

**SISTEMA BIOMÉTRICO DE RECONOCIMIENTO DE HUELLA DACTILAR EN  
CONTROL DE ACCESO DE ENTRADA Y SALIDA**

**ADRIANA MAYA VARGAS**

**\*Dr. Gabriel Ferrer**

**UNIVERSIDAD MILITAR NUEVA GRANADA**

**FACULTAD DE RELACIONES INTERNACIONALES ESTRATEGIA Y SEGURIDAD**

**ESPECIALIZACION EN ADMINISTRACION DE LA SEGURIDAD**

**Bogotá D.C., 2013**

## Lista de Figuras

	Pág.
Figura 1. Huella dactilar con el núcleo, delta, surcos y las crestas papilares.	13
Figura 2. Gemelos igual ADN – Diferentes Huellas Dactilares	14
Figura 3. Capas externas de la piel y composición de las huellas dactilares.	15
Figura 4. Huella Dactilar donde se observan la casi totalidad de los puntos característicos.	19
Figura 5. Proceso funcionamiento del sistema Biométrico	24
Figura 6. Familia taiwanesa que carece de huellas dactilares.	30

Lista de Tablas

Pág.

Tabla 1. Comparación de los sistemas de reconocimiento Biométrico.

29

## Resumen

Al analizar la evolución histórica de la dactiloscopia siempre ha sido utilizada como método de Identificación en los seres humanos, en nuestra actualidad la huella dactilar está representada en una de las tecnologías biométricas más utilizada por ser considerado como un método seguro y efectivo en controles de acceso de entrada y salida, autorizar operaciones sensibles, evitar acceso a zonas restringidas y establecer plena identidad, esto gracias a que es única en cada ser humano y con el pasar del tiempo, los avances tecnológicos será nuestra firma digital.

Este tipo de sistema presenta una serie de vulnerabilidades frente a otros sistemas de control de acceso los cuales detectados de manera oportuna y realizando auditoria a esta serie de situaciones que alteran el normal funcionamiento se puede evitar la suplantación o infiltración que trae como consecuencias pérdida de recursos tangibles e intangibles de gran importancia para la continuidad empresarial de la organización.

**PALABRAS CLAVES:** Dactiloscopia, Huella Dactilar, Biometría, Sistema biométrico, Suplantación, Infiltración.

## Justificación

Al analizar la huella dactilar como método de identificación se puede establecer la importancia que se ha dado dentro del sector de la seguridad, empresarial y en la correcta administración de justicia, evitando suplantaciones e infiltraciones que traen como consecuencia fuga de información y pérdida recursos tangibles e intangibles.

El sistema Biométrico dactilar es el sistema de acceso más utilizado no solamente en controles de acceso para ingreso y salida, también como método de control del personal dentro de la organización para hacer un mejor uso del tiempo de la jornada laboral, pago de nómina, voto electrónico, acceso a computadoras, redes y control a zonas restringidas dentro de la misma organización.

En la actualidad existen otros desarrollos tecnológicos más avanzados utilizando la huella dactilar en los que se encuentra la máquina de café que reconoce al usuario con su impresión dactilar, cajero automático utilizado para ofrecer facilidad de ingreso al sistema bancario de la población analfabeta de los países subdesarrollados o con sobrepoblación, pago de las cuentas en restaurantes para dar comodidad a los usuarios que por olvido dejan sus tarjetas débito y crédito, y otros avances que están en desarrollo como el acceso a celulares inteligentes.

Es de gran importancia resaltar que ningún sistema de acceso es seguro todos pueden tener en algún momento vulnerabilidades, pero si existen unos más seguros que otros, el sistema de reconocimiento dactilar se pueden encontrar falencias al momento de realizar la verificación

como cortes en la falange distal de los dedos, huellas hechas con cera, gelatina, silicona, trasplante por cirugía plástica, huellas dactilares adhesivas, dedos de personas vivas incluso de fallecidas y problemas de dermatitis pero esto se puede llegar a ser detectado realizando un monitoreo al control de acceso y personalizándolo.

Lo que se va a lograr evidenciar es la confiabilidad y seguridad de la huella dactilar por la verificación de identidad a través de la lectura de las crestas papilares que se forman en la última falange de los dedos de las manos, debido a que no existe en el mundo dactilogramas exactamente iguales y lo difícil que llegaría en determinado caso lograr alterar la impresión dactilar con el fin de acceder a la organización.

