VERIFICACION DEL PROCESO DE AUTENTICACIÓN BIOMÉTRICA EN ENTIDADES BANCARIAS, COMO HERRAMIENTA PARA LA PREVENCIÓN DE FALSEDAD PERSONAL

STEPHANIE JULIETTE RÍOS RODRIGUEZ

Tutor temático

Mauricio Ernesto Rojas Fierro

Tutor metodológico

Juan Manuel Silva García

UNVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE LAS RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD

DIRECCIÓN DE POSGRADOS

ESPECIALIZACION EN ADMINISTRACIÓN DE LA SEGURIDAD

2019

Verificación del proceso de autenticación biométrica en entidades bancarias, como herramienta para la prevención de falsedad personal

Resumen

En Colombia las personas que acceden a productos y servicios bancarios, se han visto flageladas por delitos como: la falsedad personal, la falsedad en documento privado y la falsedad en documento público, pues los delincuentes encuentran técnicas para suplantar las huellas y falsificar documentos públicos y privados, que una entidad bancaria solicita como requisito para el otorgamiento de préstamos, tarjetas de crédito o débito, generación de cheques, transferencias, entre otros.

Con la finalidad de prevenir el delito de falsedad personal y fraude en documento público (cedula de ciudadanía), la mayoría de entidades bancarias en Colombia, ya migró sus procesos de identificación y autentificación personal de clientes, a procesos tecnológicos de autenticación biométrica, ya que es una de las varias alternativas, que brinda marcadas mejoras de usabilidad y rendimiento, mejorando las garantías de seguridad.

Este ensayo se basa en la verificación del proceso de los protocolos de reconocimiento e identificación biométrica, basados en la huella dactilar en entidades bancarias que ya ostentan como método de identificación y autenticación en sus productos y servicios, la biometría dactilar y que adicionalmente tienen una base de datos biométricos dactilares propia, alimentada únicamente por personas que son o han sido clientes con cualquier producto de la entidad bancaria.

En este, se describirán los principales riesgos recopilados a través de la experiencia profesional en la identificación y autentificación de la biometría dactilar. Y se identificaran factores claves que contribuyen al éxito de un sistema biométrico dactilar para los servicios bancarios. Para cada factor, se describirán las principales tendencias que deben analizarse antes de la utilización. Los factores proporcionan una gama de pautas y consideraciones necesarias para el despliegue de la biometría dactilar al servicio del sector bancario.

Palabras clave: Biometría, prevención, dactiloscopia, identificación, enrolamiento, suplantación de personas, autentificación.

Abstract

In Colombia, people who access banking products and services have been flogged for crimes such as: personal falsehood, falsity in private document and falsity in public documents, as criminals find techniques to supplant forge public and private documents, which a bank requests as a requirement for the granting of loans, credit or debit cards, check generation, transfers, among others.

In order to prevent the crime of personal falsity and fraud in public document (identification card citizen ship), most banks in Colombia, have already migrated their processes of identification and personal authentication of customers, to technological processes of biometric authentication, since it is one of several alternatives, which provides marked improvements in usability and performance, improving security guarantees.

This test is based on the verification of the process of biometric recognition and identification protocols, based on fingerprinting in banks that already have as a method of identification and authentication in their products and services, fingerprint biometrics and which additionally have their own digital biometric database, fed only by people who are or have been customers with any product of the bank.

This will describe the main risks collected through professional experience in the identification and authentication of fingerprint biometrics. And key factors contributing to the success of a biometric fingerprint system for banking services will be identified. For each factor, the main trends to be analyzed before use will be described. Factors provide a range of guidelines and considerations necessary for the deployment of fingerprint biometrics to serve the banking sector.

Keywords: Biomethyria, prevention, fingerprint, identification, enrolment, impersonation of people, authentication.

Introducción

El sector bancario colombiano tiene un flujo constante en los productos y servicios que ofrece, los usuarios o clientes interactúan y obtienen dichos productos y servicios , ya sea a través de canales digitales o los más comunes y tradicionales, de forma presencial en sus oficinas.

Con el auge de la virtualidad y la competencia entre entidades bancarias, para obtener potenciales clientes de manera rápida y ágil, uno de los mecanismos de seguridad que las entidades han implementado para el control de falsedad personal, está fundamentado en la identificación de una persona, mediante biometría a través de su huella dactilar.

La inclusión de esta tecnología, se ha convertido en una barrera que dificulta a los suplantadores defraudar a las entidades bancarias, sin embargo cada vez se identifican nuevas técnicas y mecanismos para suplantar las huellas dactilares de personas de bien y con ello cometer los delitos de falsedad personal y falsedad de documento privado, y así solicitar los diferentes productos bancarios para beneficio del delincuente.

El crecimiento de la falsedad material en documento público y falsedad personal o suplantación de identidad, en la autenticación de servicios, productos y operaciones bancarias, se ven evidenciados en las cifras de la Fiscalía, ya que de enero a julio de 2017 se registraron 10.985 casos, mientras que en ese mismo periodo del 2018 se reportaron 14.411 casos, lo que significa un aumento del 31,19%. (Manrique, 2018).

Hoy en día, los proveedores de servicios biométricos están en una constante innovación para revelar vectores de fraude y no permitir que ese tipo de delitos se materialicen. Y la Ley de Habeas Data por su parte, se encarga de la protección de datos que son confidenciales y no pueden usarse para otra cosa so pena de cometer un delito, aportando de esta manera un plus en aspectos de seguridad. Entonces, aunque es técnicamente posible ser suplantado, pueden aplicarse mecanismos y procesos preventivos dentro de las entidades bancarias para disminuir la comisión de dichos delitos.

