midwesttime.com/gt400-biometric-hand-geometry-reader	

Fuente: El Autor

5. METODOLOGÍA

5.1 Sistemas de Seguridad Biometría en Colombia

Actualmente una variedad de organizaciones gubernamentales, bancos, entidades e instituciones, han implementaron en sus diferentes procesos de operaciones el uso de sistemas biométricos. Un ejemplo claro son las entidades bancarias, según RCN en su portal web "El 60% de las entidades financieras del país usan la autenticación biométrica " ⁸⁸ esto lo confirma el portal web actualícese quien en su entrevista al señor "Santiago Castro, presidente de Asobancaria, reveló que en Colombia el 60 % de las entidades financieras ya están haciendo uso de la autenticación biométrica. «Los bancos que han implementado este sistema de seguridad, realizan entre 1,1 y 1,3 millones de transacciones por mes»⁸⁹ Otra institución es la Registraduría Nacional del Estado Civil de Colombia que "ha utilizado durante los últimos 12 años la biometría como una herramienta para identificar a los colombianos " ⁹⁰. El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) " su gran meta es la articulación de estos procesos con los Servicios Ciudadanos Digitales, que son básicamente la carpeta ciudadana; la autenticación electrónica, biométrica o con cédula digital, y la interoperabilidad, para así facilitarle la vida a los colombianos. " ⁹¹. Empresas como Giros & Finanzas, Servientrega, Efecty que "brindan soluciones integrales de pago y recaudo, a través de las cuales las empresas pueden ofrecer a sus usuarios servicios de pagos de nómina, entrega de subsidios, comisiones, entre otros. Estas transacciones se ejecutan bajo los más altos estándares de seguridad a través de un sistema de validación biométrica "⁹². otra organización es la "Cámara de Comercio de Bogotá puso en funcionamiento un Sistema de autenticación biométrica de voz (Certivoz),

⁸⁸ RCN Radio, El 60% de las entidades financieras del país usan la autenticación biométrica [En Línea]. Ciudad: Bogotá. Autores: RCN 2020; Disponible en: <https://www.rcnradio.com/colombia/el-60-de-las-entidades-financieras-del-pais-usan-la-autenticacion-biometrica>

⁸⁹ Actualícese, Autenticación biométrica evita la suplantación y el fraude a través de todos sus canales [En Línea]. Ciudad: Bogotá. Autores: RCN 2019; Disponible en: <https://actualicese.com/autenticacion-biometrica-evita-la-suplantacion-y-el-fraude-a-traves-de-todos-sus-canales/>

⁹⁰ Registraduría Nacional del Estado Civil de Colombia, Identificación Biométrica: cada vez con más Usos En La Vida Cotidiana [En Línea]. Ciudad: Bogotá. Autores: Registraduría Nacional del Estado Civil de Colombia 2020; Disponible en: <https://www.registraduria.gov.co/Identificacion-biometrica-cada-vez.html>

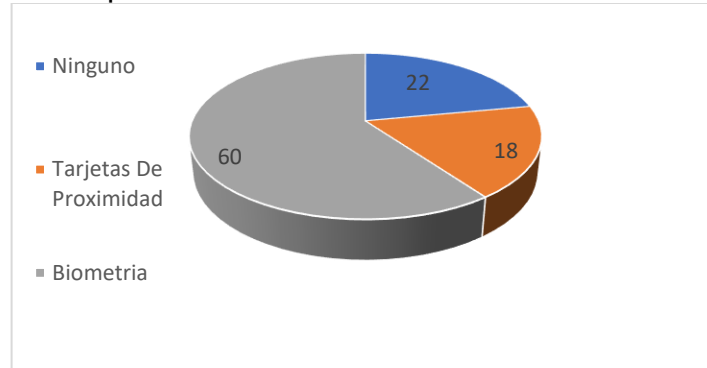
⁹¹ Ministerio de Tecnologías de la Información y las Comunicaciones, MinTIC fortalece sus servicios a los ciudadanos gracias a la implementación de la Política de Gobierno Digital [En Línea]. Ciudad: Bogotá. Autores: MINTIC 2018; Disponible en: <https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/75002:MinTIC-fortalece-sus-servicios-a-los-ciudadanos-gracias-a-la-implementacion-de-la-Politica-de-Gobierno-Digital>

⁹² Ministerio de Tecnologías de la Información y las Comunicaciones, MinTIC fortalece sus servicios a los ciudadanos gracias a la implementación de la Política de Gobierno Digital [En Línea]. Ciudad: Bogotá. Autores: MINTIC 2018; Disponible en: <https://mintic.gov.co/portal/inicio/Sala-de-Prensa/MinTIC-en-los-Medios/73987:Tecnologia-y-servicio>

implementado por Certicámara, una herramienta tecnológica que permitirá a los ciudadanos realizar trámites con entidades públicas y privadas, utilizar firmas electrónicas con valor jurídico y probatorio para trámites presenciales y no presenciales en forma rápida y segura"⁹³.

¿Qué mecanismo emplean su organización para la autenticación en el control de acceso a las instalaciones?

Figura 33. Tasa de respuesta encuesta 1.

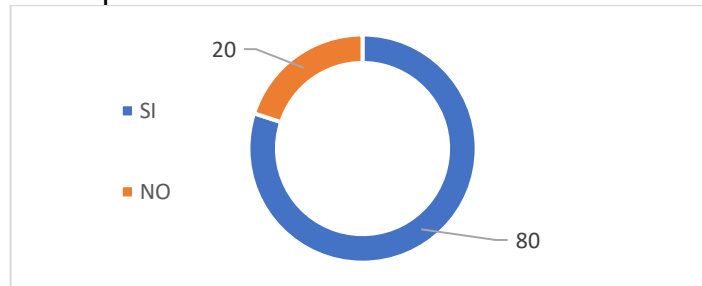


Fuente: El Autor

Se puede ver que el 65% de los encuestados usa un mecanismo biométrico para autenticarse, el 18% realiza este proceso con tarjeta de proximidad y 22% no usa ningún tipo.

¿La organización donde usted labora cuenta con algún sistemas biométricos?

Figura 34. Tasa de respuesta encuesta 2.