## Introducción

El objetivo primordial del presente ensayo es resaltar la confiabilidad de los controles de acceso de reconcomiendo dactilar debido a la importancia, trascendencia y por ser unos de los sistemas biométricos más antiguos al igual que huellas dactilares.

La identificación por huella dactilar es un método de identificación y el más usado en la actualidad por las organizaciones a nivel mundial. La huella digital en los seres humanos se caracteriza por tener unos patrones que las hace diferentes a los demás está basado en características particulares de cada ser humano las cuales no son cambiantes con el paso del tiempo, por lo anterior es que las empresas lo que buscan es entrar el mundo de la seguridad utilizando el método de identificación dactilar no solo para la protección de recursos tangibles e intangibles que son el activo vital para el buen funcionamiento de la organización y su competitividad en el mercado mundial.

La adquisición de huellas dactilares fue un proceso realizado desde siglos atrás el cual consistía en humedecer la yema de los dedos y esta era plasmada en papel. La evolución tecnológica ha hecho que todos aquellos archivos manuales de huellas dactilares sean digitalizados contando en Colombia y el mundo con bases de datos más completas de identificación dactiloscópica.

La seguridad de la información es importante ya que es la esencia primordial de las compañías su cuidado y protección debe ser de manera adecuada, oportuna para evitar ser extraída de personas internas y externas que pueden utilizarla para causar daños irreparables o acaben con la continuidad de la organización. En las empresas son múltiples las vulnerabilidades

a las que están expuestas es así las empresas están adquiriendo control de acceso biométricos cada vez más avanzados con características particulares para evitar suplantación, restringir el acceso a personas autorizadas a zonas de carácter restringido por el tipo de actividades que allí se desarrollen, la información que se guarda, para prevenir y detectar cualquier situación que altere el normal funcionamiento de los procesos de la compañía se requiere hacer monitoreo constante y oportuno para identificar cuáles son las intenciones de la persona a ingresar.

Aunado a un control de acceso para el cuidado y aseguramiento de la información, elemento en el cual las organizaciones deben crear conciencia dentro de su equipo de trabajo, su confidencialidad, la responsabilidad y las consecuencias que tiene frente al uso inadecuado de esta.

Un complemento importante y alternativo en los controles de acceso biométricos dactilares es la utilización de hardware y software, lo que permiten verificar la identidad del usuario con un parámetro ya almacenado propio de esta persona en este caso la huella dactilar.



## Contenido del Trabajo

### 1. Evolución y estado actual de la dactiloscopia.

La dactiloscopia tuvo su evolución histórica en 3 grandes etapas en las cuales se logra evidenciar que desde sus inicios se le dio la importancia como sistema de identificación y con una gran trascendencia que a la fecha todavía es utilizado.

La primera etapa se desarrolló en la **época prehistórica**, los primitivos realizaban dibujos en las cavernas como método de identificación. Posteriormente surgió la **etapa empírica**, se encontraron muchas huellas dactilares plasmadas en documentos y escritos las cuales eran de griegos y romanos, están se utilizaban como método de autenticación y finalmente la **etapa científica**, donde se descubrió que en las yemas de los dedos presentaban unas rugosidades que formaban unas figuras con relieves y surcos interpapilares.

Posteriormente se creó la dactiloscopia, Juan Vucetich en el año de 1895 y Henry Canadiense en el año de 1887, crearon el primer método de identificación decadactilar.<sup>1</sup>

### 2. Evolución y estado actual de la biometría

En la antigua babilonia, los reyes firmaban las tabletas en arcilla con la yema de los dedos.

En China se estableció que el hombre para divorciarse debía firmar el documento con las huellas dactilares, las personas estampaban la palma de las manos de los niños para poder diferenciar entre un niño y un joven.