El auge de la criminalidad y los avances tecnológicos, han permitido a los delincuentes crear técnicas que van a la vanguardia de los sistemas de identificación y autenticación de personas, creando así, brechas en los sistemas de seguridad y permitiendo con ello, la realización

de delitos relacionados con el hurto, falsedad en documento (privado y público) y falsedad personal.

La materialización de los delitos por parte de delincuentes se configura de la siguiente manera: cuando una persona se acerca a un banco a solicitar un producto, las entidades bancarias realizan unas exigencias de algunos documentos públicos y privados, y solicitan realizar la captura o enrolamiento de la huella dactilar, este procedimiento se puede realizar de dos formas: la primera por medio electrónico (biométrico) y la segunda y más tradicional, es la toma de las huellas a través del entintado de la falange distal y posterior plasmado en un documento. Es aquí precisamente en este punto, de la toma o enrolamiento de las huellas donde los delincuentes tratan constantemente de vulnerar la seguridad.

Es preciso entonces verificar, si son eficaces los procesos o técnicas utilizadas en las entidades bancarias, para la obtención y recopilación de huellas dactilares que identifican y permiten la autentificación personal de los clientes, para evitar el riesgo de ocurrencia de los delitos mencionados anteriormente.

Es por esto, que resulta relevante verificar los riesgos, analizar la temática y sentar los precedentes para que se tengan en cuenta las posibles modalidades y técnicas que utilizan los delincuentes para suplantar y robar identidad, durante el proceso de seguridad de la toma o enrolamiento de huellas.

Es necesario en este punto preguntarse si son efectivos los procesos o técnicas utilizadas en las entidades financieras, para la obtención y recopilación de huellas dactilares que identifican y permiten la autentificación personal de los clientes, para evitar el riesgo de ocurrencia de los delitos relacionados con el robo y la falsedad de identidad.

Objetivo general

Identificar los riesgos en los procedimientos de obtención o toma de huellas dactilares (por medios electrónicos y físicos), utilizadas para la identificación y autentificación personal de los usuarios o posibles clientes, en las entidades bancarias que utilizan la biometría dactilar como

herramienta para garantizar al auténtica identidad de quien se presenta como usuario o cliente para la obtención de cualquier producto o servicio. .

Objetivo específicos

- Describir las técnicas y métodos utilizados por los delincuentes, para burlar la seguridad en los procesos que realizan las entidades financieras, en la obtención o toma de huellas dactilares (enrolamiento) y permiten la autentificación personal de los usuarios o clientes.
- Determinar los factores que permiten y potencian la ocurrencia de hechos delictivos relacionados con el fraude por suplantación de personas..
- Generar las recomendaciones de seguridad pertinentes a tener en cuenta para la aplicación de procesos o técnicas para el enrolamiento, procesamiento, análisis y resultado en el proceso de autenticación biométrica, para prevenir la falsedad personal y de documento publico

Desarrollo

Los procesos bancarios y su relación con el delito de falsedad personal y falsedad material en documento público

Las entidades bancarias han creado unas políticas y procesos, que realizan áreas internas específicas, para poder otorgar a las personas los productos y servicios que la misma ofrece. Dentro de los productos y servicios se encuentran, las distintas líneas de crédito (vivienda, consumo, leasing, libre inversión, libranza, vehículos, entre otros), y las operaciones y servicios bancarios (consignaciones, transferencias, consulta de productos, etc.). Para el presente ensayo, se tomará específicamente la etapa relacionada con la obtención y toma de huellas dactilares para cualquiera de las etapas de autentificación de identidad de los productos y servicios mencionados con anterioridad.

El procedimiento para la obtención de un producto o servicio bancario, como un crédito, se presenta de la siguiente manera: inicialmente la persona se acerca a un banco a solicitar el

producto, la entidad posee unas exigencias de documentos públicos y/o privados, llenar unos formatos propios de la entidad y realizar la captura o enrolamiento de la huella dactilar, este último procedimiento se puede realizar de dos formas: la primera por medio electrónico (biométrico) y la segunda es la toma de las huellas a través del entintado de la falange distal y posterior plasmado en uno o los documentos que sean necesarios. Posteriormente el área específica de la entidad bancaria realizara un estudio de todos los documentos y datos solicitados y brindara una resolución positiva o negativa del mismo.

Figura 1. Esquema general del proceso de solicitud de un crédito en una entidad bancaria, en rojo proceso específico sobre el que trata este ensayo.

La delincuencia organizada ha encontrado distintas maneras y técnicas que se mencionaran más adelante, para realizar la suplantación de las huellas de una persona en el proceso de obtención de un producto, las entidades bancarias han respondido a estos eventos con métodos preventivos, desde la contratación de dactiloscopistas, documentólogos, capacitación del personal relacionado, automatización de software y traslado de verificación de identidad a terceros. Sin embargo, algunos eventos terminan siendo positivos para los delincuentes, porque en algún momento del enrolamiento y/o captura de las huellas, se permitió consciente o inconscientemente la apertura de una brecha para la materialización del delito.

Es importante en esta etapa relacionar los delitos que se presentan con la materialización de la suplantación de identidad, a través de la reproducción de las huellas dactilares en la solicitud de productos bancarios. El delito sobre el cual está fundamentado este ensayo es la falsedad personal. El *Código penal colombiano* en su Artículo 296, describe la conducta de falsedad personal: **“**El que con el fin de obtener un provecho para sí o para otro, o causar daño, sustituya o suplante a una persona o se atribuya nombre, edad, estado civil, o calidad que pueda

tener efectos jurídicos, incurrirá en multa, siempre que la conducta no constituya otro delito". En este caso se tratará la falsedad personal a través de la reproducción de huellas dactilares para la solicitud de productos bancarios.