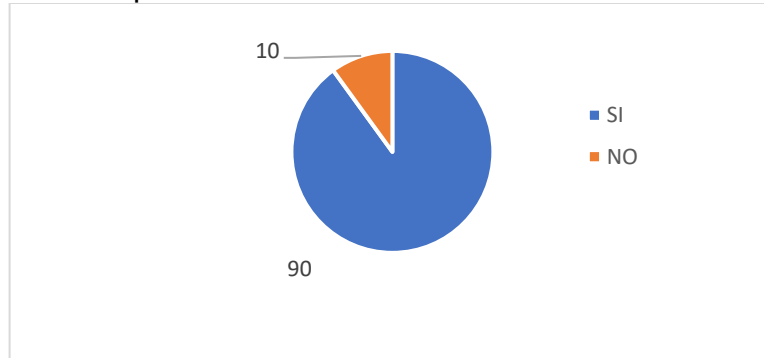
Fuente: El Autor

Se puede ver que el 80% de los encuestados en su organización cuenta con sistemas biométricos y 20% no.

⁹³ Ministerio de Tecnologías de la Información y las Comunicaciones, Certicámara puso en servicio Certivoz, sistema de autenticación biométrica de voz [En Línea]. Ciudad: Bogotá. Autores: MINTIC 2018; Disponible en: https://www.mintic.gov.co/porta/604/w3-article-9371.html?_noredirect=1

¿La organización donde usted labora cuenta con la infraestructura para implementar sistemas biométricos?

Figura 35. Tasa de respuesta encuesta 3.



Fuente: El Autor

Se puede ver que el 90% de los encuestados responde que en su organización se puede implementar sistema biométricos y 10% no.

Según predicciones de Goode Intelligence, para el año 2020 el papel que tomará la biometría dentro el sistema financiero será de gran importancia. Estas serían algunas de sus implicaciones

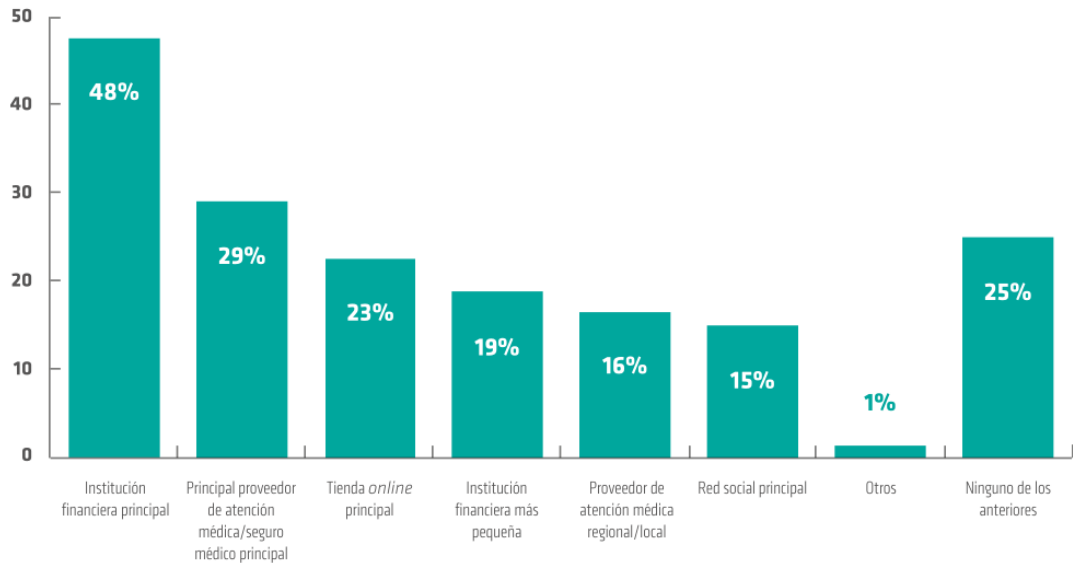
Figura 36. La biometría a 2020 en los servicios financieros



Fuente: Biometrics Research Group.(2016). Biometrics and Banking⁹⁴

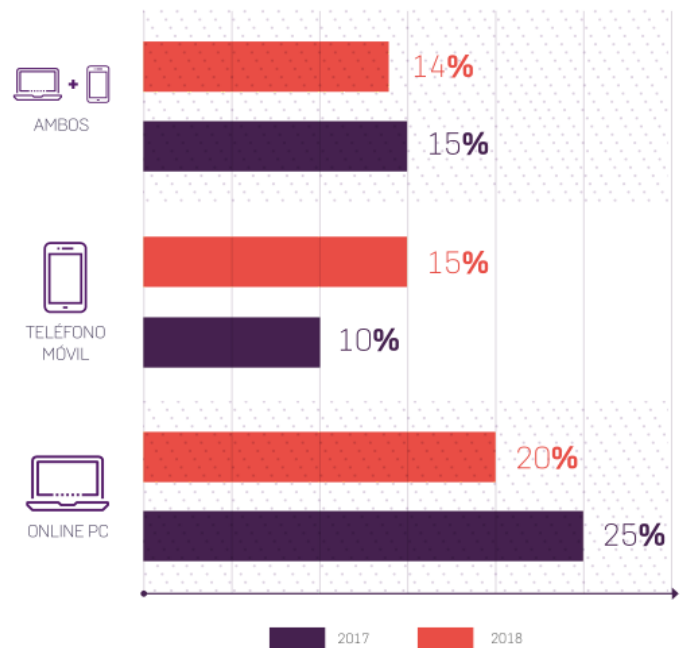
⁹⁴ (www.goodeintelligence.com, s.f.)

Figura 37. Tipos de organización en las que las personas confían más para proteger su información biométrica (perspectiva global)



Fuente: Organizaciones en las que más se confía para proteger información biométrica. IBM, 2018 ⁹⁵

Figura 38. Uso de banca online.



Fuente: FINTECHGRACIÓ: Fintechgracion Libro Version Extendida, 2020.⁹⁶

⁹⁵ (<https://www.asobancaria.com/>, 2020)

⁹⁶ (www.fintechgracion.com, 2020)

5.2 Requisitos para acceder a la Registraduría

Tabla 27: Requisitos entidades Publicas⁹⁷

Organización	Requisitos
ENTIDAD PÚBLICA	Estudio de necesidad: justificando de manera clara y concreta la necesidad de acceso a la información y la finalidad que le dará a la misma, conforme a lo establecido en la normatividad legal vigente y a sus funciones ⁹⁸ .
	Informar la modalidad de acceso, el cronograma de actividades, el formato de minucias y los aliados tecnológicos (operador biométrico y administrador de la base de datos y web service).
	Fotocopia de la cédula del representante legal.
	Actas de nombramiento y posesión del representante legal.
	Suscribir compromiso de confidencialidad.
	Documento que acredite la creación y la naturaleza de la entidad pública.
	Remitir protocolo de seguridad y análisis de riesgos sobre el proceso de autenticación biométrica con la Registraduría Nacional, conforme a los dominios de la norma ISO 27001.
	Presentación del data center con características TIER III.
	Pólizas de seguro a nombre de la Registraduría Nacional (extracontractual, una vez sea suscrito el convenio)
	Para el operador biométrico debe remitir los siguientes documentos, para cumplir con los requisitos exigidos en la Resolución 5633 de 2016 y sus anexos técnicos:
	Certificado de Existencia y Representación Legal.
	Certificación RUP
	Certificación de capacidad económica
	Experiencia certificada para autenticación biométrica
Experiencia RUP	

Fuente: El Autor

Una vez verificado el cumplimiento de requisitos, la Registraduría Delegada para el Registro Civil y la Identificación y la Gerencia de Informática darán la viabilidad para la suscripción de dicho Convenio.