En Occidente solo se confiaba en la memoria fotográfica como método de identificación hasta que Bertillon desarrollo el sistema antropométrico que consistía en tomar las medidas de partes

---

<sup>1</sup>Anónimo. (2007, 11 de diciembre). Historia de la dactiloscopia (web log post). Recuperado de <http://www.dactiloscopia-dactiloscopia.blogspot.com/2007/12/dactiloscopia.html>

del cuerpo. Este sistema fue utilizado mucho en occidente hasta que aparecieron defectos en el sistema en cambio de medidas.<sup>2</sup>

### 3. Precursores en dactiloscopia y biometría

**Marcelo Malpighi**, identificó que las características de los dedos no cambiaban y eran diferentes unas de otras y dio la primera noticia sobre estudios científicos de los dibujos papilares; **Jan Evangelist Purkinje**, estableció que las huellas eran únicas y las figuras que se formaban en ellas no cambiaban con el paso del tiempo; **Henry Faulds**, publicó varias revistas en las que trató temas de gran importancia como la identificación por medio de la huella dactilar y hace sugerencias en relación a la huella dejada en el lugar de los hechos para identificar a los delincuentes.<sup>3</sup> Posteriormente utilizó esta técnica para descubrir el culpable de un robo en Tokio.<sup>4</sup> Fue el primero que inicio con la utilización de la ficha decadactilar y comprobó que al coger objetos se dejaban huellas sin la necesidad de estar manchados los dedos; **William Herschel**, en 1858 creó una forma de que los trabajadores no fueran suplantados en día de pago, detrás del contrato de trabajo de cada empleado estampaba la huella dactilar. En el año de 1895 en Bengala India, demostró con sus propias impresiones dactilares tomadas en 1885 y 1919 los puntos característicos no presentaban ningún tipo de variación, **Francisco Galton**, se dedicó de lleno a partir de 1888 al estudio de la dactiloscopia y lo que buscaba era encontrar un método de clasificación de dactilogramas. Presenta la propuesta de la creación de un sistema de identificación afianzado en la perennidad e individualidad de las huellas dactilares, asegura que

---

<sup>2</sup>Anónimo. (2008). Historia de la biometría. Recuperado de [http://www.securetech.com.uy/servicios/info/biometria\\_5.htm](http://www.securetech.com.uy/servicios/info/biometria_5.htm).

<sup>3</sup>Martínez, J. Sistemas de Clasificación dactiloscópica. Recuperado de [http://www.getocolombia.com/Archive/MANUAL%20SISTEMA%20HENRY%20CANADIENSE%20\(YA\).pdf](http://www.getocolombia.com/Archive/MANUAL%20SISTEMA%20HENRY%20CANADIENSE%20(YA).pdf)

<sup>4</sup>Paños, S. (2010). Historia de la biometría, presentación. Recuperado de <http://www.slideshare.net/serweb/presentacion-biometria#btnNext>.

la posibilidad que dedos distintos dejen la misma huella dactilar son menos de una en 64 millones; **Juan Vucetich**, se encargó de mejorar el sistema de clasificación de Galton y hacerlo más fácil de utilizar para aquellas personas que no tenían mucho conocimiento en el tema, cuyo método se conoce como dactiloscopia, presentó el primer sistema de clasificación de las impresiones dactilares para que el gobierno de esa época estudiara las ventajas y desventajas que presentaban las mismas.

Entre 1905 y 1908 se empieza a utilizar el sistema de huella dactilar por la Fuerza Aérea, Ejército y Armada de Estado Unidos;<sup>5</sup> **Alfonso Bertillon**, creador del Sistema Antropométrico el cual utilizaba rasgos físicos como: estatura, tipo, color de pelo, ojos, tatuajes, cicatrices y medidas como nariz, orejas, pies y dedos; **Edwar Richar Henry**, ideó un método de clasificación y archivo de huellas dactilares y fue el líder de los sistemas de clasificación utilizados por la policía criminal.<sup>6</sup>

En 1969 el FBI realizó un significativo avance a la tecnología de reconocimiento de huella dactilar que consistía en sistematizar el proceso de identificación dactilar el cual causó furor pero requería de muchas personas ya que se trataba de un proceso manual. En 1975 el FBI creó el primer escáner para la extracción de minucias de las huellas.<sup>7</sup>

Los personajes que hicieron el descubrimiento y la importancia de las crestas papilares como método de identificación y clasificación se les atribuyen a Herschel, Faulds, Galton, Edwar Richar Henry y Vucetich, realizaron todas las investigaciones y estudios en la identificación de

<sup>5</sup>Anónimo. Fundamentos de la Biometría. Recuperado de <http://www.biometria.gov.ar/acerca-de-la-biometria/historia-de-la-biometria.aspx>

<sup>6</sup>Martínez, J. Sistemas de Clasificación dactiloscópica. Recuperado de [http://www.getocolombia.com/Archive/MANUAL%20SISTEMA%20HENRY%20CANADIENSE%20\(YA\).pdf](http://www.getocolombia.com/Archive/MANUAL%20SISTEMA%20HENRY%20CANADIENSE%20(YA).pdf)