El otro delito relacionado es la falsedad material en documento público, el Artículo 287 del *Código penal colombiano* expresa: falsedad material en documento público: "El que falsifique documento público que pueda servir de prueba, incurrirá en prisión de cuarenta y ocho (48) a ciento ocho (108) meses. "Si la conducta fuere realizada por un servidor público en ejercicio de sus funciones, la pena será de sesenta y cuatro (64) a ciento cuarenta y cuatro (144) meses e inhabilitación para el ejercicio de derechos y funciones públicas de ochenta (80) a ciento ochenta (180) meses".

La comisión de este delito es una de las más frecuentes formas utilizadas por los delincuentes para suplantar la identidad de una persona mediante la falsificación o adulteración de la cedula de ciudadanía, el cual es un documento público. En cuanto a lo que compete a este artículo se menciona este delito, porque para la falsificación y/o adulteración de las cedulas se realiza la suplantación de identidad de las personas, a través de la reproducción de las huellas dactilares plasmadas en las cedulas; pero este tema de la falsificación y adulteración de cedulas no será tratado a profundidad en este documento.

En adelante se dará un recorrido con temas íntimamente relacionados con las huellas dactilares y los procesos biométricos, hasta llegar a las técnicas utilizadas por los delincuentes para la reproducción de las huellas dactilares y la comisión del delito de falsedad personal.

Inicios de la biometría

En 1882, Alphonse Bertillone, quien se desempeñaba como policía en Francia, presento el primer sistema de identificación de las personas, basándose en las características físicas de cada individuo, para lo cual creo una ficha de filiación en donde plasmaba medidas antropométricas de cada individuo, Se trataba de una técnica de identificación de criminales basada en la medición de varias partes del cuerpo y la cabeza, marcas individuales, tatuajes, cicatrices y características personales del sospechoso (Rhodes, 1956). Aunque este método tuvo gran auge durante la época, fue desprestigiado con el caso de Will West y William West en 1903.

En 1892, Juan Vucetich resuelve un crimen por medio de la identificación de huellas dactilares encontradas en la escena del crimen en una provincia de Buenos Aires, Argentina. Para 1893, el Ministerio del interior del Reino Unido reconoció oficialmente que dos personas no podían tener las mismas huellas dactilares, con ello, muchos departamentos policiales implementaron la identificación dactiloscópica para identificar criminales o infractores que a menudo cambiaban su nombre e infringían la ley reincidentemente. En la década de 1980, surgen los Sistemas Automatizados de Identificación de Huellas Dactilares (AFIS**),** el cual es un sistema informático que permite la captura (enrolamiento), consulta y comparación automática de huellas dactilares.

Biometría

Como se pude observar, desde la antigüedad los rasgos biométricos aplicados al servicio de la biometría vienen siendo aceptados como identificadores unívocos de cada individuo, pues cualquier característica del ser humano, tanto psicológica como fisiológica puede ser empleada como rasgo biométrico, siempre que reúna las cualidades siguientes (Antonelli, 2006):

- Universalidad
- Distintividad
- Estabilidad
- Evaluabilidad
- Rendimiento
- Aceptabilidad

Es entonces importante mencionar el concepto de biometría, según la RNEC, La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, como la huella digital que, al ser una característica única de cada individuo, permite distinguir a un ser humano de otro (Registraduria Nacional del Estado civil, 2006)

En la actualidad existen diversos rasgos biométricos que son empleados según su favorabilidad o desfavorabilidad para su aplicación, entre ellos se encuentran, siguiendo a Serratosa (2019):

1. Cara

2. Termograma de rostro

3. Oído

4. Iris

5. Retina

6. Geometría de la mano y dedos

7. Huella dedo y mano

8. Venas de la mano

9. Voz

10. Firma

11. Forma de caminar

12. Manera de teclear

13. Olor

14. ADN

Estos rasgos biométricos son los que se identifican gráficamente, para mayor comprensión, en la Figura 2:

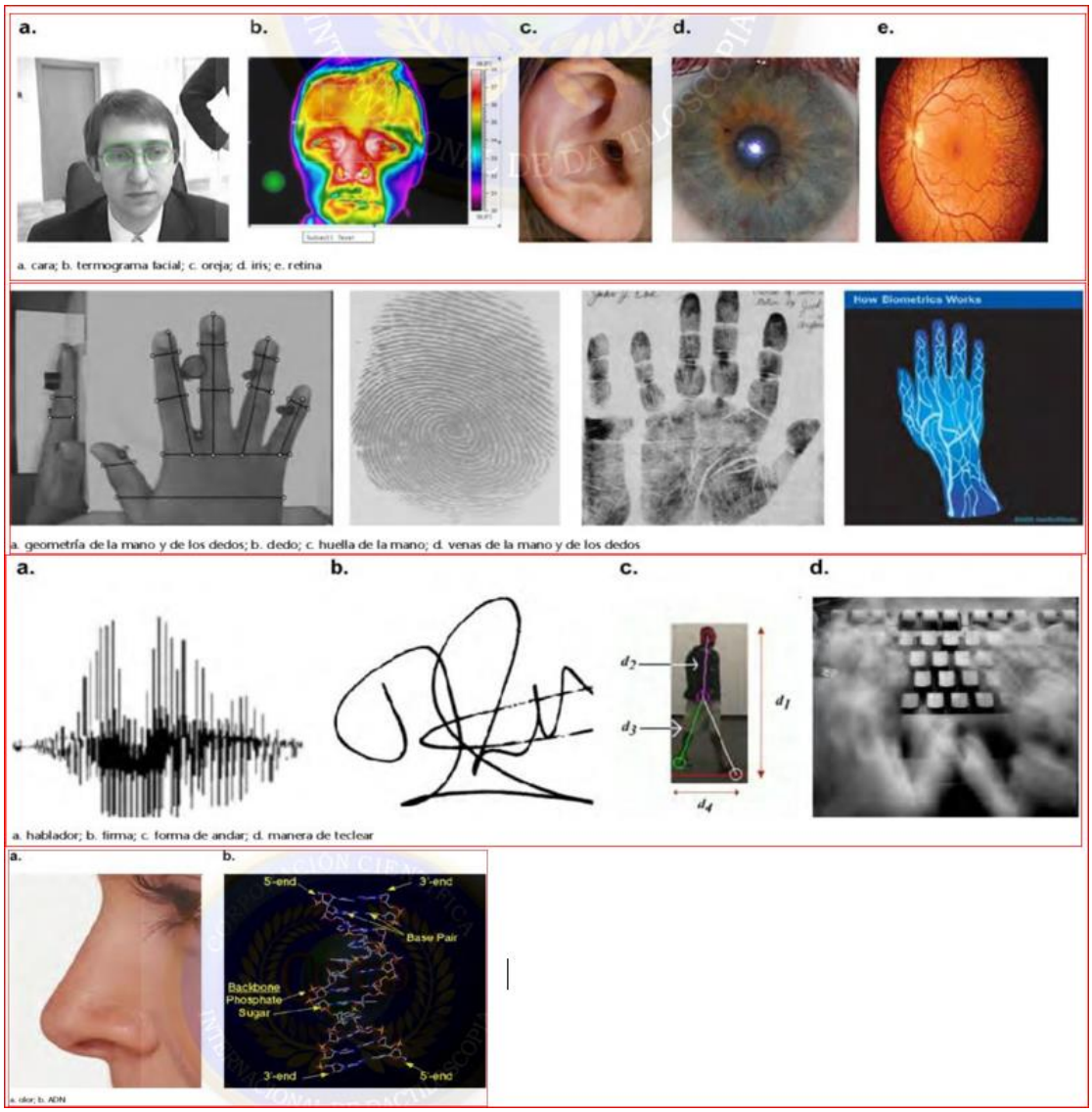

Figura 2. Rasgos Biométricos (Serratosa, 2009).

Un sistema biométrico entonces, se encarga de reconocer patrones para funcionar de la siguiente manera:

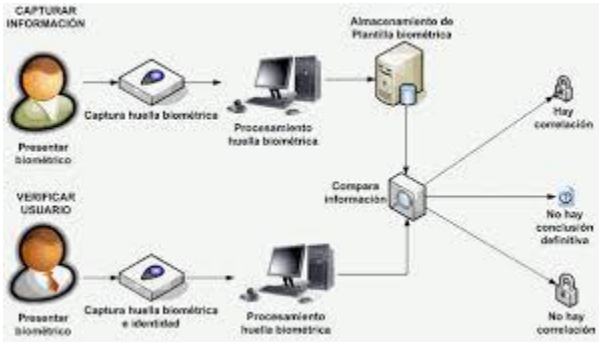

Figura 3. Funcionamiento de un sistema biométrico (Ingenieria biometrica y sus aplicaciones, 20015)**.**

Huellas dactilares

Las huellas dactilares están ubicadas en la falange distal de los dedos de la mano y pies de cada individuo, poseen características de Inmutabilidad, perennidad y diversiformidad. La piel presente en las crestas de fricción posee características de singularidad que acompañan al ser humano durante su vida y hasta el proceso de descomposición después de la muerte.

La base de la singularidad comienza en la gestación del feto, las almohadillas interdigitales aparecen por primera vez, alrededor de 6 semanas de edad gestacional estimada (EGA), seguido de cerca en el tiempo por las almohadillas tenar e hipotenar. Aproximadamente a las 7-8 semanas (EGA), las almohadillas palmares comienzan a desarrollarse en las yemas de los dedos, empezando por el pulgar y progresando hacia el dedo meñique en el mismo gradiente radio cubital seguirá esa formación de la cresta. También en aproximadamente 8 semanas EGA, el pliegue tenar se empieza a formar en la palma, seguido por los pliegues de flexión de los dedos en torno a 9 semanas EGA (Wertheim, 2002).

De esta manera desde la gestación se han formado los dibujos papilares, que no son otra cosa que una característica propia de cada individuo, la cual permite una identificación

inequívoca del mismo. Una huella dactilar es la impresión visible o moldeada que produce el contacto de las crestas papilares (EcuRed).

Las huellas dactilares están formadas por una serie de crestas y surcos, a su vez los surcos presentan características como terminaciones o bifurcaciones de estos, los cuales son llamados “puntos característicos o minucias”; cada uno de estos puntos tiene una peculiaridad y una posición única, que puede ser medida cualitativa y cuantitativamente. Cotejando esta distribución es posible conseguir la plena identidad de una persona. Para la obtención de una huella dactilar sobre una superficie tradicionalmente, se aplica una fina capa de tinta en la punta de los dedos y luego apoyándolos sobre una tarjeta o papel; las crestas quedarán en la reproducción en color negro mientras que los surcos serán los espacios en blanco.

Figura 4. Huella, crestas y surcos (Elaboración propia)

En las entidades financieras se vienen capturando las huellas por medio de dos técnicas, la primera de forma manual y la segunda enrolando por medio de un sensor óptico (Biométrico). Para la forma manual se comprenden las siguientes tareas:

1. Capturar la imagen de la huella dactilar por medio del entintado en la tarjeta.
2. Realizar el respectivo análisis, detectar las 'minucias' (características distintivas) en la imagen plasmada.