⁹⁷ (<https://www.registraduria.gov.co/>, s.f.)

⁹⁸ (IBID, 2020)

Tabla 28: Requisitos entidades Privadas⁹⁹

Organización	Requisitos
ENTIDAD PÚBLICA	Estudio de Necesidad: justificando de manera clara y concreta la necesidad de acceso a la información y la finalidad que le dará a la misma, conforme a lo establecido en la normatividad legal vigente y al cumplimiento de su objeto social
	Informar el modelo de operación, el cronograma de actividades, el formato de minucias y los aliados tecnológicos (operador biométrico y administrador de la base de datos y Web Service).
	Certificado de existencia y representación legal.
	Fotocopia de la cédula del representante legal.
	Certificado de parafiscales, de conformidad con el art. 50 de la ley 789 de 2002 (debe ser aportada mes a mes).
	Certificaciones de Policía, Procuraduría y Contraloría, consulta que debe hacerse con el NIT de la entidad.
	Certificación bancaria de la empresa solicitante.
	Remitir protocolo de seguridad y análisis de riesgos sobre el proceso de autenticación biométrica con la Registraduría Nacional, conforme a los dominios de la norma ISO 27001.
	Presentar data center con características TIER III.
	Formato de beneficiario de cuenta debidamente diligenciado.
	Pólizas de seguro a nombre de la Registraduría Nacional (contractual y extracontractual, una vez suscrito el contrato)
	Para el operador biométrico debe remitir los siguientes documentos, para cumplir con los requisitos exigidos en la Resolución 5633 de 2016 y sus anexos técnicos:
	Certificado de Existencia y Representación Legal.
	Certificación RUP
Certificación de capacidad económica	
Experiencia RUP	

Fuente: El Autor

⁹⁹ (IBID, 2020)

5.3 Convenios con la Registraduría

De conformidad con las disposiciones del Decreto 019 de 2012, la Ley 1753 de 2015 y la Resolución 3341 de 2013, el Registro Nacional de Estado Civil permite a las entidades públicas y las personas que ejercen funciones públicas confrontar en línea a través del sistema de autenticación biométrica, la información sobre las huellas digitales de los ciudadanos con la información contenida en base de datos del dispositivo. Este sistema permite recibir respuestas en menos de un segundo. La Registraduría ha suscrito 30 convenios, que se encuentran vigentes a la fecha.¹⁰⁰

Tabla 29: Convenios.¹⁰¹

Organizaciones	Convenio
Unión colegiada de notariado colombiano	001 de 2018
Banco agrario	002 de 2014
Confecámaras	006 de 2018
Aeronáutica	024 de 2016
Policía nacional	046 de 2017
Cancillería	056 de 2017
Unidad para la atención y reparación	070 de 2018
Federación nacional de departamentos	073 de 2018
Fondo nacional del ahorro	075 de 2018
Asociación notarial de innovación y tecnologías	074 de 2018
Colpensiones	076 de 2019
EPM	077 de 2019
ICFES	078 de 2019

Fuente: Registraduría Nacional Del Estado Civil, Colombia - Convenios de Biometría. (2020)

¹⁰⁰ (IBID, 2020)

¹⁰¹ (IBID, 2020)

5.4 Historial de Convenios de Autenticación Biométrica

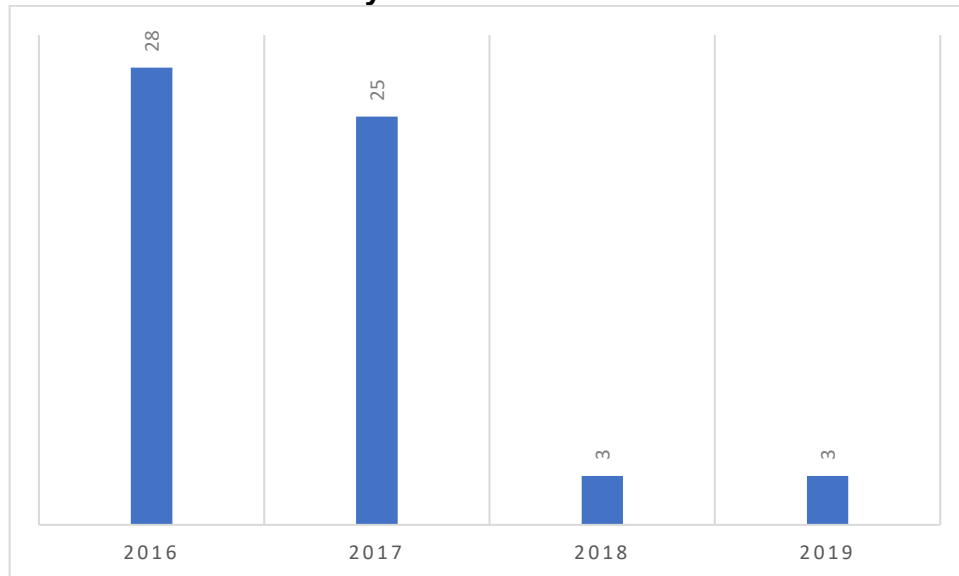
La tabla y el gráfico se elaboran con datos los informes de gestión anual correspondientes a los años 2015, 2016, 2017, 2018 y 2019 de la Registraduría Nacional del Estado Civil.