<sup>7</sup>Anónimo. Historia de la Biometría. Recuperado de <http://www.biometria.gov.ar/acerca-de-la-biometria/historia-de-la-biometria.aspx>

las personas utilizando la dactiloscopia la cual es utilizada en la actualidad dejando resultados significativos.<sup>8</sup>

Desde la Biblia, se empieza a dar valor y significado a las huellas dactilares, Eliù al cantar de la sabiduría de Dios dice “*Él pone un sello en las manos de los hombre, a fin de que todos reconozcan sus actos*”,<sup>9</sup> en esta corta frase se evidencia que se puede demostrar la responsabilidad de lo que se haga sin perder de vista los valores.

A través de la historia el sistema de identificación con huella dactilar ha sido utilizado para identificar a los responsables de crímenes como el de la mujer que asesino a sus dos hijos en la escena del crimen fue encontrada la huella dactilar del dedo índice izquierdo<sup>10</sup> y el caso de un narcotraficante a quien le cambiaron el tejido del dedo gordo del pie derecho y se lo colocaron en el dedo pulgar de la mano derecha el único fin evadir las autoridades y seguir con el actuar criminal.<sup>11</sup>

#### 4. La huella dactilar en su estructura como método de identificación

Está formada por crestas papilares y surcos interpapilares están localizados en la piel los cuales forman los dibujos en la falange distal de los dedos de las manos, lo que hace que se formen puntos característicos, un núcleo y uno o varios deltas, con el fin de llevar a cabo la verificación de identidad.

---

<sup>8</sup>Maza, M. Manual de Criminalística. Recuperado de [http://clasev.net/v2/pluginfile.php/11083/mod\\_resource/content/0/INTRODUCCION\\_A\\_LA\\_DACTILOSCOPIA.pdf](http://clasev.net/v2/pluginfile.php/11083/mod_resource/content/0/INTRODUCCION_A_LA_DACTILOSCOPIA.pdf)

<sup>9</sup>Valcárcel, A. (1949). La Dactiloscopia en su aplicación a los Seguros Sociales. Recuperado de [http://bvingesa.msc.es/bvingesa/es/catalogo\\_imagenes/grupo.cmd?path=1001350&responsabilidad\\_civil=on](http://bvingesa.msc.es/bvingesa/es/catalogo_imagenes/grupo.cmd?path=1001350&responsabilidad_civil=on)

<sup>10</sup>Galvis, C. (2007). Historia de la Biometría y las tecnologías Biométricas. Recuperado de <http://www.monografias.com/trabajos43/biometria/biometria.shtml>

<sup>11</sup>Ríos, F. (2008, 20 de julio). Las huellas siempre delatan. *El Espectador*. Recuperado de <http://www.elespectador.com/node/27306/print>

A continuación se explicará como diferenciar un surco interpapilar de una cresta papilar:: Al entintar el dedo y colocarlo sobre la superficie lo de color negro se llama crestas y el color de la superficie ya sea papel u otra se denominan surcos.

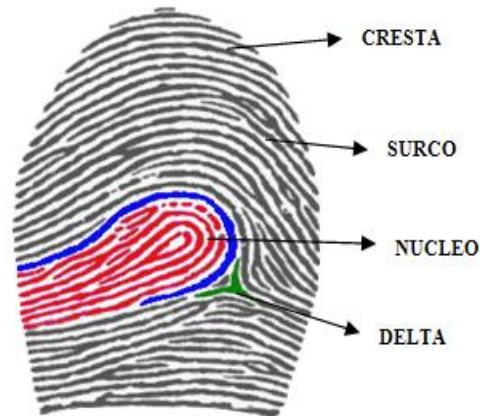


Figura 1. Huella dactilar donde se observa el núcleo, delta, surcos y crestas papilares.

#### 4.1. Origen de las crestas papilares

El origen de las crestas papilares tiene su evaluación con un aporte genético y otro en el ambiente en que se desenvuelve el feto en el seno de la madre.