3. Comparar un conjunto de datos de minucias de las huellas dactilares del cliente o titular, con la huella plasmada en la cedula de ciudadanía.

Para enrolar e identificar por medio de un sensor óptico, se tendrán en cuenta los siguientes pasos:

1. Inicialmente se realiza un registro del cliente, introduciendo en el sistema los datos personales y el rasgo biométrico, para este caso huellas dactilares, además el sistema extrae características propias y las almacena en la base de datos.
2. Para realizar una verificación de autenticidad el sistema verificara las huellas del individuo comparando su rasgo biométrico con sus rasgos previamente almacenados en la base de datos y en bases de datos que le presten soporte a la entidad.
3. El sistema reconoce o no al cliente a partir de sus rasgos biométricos dentro de una base de datos.

Regulación de la biometría en Colombia

La biometría en Colombia nace en la Ley 38 de 1.993 por la cual se unifica el sistema de dactiloscopia y se adopta la Carta dental para fines de identificación: ARTÍCULO 2o. Para fines de identificación de las personas unificase la dactiloscopia según el sistema utilizado por la Registraduría Nacional del Estado Civil, con base en el registro decadactilar.
PARÁGRAFO: La unificación de los registros dactiloscópicos es obligación de todas las entidades del Estado, de acuerdo con lo expresado en el Artículo 2do de esta Ley.

A partir de la Ley 527 de 1999 y del Decreto 2364 de 2012, se desarrolló el marco jurídico para la identificación electrónica (validación de identidad) y firma electrónica. A demás de ser las normas que facilitan el uso de esta tecnología en medios electrónicos para llevar a cabo tanto procesos de validación de identidad como firma de documentos electrónicos.

Así mismo, se halla vigente el Decreto Ley Anti-trámites que en su artículo 18, establece el uso de huella dactilar en medios electrónicos como mecanismo de identificación, y la necesidad para las entidades públicas y determinados particulares, de comparar la identidad del titular de la huella frente a la base de datos de la Registraduría. (Certicámara, 2019)

Por otro lado, la Resolución Número 8410 del 22 de agosto de 2013, reglamento las condiciones y el procedimiento para la expedición física de la información no sujeta a reserva legal de la base de datos del Archivo Nacional de Identificación (ANI) de la Registraduría Nacional del Estado Civil, que requieran los particulares. Y el Registrador Nacional del Estado Civil expidió la Resolución número 10690 del 23 de septiembre de 2015, por la cual se reglamentan las condiciones y el procedimiento para el acceso a las bases de datos dispuesta por la Registraduría Nacional del Estado Civil, para el uso de los particulares autorizados por la ley, en el proceso de autenticación biométrica.". (Ley38, 1.993)

La Registraduría Nacional del Estado Civil (RNEC) de la Resolución 5633 de 2016 y sus anexos técnicos (resolución 13691 de 2016), reglamenta e imparte instrucciones de acceso a la réplica de la bases de datos de RNEC, la cual es la base de datos biométricos y biográficos más completa, confiable y actualizada del país, la cual cuenta con más de 500 millones de huellas dactilares, de aproximadamente 50 millones de colombianos, y se encuentra blindada por altos estándares de seguridad que brindan garantías de integridad, confidencialidad y disponibilidad de la información, así como por requisitos que aseguran el cumplimiento de las normas de protección de datos personales y hábeas data. (Certicámara, 2019). Es importante mencionar que en esta base solamente se consulta información de personas de nacionalidad colombiana mayores de edad.

Es importante estar al tanto, que la base de datos biométrica de la Registraduría se actualiza a través de otras fuentes de información, entre las que se encuentran, bases de datos de la Fiscalía General de la Nación, de la Policía Nacional, y fuentes internas tales como el Registro Civil y el Archivo Nacional de Identificación, que son útiles, por ejemplo, para establecer si una persona ha fallecido disminuyendo riesgos de suplantación de identidad. (Certicamara S.A, 2019)

En cuanto a la regulación del sector financiero, es la Circular 042 de 2012 de la Superintendencia Financiera de Colombia, la que permite servirse de la biometría como un mecanismo fuerte de autenticación, asegurando la identidad de la persona con un alto grado de confianza (Certicámara, 2019).

Margen de error de la autenticación biométrica en un sistema de base de datos propio de la entidad bancaria

A nivel mundial la dactiloscopia, es una de las ciencias más utilizadas de identificación, la cual permite establecer fehacientemente la identidad de un individuo. En distintas oportunidades se ha mencionado que este método no posee margen de error, ya que ha sido clasificado por encima del ADN y la Carta Dental, siendo un motivo de controversia en el mundo científico (Delgado, Margen de error de la dactiloscopia).

Existen diversos métodos decadactilares de clasificación como son: Henry, Henry Americano, Henry Canadiense, Vucetich, Vucetich Oloris, entre otros, y los programas computarizados de biometría como el AFIS y los creados por empresas privadas. Todos los anteriores sistemas están regidos por fundamentos científicos universales de las crestas dactilares, En dactiloscopia la posibilidad de hallar dos personas con las mismas impresiones dactilares es cero o sencillamente imposible (Delgado, Margen de error de la dactiloscopia)

Los países han implementado sus propias normas y adquirido el sistema de clasificación dactilar que más le conviene, pues la dactiloscopia está fundamentada en principios científicos, los sistemas de clasificación catalogan las huellas dactilares por sus características epidérmicas, tanto cualitativamente como cuantitativamente y a través de la identificación de puntos característicos o minucias. En la actualidad el método científico ACEV (Análisis, Comparación, Evaluación y Verificación) es el método con mayor confiabilidad por estar sustentado científicamente, este método establece 3 niveles para establecer o no identidad (Ashbaugh, 1999):

- Nivel uno = morfología de la huella y región a la que pertenece (Dactilar, Palmar o plantar).
- Nivel dos = Identificación de puntos característicos
- Nivel tres = análisis de poros y forma de las crestas

Para la correcta identificación dactiloscópica se debe tener en cuenta tanto el método cualitativo, como el cuantitativo, pues la identificación se realiza con los dos juicios, un mostrara cantidad de particularidades y el otro, características de las particularidades.