Tabla 30: Historial de Convenios

Reporte	Años	Cantidad De Convenios Nuevos
INFORME GESTIÓN 2016. ¹⁰²	2016	28
INFORME GESTIÓN 2017. ¹⁰³	2017	25
INFORME GESTIÓN 2018. ¹⁰⁴	2018	3
INFORME GESTIÓN 2019. ¹⁰⁵	2019	3

Elaborado: El Autor

Figura 39. Historial convenios y autenticación biométrica



Elaborado: El Autor

¹⁰² (IBID, 2020)

¹⁰³ (IBID, 2020)

¹⁰⁴ (IBID, 2020)

¹⁰⁵ (IBID, 2020)

5.5 Historial de Contratos de biometría

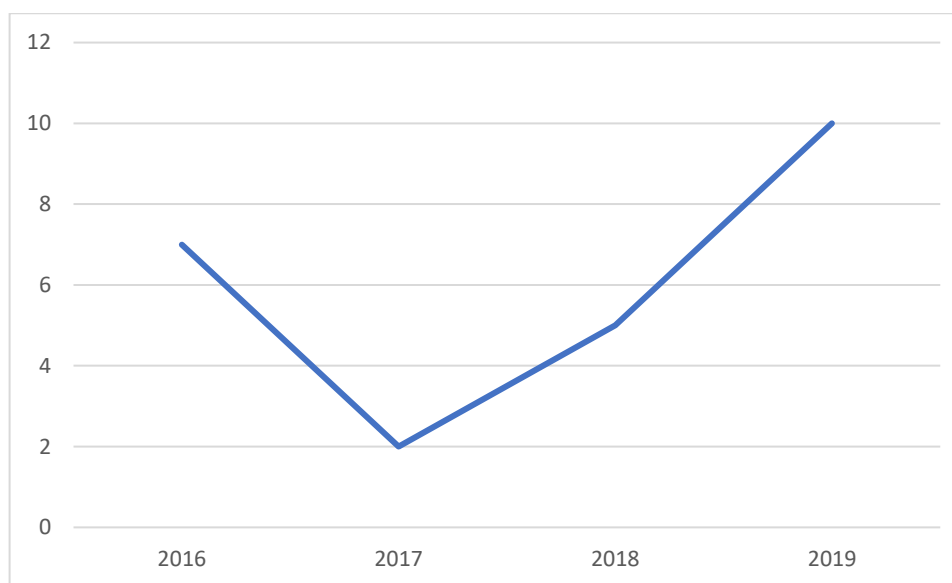
La tabla y el gráfico se elaboran con datos los informes de gestión anual correspondientes a los años 2015, 2016, 2017, 2018 y 2019 de la Registraduría Nacional del Estado Civil.

Tabla 31: Historial de Contratos

Reporte	Años	Cantidad de Contratos Nuevos
INFORME GESTIÓN 2016. ¹⁰⁶	2016	7
INFORME GESTIÓN 2017. ¹⁰⁷	2017	2
INFORME GESTIÓN 2018. ¹⁰⁸	2018	5
INFORME GESTIÓN 2019. ¹⁰⁹	2019	10

Elaborado: El Autor

Figura 40. Historial Contratos



Elaborado: El Autor

¹⁰⁶ (IBID, 2020)

¹⁰⁷ (IBID, 2020)

¹⁰⁸ (IBID, 2020)

¹⁰⁹ (IBID, 2020)

5.6 Consultas y autenticación biométrica en línea

Durante la vigencia 2019 se realizó un total de 70.072.766 consultas biométricas por parte de las entidades con las cuales la RNEC tiene convenios y contratos como se observa continuación:¹¹⁰

Tabla 32: Consultas y autenticación biométrica en línea 2019

N.º	Cliente	2019
1	Aeronáutica civil	54.677
2	Asobancaria	18.475.021
3	Asocaias	492.650
4	Asociación Notarial de Innovación y Tecnología (ANIT)	6.731.071
5	Banco agrario	30
6	Banco Colpatria	2.602.679
7	Banco cooperativo Coopcentral	10.898
8	Banco de Bogotá	2.304.589
9	Centaurus mensajeros s.a.	227
10	Colombia móvil S.A E.S.P - TIGO	1.005
11	Colombia telecomunicaciones S.A . E.S.P.	1.110.032
12	Colpensiones	7.916
13	Comcel s.a.	6.125.591
14	Confecámaras	1.701.073
15	Consorcio SIGS	1.372.762
16	Comeva medicina prepagada SA	19.034
17	Cotrafa	23.303
18	Domina	119.591
19	Empresas públicas de Medellín (EPM)	4.113
20	Fondo nacional del ahorro	756.607
21	Gm Financiam Colombia s.a	198
22	Ministerio de relaciones exteriores	2.567.821
23	OLIMPIA ceas (CRC)	964.433
24	Policía nacional	3.504.804
25	Protección s.a.	1.341.670
26	RNEC: inscripción de Cédulas 2017-2018	6
27	RNEC: inscripción de Cédulas 2018-2019	4.840.397
28	Serfinansa	472.898
29	Telmex Colombia s.a.	80.165
30	Une-EPM telecomunicaciones S.A	24
31	Unidad para la atención y reparación integral a las víctimas	668
32	Unión colegiada del notariado colombiano	14.242.100
33	Unión de entidades de economía solidaria (Unioncoop)	144.713
Total		70.072.766

Fuente: Registraduría Nacional Del Estado Civil, Colombia. Consultas y autenticación biométrica en línea. (2020)

¹¹⁰ (IBID, 2020)

5.7 Historial de Consultas y autenticación biométrica en línea

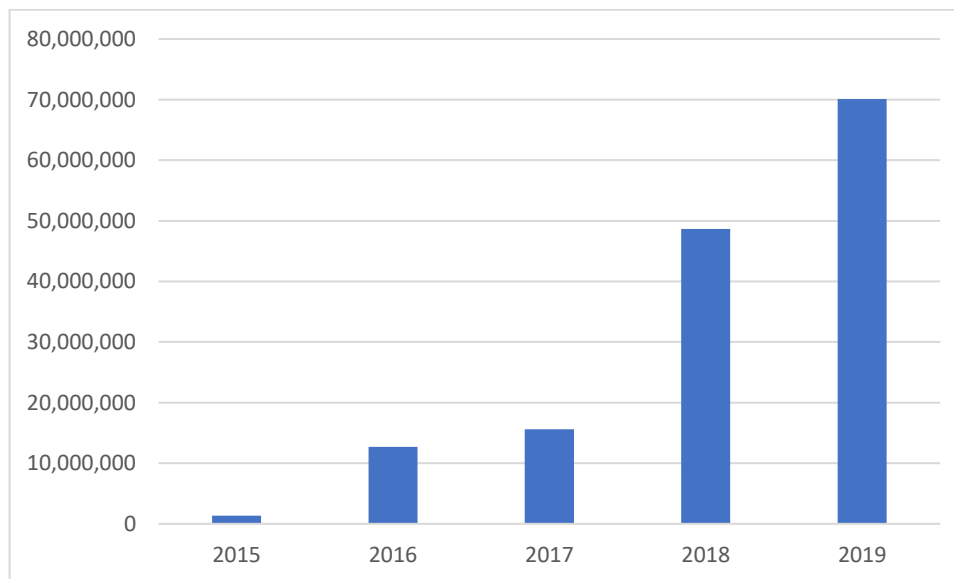
La tabla y el gráfico se preparan con los informes de gestión correspondientes a los años 2015, 2016, 2017, 2018 y 2019 de la Registraduría Nacional del Estado Civil.