El Genoma aporta el material genético y contribuye a formar las características propias de las huellas dactilares y el ambiente donde está expuesta la piel se encuentran unos factores como la nutrición, presión sanguínea, líquido amniótico, temperatura y posición del feto esto hace que se dé la formación y el aspecto distintivo a la huella digital, es natural que entre personas de la misma familia padres, hijos y hermanos o hasta en la misma mano de una persona se encuentren

similitudes en la forma de la huella pero nunca llegan a ser iguales, por lo anterior es que los gemelos no poseen huellas iguales, solo patrones similares.

En la piel se encuentra 3 capas externas epidermis, dermis e hipodermis, los dibujos dactilares se forman en la capa epidérmica y dérmica, en la dermis se encuentran las papilas y los relieves son las crestas que se forman de estas papilas.<sup>12</sup>

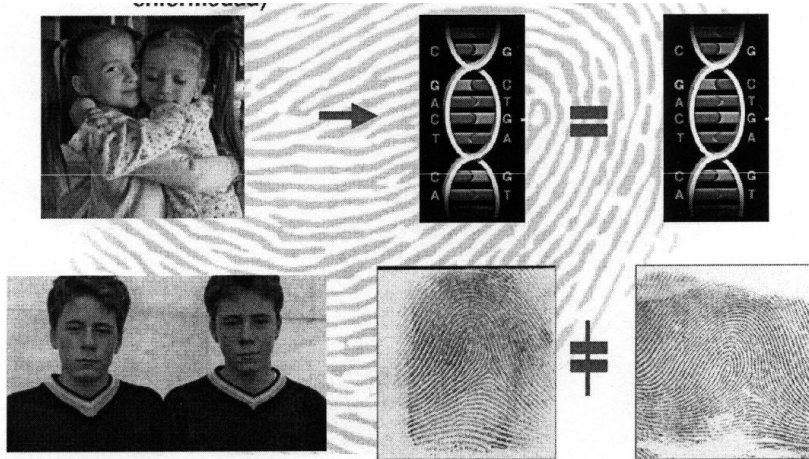


Figura 2. Gemelos igual ADN – Diferentes Huellas Dactilares.

#### 4.2. Composición de las huellas dactilares

Están constituidas por sudor, aceites corporales, grasas y sustancias químicas externas a la piel sustancias expulsadas por las glándulas sebáceas, glándulas sudoríparas y poros que hacen que al coger un objeto cualquiera que sea quede plasmada la huella dactilar sobre la superficie manipulada.<sup>13</sup>

Las **Glándulas sebáceas**, produce grasa que es expulsada a la dermis para proteger la superficie de la piel y se forman en el sexto mes de gestación; la **Glándula sudorípara**, genera

<sup>12</sup>Carro, R. De las crestas Papilares (I). Recuperado de <http://dialnet.unirioja.es/download/articulo/2869886.pdf>.

<sup>13</sup>Chávez. C. (2008). Huellas Dactilares. Recuperado de <http://es.scribd.com/doc/3996151/Huellas-Dactilares>

sudor que emana a la dermis por los poros y **los Poros**, son orificios que se encuentran en la parte superior de la piel por donde sale el sudor y se expande a los surcos interpapilares.<sup>14</sup>

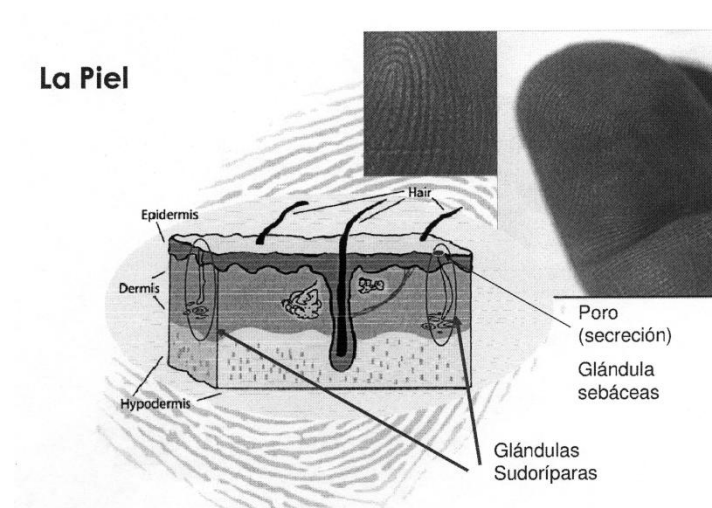


Figura 3. Capas externas de la piel y composición de las huellas dactilares.