En los procesos de cotejo dactiloscópico en documentos no hay que confundir la originalidad del documento, con la originalidad de la impresión dactilar. Pues no determinar si la impresión dactilar es original o reproducción, conlleva a un margen de error, frente a que sí fue plasmada o no por el individuo, no frente a la unicidad, pues la persona pudo ser víctima de una suplantación o hurto de identidad (Delgado, Margen de error de la dactiloscopia).

Es un principio de seguridad aplicado a la dactilotecnia que quien realiza un cotejo de forma manual tenga conocimiento de donde procede la huella, que pueda confirmarlo con cualquiera de los sentidos, y debe desconfiar de las huellas que aparecen aisladamente, del mismo modo quien realiza el enrolamiento o toma a través del biométrico debe asegurarse con los sentidos que no exista ningún elemento entre el dedo y el sensor biométrico.

Con los patrones mencionados se puede establecer que el margen de error de la dactiloscopia estará condicionado por las buenas técnicas, observación y aplicación de principios que la misma requiere para establecer o no la identidad de un individuo; por lo tanto, es pertinente mencionar que la buena práctica, no permitirá margen de error alguno, durante el proceso de obtención de las huellas ya sea de forma manual (tradicional) o al realizar el enrolamiento en el biométrico.

Autenticidad de las huellas dactilares

Para abordar este tema es importante mencionar el concepto de falsificación, según la RAE Acción y efecto de falsificar. Y falsificar es 1. tr. Falsear o adulterar algo.
2. tr. Fabricar algo falso o falto de ley. (Diccionario de la lengua española)

Con este concepto entonces, observamos que las impresiones dactilares no se falsifican, se reproducen y ello se puede realizar a través de técnicas de reproducción 2D y 3D.

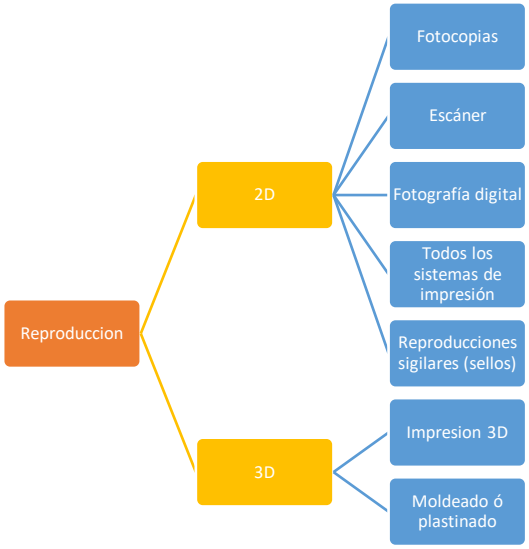

Figura 5. Técnicas de reproducción de las huellas en 2D y 3D (Elaboración propia)

La obtención de los dibujos de los relieves papilares naturales se ubica en el procedimiento técnico de las Artes gráficas (Conjunto de los procedimientos para imprimir textos, dibujos, grabados, et.), que se asemejan a las técnicas tipográficas y flexográficas. (Delgado, Monografias, 2008)

La técnica tipográfica radica en utilizar tinta a porta imágenes o tipos sólidos en alto o bajo relieve, que copian puntualmente la imagen. La técnica Flexográfica realiza igual procedimiento, pero de material flexible sobre soportes sólidos.

Sustentado que los dibujos papilares naturales son sellos y que se asemejan a la técnica Tipográfica y Flexográfica, sus imágenes impresas por contacto directo visibles y latentes

poseen características identificativas intrínsecas cualitativas y cuantitativas de especificidad imperceptibles al ojo humano, que le confieren su esencia de originales, el dactiloscopista requiere conocer muy bien dichas minucias identificativas, que son las que le permiten establecer si se trata de dibujos papilares originales o de dibujos papilares artificiales. (Delgado, Monografias, 2008)

La reproducción de los relieves papilares naturales con la técnica 2d se realiza con o sin el consentimiento del titular, es decir puede ser obtenida y copiada de una superficie directamente de una huella latente, o de una huella plasmada en un documento que el cliente origino por voluntad propia. Estas huellas se copian a través de scanner, cámaras, fotocopiadoras, o cualquier otro sistema de impresión. La reproducción de las huellas en 2d, puede ser la base para reproducir una huella en 3d.

Reproducción de las huellas en 3D

Para la obtención de huellas reproducidas en 3d se utilizan dos técnicas: el moldeado o plastinado y la impresión con impresoras 3D.

En el moldeado o plastinación se utilizan materiales, como plastilinas, siliconas y o cualquier otro material que asemeje esta textura, y que, al estar en contacto con las crestas de fricción, reproduzca exactamente la textura de la piel, los mejores materiales de moldeo reproducirán características hasta de 3 nivel (poros). Luego de la primera fase de copiado directo de la huella del titular, se debe realizar el contra molde, pues si se deja solo la primera impresión, la imagen quedara invertida al ser plasmada sobre o una superficie o colocar la huella sobre el biométrico. Luego de realizado el contra molde se podrá obtener el sello en 3D de la huella. Como resultado se obtendrán sellos con reproducción de poros y micro características propios de la huella natural, por lo tanto, pasan con facilidad por originales.