Tabla 33: Historial Consultas y autenticación biométrica en línea

Reporte	Años	Cantidad de Consultas Nuevas
INFORME GESTIÓN 2015 ¹¹¹	2015	1.331.326
INFORME GESTIÓN 2016 ¹¹²	2016	12.721.230
INFORME GESTIÓN 2017 ¹¹³	2017	15.595.116
INFORME GESTIÓN 2018 ¹¹⁴	2018	48.649.381
INFORME GESTIÓN 2019 ¹¹⁵	2019	70.072.766

Elaborado: El Autor

Figura 41. Historial Consultas y autenticación biométrica en línea



Elaborado: El Autor

¹¹¹ (<https://www.registraduria.gov.co/>, 2020)

¹¹² (IBID, 2020)

¹¹³ (IBID, 2020)

¹¹⁴ (IBID, 2020)

¹¹⁵ (IBID, 2020)

5.8 Operadores Biométricos

En atención a la normatividad vigente la Registraduría Nacional del Estado Civil certifica a los aliados tecnológicos a través de los cuales las entidades públicas y particulares autorizados por la ley, podrán acceder al proceso de autenticación biométrica, conforme a lo establecido en el artículo 19 de la Resolución 5633 de 2016.¹¹⁶

Tabla 34: Operadores Biométrico en Colombia.

RAZÓN SOCIAL	NIT	EXPEDICIÓN	VENCIMIENTO	CERTIFICADO	SITIO WEB
		(AAAA/MM/DD)	(AAAA/MM/DD)		
GESTIÓN DE SEGURIDAD ELECTRONICA S.A – GSE SA	900204272-8	27/08/2019	26/08/2021		
GEAR ELECTRIC S.A.S.	900410963-1	4/07/2019	23/05/2021		
SECURID S.A.S.	900534955-5	27/06/2019	5/06/2021		
ID3 TECHNOLOGIES S.A.S.	901045081-9	27/06/2019	8/06/2021		
CERTICAMARA S.A.	830084433-7	18/06/2019	23/05/2021		
GRUPO ASD S.A.S.	860510031-7	16/11/2018	15/11/2020		
OLIMPIA MANAGEMENT S.A.	900032774-4	12/09/2018	11/09/2020		

Fuente: Registraduría Nacional Del Estado Civil, Colombia Operadores Biométricos. (2020)

¹¹⁶ (<https://www.registraduria.gov.co/>, 2020)

5.9 Dispositivos Biométricos

Dispositivos homologados que cumplen con los requerimientos establecidos en el anexo técnico No. 2 de la resolución 5633 de 2016¹¹⁷

Tabla 35: Dispositivos Biométricos

#	MARCA	FABRICANTE	MODELO	TIPO	DISTRIBUIDOR	ALCANCE	FECHA HOMOLOGACIÓN	FICHA TÉCNICA
							(AAAA/MM/DD)	
1	IDEMIA	IDEMIA	MSO-301	USB ESTACIONES FIJAS	- IDEMIA	ANEXO TEC. 2 V2	20/11/2019	
2	HID LUMIDIMG	HID GLOBAL	Lumidigm V421-NC-01	USB ESTACIONES FIJAS	- IDCO Solutions S.A.S.	ANEXO TEC. 2 V2	17/01/2019	
3	CHAINWAY	SHENZHEN CHAINWAY INFORMATION TECHNOLOGY CO., LTD.	P80	MOVIL INTEGRADO	- OLIMPIA MANAGEMENT S.A	ANEXO TEC. 2 V1	28/11/2018	
4	IDENTICA	IDENTICA	ID MATCH 5 Wifi E3	MOVIL WIFI - NO INTEGRADO	IDENTICA S.A.	ANEXO TEC. 2 V1	26/03/2018	
5	IDENTICA	IDENTICA	ID MATCH 3 V2 E3	USB ESTACIONES FIJAS	- IDENTICA S.A.	ANEXO TEC. 2 V1	20/03/2018	
6	CHAINWAY	SHENZHEN CHAINWAY INFORMATION TECHNOLOGY CO., LTD.	CHAINWAY C71 OPTICAL FINGERPRINT	MOVIL INTEGRADO	- OLIMPIA MANAGEMENT S.A	ANEXO TEC. 2 V1	16/11/2017	
7	DYDEX-HS-SAS	RM SECURITY PRODUCTS	BIOVERIF-IOT WIFI	MOVIL WIFI - NO INTEGRADO	DYDEX-HS-SAS	ANEXO TEC. 2 V1	23/08/2017	
					Resellers autorizados:			

¹¹⁷ (IBID, 2020)

					<ul style="list-style-type: none"> • Informática El Corte Inglés (IECISA) 			
					<ul style="list-style-type: none"> • Inversiones Tecnológicas de América S.A. 			
8	BLUEBIRD	BLUEBIRD	RT080 iBio	MOVIL INTEGRADO	- WIRELESS & MOBILE WM	ANEXO TEC. 2 V1	8/08/2017	
9	BLUEBIRD	BLUEBIRD	EF500 iBio	MOVIL INTEGRADO	- WIRELESS & MOBILE WM	ANEXO TEC. 2 V1	4/08/2017	
10	MORPHO	MORPHO S.A.	MORPHO TABLET 2	MOVIL INTEGRADO	- MORPHO	ANEXO TEC. 2 V1	14/06/2017	
11	SUPREMA	SUPREMA INC.	BIOMINI SLIMS	USB ESTACIONES FIJAS	- KANAL SUPREMA COLOMBIA SAS	ANEXO TEC. 2 V1	1/06/2017	
					Resellers autorizados:			
					<ul style="list-style-type: none"> • Informática El Corte Inglés (IECISA) 			
					• Certicámara			
					• Homini			
					• Blueontech			
					• Simobi			
12	MORPHO	MORPHO S.A.	MSO-1300 E3	USB ESTACIONES FIJAS	- MORPHO	ANEXO TEC. 2 V1	5/04/2017	

Fuente: Registraduría Nacional Del Estado Civil, Colombia - Dispositivos Biométricos.. (2020)¹¹⁸

¹¹⁸ (IBID, 2020)