#### 4.3. Características de las crestas papilares

A nivel mundial existen varios métodos de clasificación dactilar entre los que se encuentran vucetich, Henry Americano, Henry Canadiense entre otros, y como complemento a esto una excelente herramienta de biometría llamada AFIS la cual es utilizada para mejorar y dar una mejor calidad de imagen a la huella, todo lo anterior está fundamentado científicamente por las crestas papilares y las características que a continuación se mencionan.<sup>15</sup>

**Inmutabilidad**, se mantienen invariables en su forma, tamaño y ubicación, aunque al causar afectación de la dermis al sanar la lesión se genera un dibujo cicatrizal; **perennes**, las huellas no cambian con el tiempo se forman en su integridad en el sexto mes de vida intrauterina del ser



<sup>14</sup> Anónimo. Colegio de especialistas forenses. Dactiloscopia. Recuperado de <http://coesfo.es.tl/Dactiloscop%EDa.htm>

<sup>15</sup> Delgado, S. El margen de error de la dactiloscopia. Recuperado de <http://www.forodeseguridad.com/artic/discipl/4117.htm>

humano y permanecen hasta la muerte hasta encontrar el cuerpo en estado de putrefacción o descomposición cadavérica.<sup>16</sup> Locard, realizó una prueba para la dactiloscopia, se quemó los pulpejos de los dedos de las manos con agua hirviendo, hierro candente y aceite caliente para demostrar que después de la curación de las heridas las huellas dactilares aparecían siendo las mismas en su forma, ubicación y situación. Se encontró como ultima características que son **diversiformes**, son únicas tiene su propio dibujo, lo que significa que no existen huellas iguales ni en los dedos de la misma mano ni diferentes manos.<sup>17</sup>

#### 4.4. Puntos Característicos o Dactiloscópicos de la huella dactilar







Son los detalles que se forman en las crestas papilares y hacen la diferencian entre una huella y otra en los cuales su fundamenta la identidad de las personas.




	<p><b>Abrupta:</b> Cresta papilar que se ubica entre dos crestas paralelas, termina en cualquier momento sin volver aparecer.</p>
	<p><b>Bifurcación:</b> Cresta papilar que inicia de la parte izquierda de la huella dactilar y en cualquier momento del recorrido se divide en 2 crestas que continúan paralelamente.</p>

<sup>16</sup>Carro, R. (2009, 14 de mayo). El investigador: De las crestas papilares II (web log post). Recuperado de <http://policiasenlared.blogspot.com/2009/05/de-las-crestas-papilares-ii.html>.

<sup>17</sup>Jiménez, V. (2011). Crestas Papilares. Recuperado de <http://es.scribd.com/doc/64679879/CRESTAS-PAPILARES>.



	<p><b>Convergencia:</b> Cresta papilar que inicia su recorrido de la parte derecha de la huella dactilar y en cualquier momento del recorrido se divide en 2 crestas que continúan paralelamente.</p>
	<p><b>Desviación:</b> Dos crestas papilares que inician su recorrido de lados opuestos de la huella dactilar tienden a fusionarse pero se desvían ligeramente.</p>
	<p><b>Empalme:</b> Cresta corta de dirección inclinada que se une en sus 2 extremos por 2 crestas papilares que corren paralelamente.</p>
	<p><b>Fragmento:</b> Crestas de extremos abruptos.</p>
	<p><b>Interrupción:</b> Cresta que presenta ruptura en su recorrido deja un pequeño espacio entre la terminación e inicio de las crestas.</p>
	<p><b>Ojal:</b> Espacio elíptico que forman 2 crestas papilares.</p>

	<p><b>Punto:</b> Fragmento de cresta muy pequeño se encuentra en el centro de las interrupciones.</p>
	<p><b>Secante:</b> Son 2 crestas que van en dirección paralela y se unen formando un aspa.</p>
	<p><b>Transversal:</b> Cresta que se aparta de la dirección que trae y es cruzada por otra cresta que va en sentido contrario.<sup>18</sup></p>

<sup>18</sup>Mendoza, M. (2006). Postgrado de criminalística Instituto de Trabajos Superiores Policía Nacional de Nicaragua. Recuperado de <http://www.policia.gob.ni/cedoc/sector/acapol/postgrado/8%20CaracteristicaDactilares.pdf> y Leño, E. (1982). Curso de dactiloscopia clasificación de y archivo Sistema Henry. Registraduría Nacional del Estado Civil División de Identificación. Pág.21