Figura 6. Sello. Tomado de (Samuel Delgado, 2018)

Las huellas fraudulentas generadas de manera artificial en 3D por plastinación o moldeo, son obtenidas mediante un molde obtenido en directo de la piel de fricción, es decir que existe una intervención directa del titular como cómplice de su fabricación.

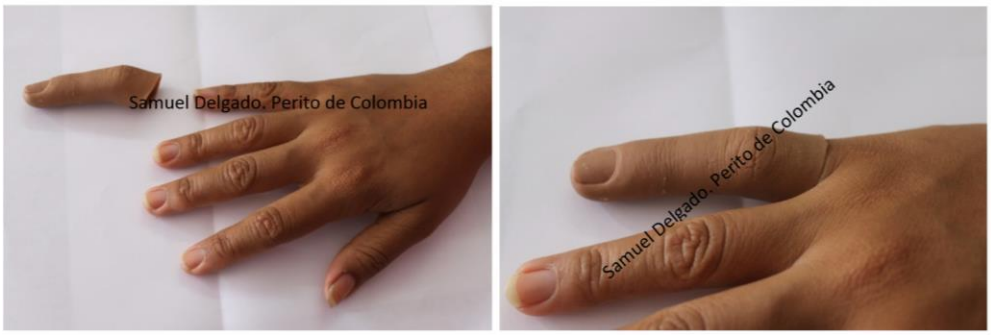

Figura 7. Imagen de la reproducción completa de un dedo a través de moldeo**.** (Samuel Delgado, 2018)

Conclusiones

- ✓La identidad personal y la seguridad han sido dos pilares que, desde hace tiempo, han inquietado a los servidores encargados de su custodia. Tener la certeza de saber que una persona es quien dice ser, dejó de ser un suceso de confianza, para ser una realidad gracias a la aplicación de la biometría.
- ✓El desarrollo de nuevas tecnologías ha hecho surgir a la biometría más allá del tema de identificación; la seguridad se ha transformado en su razón de ser. En la actualidad y

con la situación de criminalidad del país, la suplantación de personas y el robo de identidad ha afectado distintos sectores económicos y sociales, es entonces la biometría la mejor herramienta para reducir esta posibilidad de fraude.

- ✓Los sistemas biométricos dactilares en la identificación de personas poseen información de huellas digitales, lo cual es relevante e inestimable, pues cada una de las huellas presentes en los diez dedos de las manos son completamente diferentes en cada ser humano, no se tiene la facilidad de penetrar un patrón de huella dactilar como se hace con una contraseña, las huellas no pueden ser perdidas y olvidadas, por ello representan un alto estándar de seguridad.
- ✓Las entidades bancarias son un blanco constante de los delincuentes y lo primero que estos buscan al atacar un sistema biométrico es identificar los protocolos, sistema operativo y el personal que allí labora, radica entonces la importancia de la calidad de aplicación de estándares y técnicas de seguridad aplicados a la biometría dactilar.
- ✓La dactiloscopia se pone al servicio de las entidades bancarias, no como en el caso de la identificación personal en un crimen, sino para recordarle a un cliente la responsabilidad que tiene con la entidad y que puede ser demostrada a través de su huella dactilar.

Recomendaciones

Para la correcta interpretación de las recomendaciones, se debe tener en cuenta el medio de la captación de huellas: manual o a través de lector biométrico. Se brindan recomendaciones por cada factor y las recomendaciones bimodales.

Captación manual

La buena toma de las huellas dactilares.

El propósito de la toma de huellas es confirmar o descartar la fuente de la impresión, por ello, el uso de tintas, sustratos y técnicas de plasmado de buena calidad, ayudan a una buena comparación y posterior resolución de identificación personal. La manera en que la piel de los dedos (crestas de fricción) toca un sustrato influye la apariencia. Cada vez que se realiza un

plasmado o toque tiene diferentes influencias que causan diversificaciones en el aspecto de las impresiones. es decir, las huellas tomadas simultaneas, rodadadas, con deslizamiento o torsión, influirán en la flexibilidad de la piel, originando distorsiones. Por su parte los sustratos o superficies en donde son pasmadas las huellas influencian las variaciones en la apariencia, influirán en las impresiones: el contorno, la limpieza, la textura, o la naturaleza porosa del sustrato.

Toma de la huella por parte del asesor.

Las huellas siempre deben ser tomadas en presencia y por los asesores, no se deben aceptar huellas que no fueran tomadas en presencia y/o que provengan de una fotocopia o scanner. Conocer la fuente de la huella es un principio para determinar autenticidad de esta.

Captación por medio de lector biométrico

Condición del dedo.

La buena preparación de los dedos, retirar sudor, limpiar cremas o aceites influyen en una buena captación de las huellas. al momento de tomar el registro no pueden estar los dedos húmedos o sucios, también las altas temperaturas y la humedad pueden influir notablemente en la toma de la huella a través del lector.

Correcta utilización del biométrico.

En el momento de tomar una huella por medio del biométrico, se debe tener en cuenta que el cliente no coloque el dedo en un lugar diferente en cada toma, pues esto genera desplazamientos y rotaciones, por lo tanto, el lector tendrá un área común muy disminuida en las huellas tomadas y quedaran sin capturar partes de la huella, generando errores.

Técnica del biométrico.