CONCLUSIONES

Esta monografía proporciono un enriquecimiento individual ya que, gracias a la elaboración de este documento se generó una serie de conocimientos como futuro especialista en seguridad informática. De esta manera, con los resultados obtenidos de esta investigación, en relación con la biometría y la seguridad informática en los métodos de autenticación podemos concluir un análisis general de los capítulos anteriores de este documento. La biometría es exclusiva de las personas, lo que la convierte en una forma confiable y segura para la autenticación. Conjuntamente, su gran variedad de métodos de reconocimiento ya sea por rasgo fisiológicos como huellas dactilares, facial, iris entre otros y de comportamiento como firma y movimiento de labios, le permiten a esta herramienta que por medio de dispositivos automatizados reconozcan y verifiquen la identidad de un individuo. Además, la autenticación basada en biometría ha atraído considerable atención por su precisión, confiabilidad, universalidad y permanencia. Los sistemas basados en tecnología tienen sus limitaciones y la biometría no es la excepción. La identificación biométrica ofrece un mundo de diversos usos, sin embargo, también cuenta con algunas desventajas que deben considerarse, La principal puede ser que no se puede cambiar su información biométrica. Entonces, una vez que otra persona tiene la información, ya no es privada. En el caso de la biometría conductual, el hecho de que dependa un poco de su estado de ánimo, su actividad y su salud puede ser una desventaja, ya que puede influir en el FAR (índice de falsa aceptación).

Sin embargo, las desventajas no se comparan con los grandes beneficios que ofrece la biometría. A medida que esta tecnología evoluciona, se vuelve más sofisticada y sus mecanismos de autenticación más seguros para cada sistema de reconocimiento. Hemos determinado que la identificación biométrica para la autenticación individual es rápida y puede identificar instantáneamente a cualquier persona en segundos. Los sistemas de reconocimiento biométrico han demostrado ser precisos y muy efectivos en diversas aplicaciones. La creciente popularidad de esta tecnología atrae la atención de quienes buscan otra capa de seguridad dando como resultado experiencias de autenticación sin la necesidad de tener un objeto o recordar contraseña.

En mi opinión esta herramienta ofrece eficiencia y mayor fiabilidad. No es sorprendente que en los últimos años diversas organizaciones gubernamentales y privadas del territorio nacional hayan implementado sistemas de autenticación biométrica con la finalidad de mejorar su proceso y garantizar seguridad de ellos. De la investigación realizada, concluimos que las personas ya están comenzando a familiarizarse con el sistema biométrico. Además, las personas se sienten más cómodas usando estas tecnologías como mecanismo de autenticación que las tradicionales. De esta manera, estas tecnologías desempeñan un papel muy importante en la seguridad al proporcionar soluciones altamente seguras de identificación y verificación personal.

RECOMENDACIONES

Se recomienda que las pequeñas y medianas empresas que no han implementado esta herramienta migren a esta tecnología, existen sistemas adecuados para controlar el acceso a ubicaciones físicas, registrar las horas y la asistencia de los empleados y visitantes esto con la finalidad ahorrar dinero y operar de manera más eficiente. Asimismo, para implementar esta tecnología, se deben considerar algunos aspectos de la infraestructura tecnológica en la organización.

Las organizaciones privadas y estatales deben tener mucho cuidado al procesar y almacenar datos biométricos, estos datos deben clasificarse como críticos, sensibles y las entidades deben implementar diversos mecanismos estrictos para garantizar la confidencialidad de dicha información. El almacenamiento adecuado de los datos biométricos comienza con la encriptación de dicha información. El almacenamiento de los datos biométricos en un lugar genera preocupaciones sobre las consecuencias de seguridad si el sitio está o es vulnerado. Si bien los datos biométricos son difíciles de falsificar y utilizar en ataques, como futuro especialista en seguridad en informática desde mi punto de vista, se deben reducir las posibilidades de que los atacantes puedan acceder a esta información. Por esta razón, los datos biométricos deben almacenarse en múltiples ubicaciones como parte de una estrategia de seguridad.

Los sistemas de identificación biométrica se proponen como una alternativa más segura a los sistemas clásicos de autenticación basados en conocimiento o en objetos. Los dispositivos como computadoras portátiles, tabletas y teléfonos móviles de gama baja y media tienen escáneres de reconocimiento biométrico. Muchos usuarios desconocen esta función de seguridad que les proporciona estos dispositivos, que pueden usar como método de autenticación para acceder a su terminal y a las aplicaciones.

REFERENCIAS BIBLIOGRÁFICAS

ANIL K. Jain. PATRICK Flynn. ARUN A. Ross. Handbook of Biometrics # ed 1. New York: ed. Springer Science+Business Media, LLC, 2007 151 p. ISBN: 978-0-387-71041-9.

AMARAÑÓN GONZALO, Álvarez. Seguridad Informática Para La Empresa Y Particulares. # ed. MADRID: MCGRAW-HILL, 2004. 96 p. ISBN: 84-481-4008-7.

ASOCIACIÓN GENERAL DE CONSUMIDORES, Dispositivos electrónicos [sitio web]. Madrid: ASGECO; [Consulta: 01 abril 2020]. Disponible en: <http://asgeco.org/consumeoriginal/dispositivos-electronicos/>

CENTRO CRIPTOLÓGICO NACIONAL, GUÍA DE SEGURIDAD - GLOSARIO Y ABREVIATURAS [sitio web]. Madrid. ccn-cert [Consulta: 08 abril 2020]. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html

COSTAS SANTOS, Jesús, Seguridad Informática. # ed. 1. Madrid: Ra-Ma S.A. Editorial y Publicaciones, 2010. 55 p. ISBN: 978-84-9964-313-7

El Economista, ¿Qué y cuáles son los datos biométricos? [sitio web]. México: León A. Martínez [Consulta: 22 abril 2020]. Disponible en: <https://www.eleconomista.com.mx/tecnologia/Que-y-cuales-son-los-datos-biometricos-20180529-0068.html>

ERZIN, Engin & YEMEZ, Y. & TEKALP, A. & ERCIL, Aytul & ERDOGAN, Hakan & Abut, H.. (2006). Multimodal Person Recognition for Human-Vehicle Interaction. Multimedia, IEEE. 13(2). 18 - 31. 10.1109/MMUL.2006.37.

GARCIA ORTEGA, Javier, ALONSO FERNANDEZ, Fernando. BELMOTE COOMONTE, Rafael. Briometria y Seguridad # Ed 1. Madrid, Ed: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones, 2008 31 p. ISBN: 978-84-7402-350-3.

PORTANTIER, Fabian. Seguridad Informática, Gestión de la Seguridad En: USERS. 2012. vol. 1. no. 192, p. 38.