Los biométricos utilizados en las entidades bancarias utilizan diferentes técnicas para la comparación y análisis de las huellas que capturan, la mayoría trabajan con la técnica de las minucias dactilares, se recomienda además de las minucias utilizar un biométrico que utilice la técnica basada en los poros de la piel, pues estos poseen un alto grado discriminativo y por lo tanto de mayor confiabilidad; con esto prácticamente las huellas reproducidas con técnicas en 3D podrán verse evidenciadas con mayor facilidad evitando incidentes de seguridad.

Adquirir sistemas tecnológicos con estándares internacionales.

Las entidades bancarias deben obtener sistemas tecnológicos con estándares de calidad, esto con el fin de evitar que el sistema al realizar las comparaciones arroje falsas alarmas o falsos positivos. A nivel mundial la principal entidad que sistematiza las actividades de estandarización biométrica es el Sub-Comité 17 (SC17) del Joint Technical Committee on Information Technology (ISO/IEC JTC1), del International Organization for Standardization (ISO) y el International Electrotechnical Commission (IEC). Los mejores estándares que deben ser tenidos en cuenta para las entidades bancarias son: el Estándar ANSI X.9.84 y el Estándar ANSI 378. El primero precisa las condiciones de los sistemas biométricos para la industria de servicios financieros, haciendo precisión a la transmisión y almacenamiento seguro de datos biométricos, y a la seguridad del hardware utilizad; el segundo establece condiciones para incorporar e intercambiar la información de las huellas dactilares por medio de las minucias, su principal propósito es que un sistema biométrico dactilar pueda ejecutar tecnologías de verificación de identidad e identificación, utilizando información biométrica proveniente de cualquier otro sistema.

Bimodal

Condiciones dadas por actividades.

Es importante tener en cuenta para la captación de las huellas personas que realizan cierto tipo de actividades, por ejemplo, aquellas actividades laborales donde se manipulan químicos, actividades donde se utilizan guantes de látex por mucho tiempo, actividades donde se está en constante contacto con papel, y actividades bruscas de roce de materiales con los dedos, pues esto afecta las huellas dactilares. Las enfermedades como dermatitis y gota causan deformidades y perdida de los dermatoglifos de la piel de fricción, esto también se debe tener en cuenta para su posterior estudio.

Revisión minuciosa de los dedos y manos.

Para que el proceso de suplantación por medio de reproducción de las huellas en 3D sea exitoso, se requiere participación por parte de la persona a suplantar, estar al tanto sobre el tipo de arquitectura del sistema biométrico y tener colaboración de la persona que va a realizar la captura o plasmado de las huellas. Por esto es muy importante capacitar al personal en su mayoría asesores, para que revise minuciosamente los dedos del cliente o posible cliente, utilizando el sentido del tacto y desconfíe de cualquier medio que pueda percibir sobre el dedo real. Si esta revisión es pasada por alto, este tipo de suplantación se puede detectar instalando mecanismo de vida dentro del propio sensor de la huella dactilar.

Otras opciones.

Las entidades bancarias, además de los sistemas de lectores biométricos dactilares, pueden utilizar otros sistemas biométricos para reforzar la seguridad, entre ellos se puede aplicar el reconocimiento facial y el patrón de voz para autentificar o verificar la identidad de las personas.

Referencias

Ingenieria biometrica y sus aplicaciones. (2015). Retrieved from http://ingbiometricaysusaplicaciones.blogspot.com/

Antonelli, A. C. (2006). A new approach to fake finger detection based on skin distortion.

Ashbaugh, D. R. (1999). *Quantitative-Qualitative friction ridge analysis:an introduction to basic and advenced ridgeology.*

Certicámara. (2019). *¿Para que sirve el registro biometrico en Colombia?* Retrieved from Tecnoseguro: https://www.geovictoria.com/registro-biometrico-en-colombia-asistencia/

Certicamara S.A. (2019). *Asi ha impactado la biometria nuestro dia a dia*. Retrieved from Portafolio : https://www.portafolio.co/tendencias/asi-ha-impactado-la-biometria-nuestro-dia-a-dia-533775

Delgado, S. A. (2008). *Monografias.* Retrieved from Originalidad huellas dactilares: http://www.monografias.com/trabajos-pdf/originalidad-huellas-dactilares/originalidad-huellas-dactilares.pdf

Delgado, S. A. (n.d.). *Margen de error de la dactiloscopia*. Retrieved from Foro de seguridad: http://www.forodeseguridad.com/artic/discipl/4117.htm

Diccionario de la lengua española . (n.d.). *Real Academia Española*. Retrieved from https://dle.rae.es/

EcuRed. (n.d.). *EcuRed*. Retrieved from www.EcuRed.com

Ley38. (1993). Diario Oficial de la Republica de Colombia. Retrieved from https://normativa.colpensiones.gov.co

Manrique, A. (2018). *Conexion capital.* Retrieved from http://devcnx.conexioncapital.co/incrementan-delitos-suplantacion-identidad/

Registraduria Nacional del Estado civil. (2006). *Registraduria Nacional del Estado civil*. Retrieved from https://wsr.registraduria.gov.co

Rhodes, H. T. (1956). *Alphonse Bertillon: Father of Scientific Detection.* Londres. Retrieved from http://www.mcnbiografias.com/

Samuel Delgado. (2018). ¿Se pueden copiar los poros de las crestas papilares? *Minucias scientific*, http://www.dactiloscopia.org.co/.

Serratosa, F. (2009). La biometría para identificacion de las personas. España. Retrieved from https://www.academia.edu

Wertheim, K. (2002). *Instituto Nacional de Justicia.* Retrieved from www.nij.gov