PORTANTIER, Fabian. Seguridad Informática, Gestión de la Seguridad En: USERS. 2012. vol. 1. no. 192, p. 12.

fintechgracion, fintechgracion [sitio web]. Scottsdale: fintechgracion; [Consulta: 01 mayo 2020]. Disponible en: https://www.fintechgracion.com/wp-content/uploads/Fintechgracion_Libro_VersionExtendida.pdf

Hewlett Packard, ¿Qué Es El Almacenamiento De Datos? [sitio web]. Delhi: Hewlett Packard Enterprise Development LP [Consulta: 13 mayo 2020]. Disponible en: <https://www.hpe.com/es/es/what-is/data-storage.html>

Instituto Nacional de Ciberseguridad, Glosario de términos de ciberseguridad [En Línea]. Ciudad: Madrid. Autores: INCIBE 2017; Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

Instituto Nacional de Ciberseguridad, Glosario de términos de ciberseguridad [sitio web]. Madrid: INCIBE [Consulta: 08 abril 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

ISO27000, ¿GLOSARIO? [sitio web]. Roubaix: iso27000; [Consulta: 15 abril 2020]. Disponible en: <http://www.iso27000.es/glosario.html>

Ministerio de Tecnologías de la Información y las Comunicaciones, Modelo de Seguridad y Privacidad de la Información [sitio web]. Bogota: Mintic [Consulta: 016 abril 2020]. Disponible en: https://www.mintic.gov.co/gestioni/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Observatorio tecnológico, Sistemas físicos y biométricos de seguridad [sitio web]. Madrid: Elvira Misfud [Consulta: 25 abril 2020]. Disponible en: <http://recursostic.educacion.es/observatorio/web/fr/cajon-de-sastre/38-cajon-de-sastre/1045-sistemas-fisicos-y-biometricos-de-seguridad>

PWC, Fraude al descubierto Encuesta Global Crimen Económico 2018 Colombia [sitio web]. Bogotá: PwC [Consulta: 26 abril 2020]. Disponible en: https://www.pwc.com/co/es/assets/document/crimesurvey_2018.pdf

RCN Radio, El 60% de las entidades financieras del país usan la autenticación biométrica [sitio web]. Bogotá: RCN [Consulta: 04 abril 2020]. Disponible en: <https://www.rcnradio.com/colombia/el-60-de-las-entidades-financieras-del-pais-usan-la-autenticacion-biometrica>

Registraduría Nacional del Estado Civil de Colombia, Identificación Biométrica: cada vez con más Usos En La Vida Cotidiana [sitio web]. Bogotá.: Registraduría Nacional del Estado Civil de Colombia [Consulta: 03 abril 2020]. Disponible en: <https://www.registraduria.gov.co/Identificacion-biometrica-cada-vez.html>

Registraduría Nacional del estado civil, Autenticación biométrica en Colombia. [sitio web]. Ciudad: Bogotá. Autores: Registraduría Nacional del estado civil [Consulta: 05 mayo 2020]. Disponible en: <https://web.certicamara.com/media/221765/autenticacion-biometrica-en-colombia.pdf>

Superintendencia de Industria y Comercio, ¿Protección de Datos Personales? [sitio web]. Bogotá: SIC [Consulta: 03 mayo 2020]. Disponible en: <https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>

Universidad Nacional Autónoma de México - Revista Digital Universitaria, El Fraude y la Delincuencia Informática: Un Problema Jurídico y Ético [sitio web]. México: Begoña Albizuri. [Consulta: 11 abril 2020]. Disponible en: <http://www.revista.unam.mx/vol.3/num2/art3/>

USERS. Hacking desde Cero - Seguridad Física y Biometría En: USERS. 2011. vol. 1. no. 66, p.

ANEXOS

RESUMEN ANALÍTICO ESPECIALIZADO – RAE

1. INFORMACIÓN GENERAL

Título	Biometría y la Seguridad Informática en los Métodos de Autenticación
Autor	Jonny Julián Sánchez Gómez
Tipo de documento	Monografía
Director	Martin Camilo Cancelado Ruiz
Año	2020
Palabras clave	Autenticación, Biometría, Dispositivo, Identificación, Información, Ley, Políticas, Regulación, Seguridad Informática, Sistemas, Tecnología, Vulnerabilidades,

2. RESUMEN

Esta monografía hace parte del trabajo de grado para optar a el título de especialista en seguridad informática. En este documento se ha investigado sobre, los diferentes dispositivos biométricos que existen hasta el día de hoy. El proceso de probar la identidad de una persona se conoce como los mecanismos de autenticación, el propósito de esta investigación es, ayudar a fortalecer la seguridad informática de los usuarios, instituciones y organizaciones. Los sistemas biométricos establecen tres pilares fundamentales los cuales son: confidencialidad, integridad y disponibilidad, la biometría es una herramienta tecnológica que nos permite reconocer y autenticar los individuos basándose en sus características biológicas y de comportamiento. Actualmente estos sistemas biométricos permiten a las empresas realizar sus procesos de una forma más segura y rápida, garantizando a las empresas una mayor productividad. Las organizaciones buscan diferentes mecanismos para proteger la información, si bien los métodos tradicionales son efectivos también tienen sus inconvenientes; como claves que se olvidan o que son muy fáciles de descifrar, o el fraude realizado por algún miembro de la familia. Pero como todos los avances tecnológicos no todo es perfecto, estos también tienen sus ventajas y desventajas y aunque el sistema biométrico es más difícil de vulnerar, se debe estar en continua investigación e innovación tecnológica para así poder estar preparados ante cualquier ataque que pueden realizar al sistema donde la información que se halla obtenida o almacenada en una base de datos puedan ser robados o hackeados.

3. DESCRIPCIÓN DEL PROBLEMA DE INVESTIGACIÓN

Las organizaciones hoy en día buscan diferentes mecanismos para contrarrestar el fraude o los ataques phishing o la suplantación de identidad, y han experimentado en algún momento un ataque a su sistemas o un ciberataque, una de las medidas adoptadas por algunas organizaciones es la biometría para ayudar a mitigar esta situación y tratar de proteger sus bases de datos, si bien es cierto los métodos de identificación tradicionales son efectivos pero por lo general son molestos e incómodos y también presentan debilidades los cuales afectan a los usuarios. Entonces es en esos momentos cuando nos hacemos la pregunta ¿son estos sistemas realmente más seguros que los métodos tradicionales de gestión de identidad? ¿podrían poner en riesgo la seguridad y la privacidad de la información del usuario? Aunque la tecnología ha avanzado ¿son los procesos biométricos 100% seguro? y ¿son los sistemas biométricos perfectos? Hay otro tema a considerar y es la confiabilidad de la biometría. Las caras cambian con la pérdida o ganancia de peso, y las personas se ven diferentes a medida que envejecen. Las huellas digitales, si bien son exclusivas de las personas, también tienen similitudes. ¿Y qué hay de cortes o quemaduras en un dedo? ¿Es realmente un sistema tan perfecto para la autenticación?

4. OBJETIVOS

Describir el funcionamiento de los diferentes sistemas biométricos y sus procesos de autenticación, verificación y almacenamiento de datos los cuales garanticen que la información sea confiable, precisa y rápida

- Exponer el funcionamiento de la autenticación en los diferentes mecanismos de los sistemas biométricos en la seguridad informática.
- Determinar las ventajas y desventajas de autenticación en los diversos sistemas de biométricos en la seguridad informática.
- Establecer los riesgos asociados con el uso de esta herramienta tecnológica en el ámbito de la seguridad informática.
- Investigar la efectividad y la eficiencia de la autenticación con el uso de los sistemas biométricos en la seguridad informática.

5. METODOLOGÍA

Para esta investigación recurrimos y utilizamos la investigación con documentos cualitativos y material digital y audiovisual. El tipo de investigación que se aplicó fue documental argumentativo explicativa para así poder alcanzar los objetivos de este documento monografía

6. PRINCIPALES REFERENTES TEÓRICOS Y CONCEPTUALES

Capítulo 1 biometría y la seguridad informática en los métodos de autenticación. Las organizaciones están en la búsqueda de diferentes mecanismos que ayuden a contrarrestar el fraude y los ataques cibernéticos para proteger la información que tiene en sus bases de datos, en la seguridad existen factores de autenticación: algo que el usuario sabe, algo que tiene el usuario o algo que es el usuario, En esta monografía se pretende realizar una investigación, un análisis y una interpretación en relación con los diferentes sistemas biométricos, ya que, en estos, se puede hacer uso de una gran variedad de características fisiológicas y morfológicas de las personas. Los beneficios de estos sistemas, la privacidad, el control a su acceso y la veracidad de los datos

Capítulo 2: Para la comprensión de los diferentes aspectos que comprende esta monografía, se hace necesario la definición de algunos conceptos como son autenticación, biometría, confidencialidad, contraseña, control, datos biométricos, datos personales, disponibilidad, dispositivo electrónico, fraude informático, descritos en este capítulo, de igual forma, muchos de nosotros creíamos que la biometría solo consistía en la lectura de huellas digitales, pero no, la realidad es que los sistemas biométricos abarca muchos métodos de reconocimiento de personas basados en propiedades fisiológicas o de conducta. Como toda tecnología la biometría presenta desventajas entre las cuales podemos encontrar la privacidad de los datos biométricos. Igualmente, Esta tecnología esta supervisada por organización internacionales que se encargan el desarrollo de estándares, mecanismo y técnicas para el desarrollo, la implementación y el uso para cada uno de los sistemas de reconocimiento. Asimismo, en Colombia existe una normativa legal para la implementación y uso de estos sistemas de información biométricos en las entidades gubernamentales y privados. Los sistemas biométricos es una industria en constante evolución. De esta manera, esta tecnología ha sido valorada en los últimos años en el mercado mundial, esta tecnología se destaca por proporcionar un alto nivel de seguridad en los sectores privado, público y comercial

Capítulo 3: Actualmente una variedad de sectores como entidades e instituciones gubernamentales y privadas, han implementaron y utilizan en sus diferentes procesos de operaciones el uso de sistemas de reconocimiento biométricos. Un ejemplo claro son las entidades bancarias, que los últimos cinco años han hecho de esta tecnología un aliado para agilizar sus procesos, evitar el fraude y la suplantación de identidad, igualmente la Registro

Nacional de Estado Civil es la gestión y el permiso para acceder a las entidades públicas y las personas que ejercen funciones públicas confrontar en línea a través del sistema de autenticación biométrica, la información sobre las huellas digitales de los ciudadanos con la información contenida en base de datos, la registraduría solicita ciertos requisitos legales y tecnológicos a las organizaciones con el fin de cumplimiento a los estándares internacionales. El número de acuerdos para acceder a las bases de datos crece anualmente, lo que se revela en los informes de gestión de los últimos 5 años de esta entidad.

8. CONCLUSIONES

La investigación sobre los sistemas biométricos y la seguridad informática han dejado una serie de conocimiento y enriquecimiento acerca de este tema. La biometría es exclusiva de las personas, lo que la convierte en un sistema confiable y seguro para la autenticación de las personas, su gran variedad de métodos de reconocimiento ya sea por rasgos fisiológicos o de comportamiento Sin embargo, las desventajas no se comparan con los grandes beneficios que ofrece la biometría. A medida que esta tecnología evoluciona, se vuelve más sofisticada y sus mecanismos de autenticación más seguros para cada sistema de reconocimiento. esta herramienta ofrece eficiencia y mayor fiabilidad. No es sorprendente que en los últimos años diversas organizaciones gubernamentales y privadas del territorio nacional hayan implementado sistemas de autenticación biométrica con la finalidad de mejorar su proceso y garantizar seguridad de ellos.

9. RECOMENDACIONES

Se recomienda que las pequeñas y medianas empresas que no han implementado esta herramienta migren hacia esta tecnología, existen sistemas adecuados para controlar el acceso a ubicaciones físicas, registrar las horas y la asistencia de los empleados y visitantes esto con la finalidad ahorrar dinero y operar de manera más eficiente. Sin embargo, es bueno que las organizaciones tengan mucho cuidado al procesar y almacenar datos biométricos. Los sistemas biométricos se proponen como una alternativa a los demás sistemas de autenticación que se basan en conocimientos u objetos, aunque muchas personas desconocen las bondades de este método de autenticación

9. REFERENCIAS

fintechgracion, fintechgracion [sitio web]. Scottsdale: fintechgracion; [Consulta: 01 mayo 2020]. Disponible en: https://www.fintechgracion.com/wp-content/uploads/Fintechgracion_Libro_VersionExtendida.pdf

Registraduría Nacional del Estado Civil de Colombia, Identificación Biométrica: cada vez con más Usos En La Vida Cotidiana [sitio web]. Bogotá.: Registraduría Nacional del Estado Civil de Colombia [Consulta: 03 abril 2020]. Disponible en: <https://www.registraduria.gov.co/Identificacion-biometrica-cada-vez.html>

Registraduría Nacional del estado civil, Autenticación biométrica en Colombia. [sitio web]. Ciudad: Bogotá. Autores: Registraduría Nacional del estado civil [Consulta: 05 mayo 2020]. Disponible en: <https://web.certicamara.com/media/221765/autenticacion-biometrica-en-colombia.pdf>

PWC, Fraude al descubierto Encuesta Global Crimen Económico 2018 Colombia [sitio web]. Bogotá: PwC [Consulta: 26 abril 2020]. Disponible en: https://www.pwc.com/co/es/assets/document/crimesurvey_2018.pdf