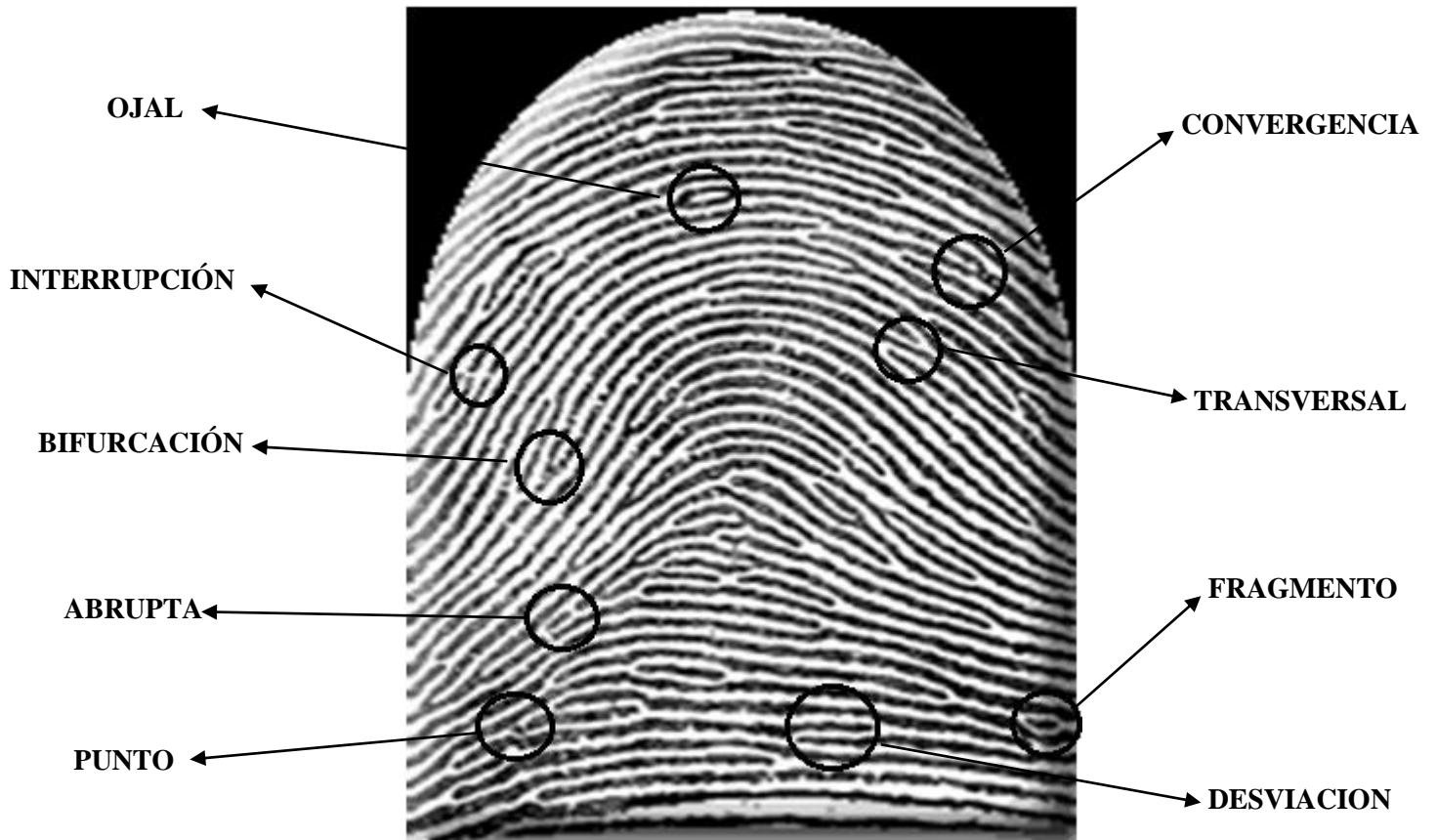


Figura 4. Huella Dactilar donde se observan la casi totalidad de los puntos característicos.

En la imagen anterior se observan los puntos característicos que son analizados por el sistema biométrico dactilar para hacer el proceso de identificación o autenticación.

#### 4.5 Sistemas de crestas papilares

En el dactilograma teniendo en cuenta su situación, forma y dirección las crestas papilares están agrupadas en 3 sistemas, donde se encuentra el mayor número de puntos característicos.

	<b>MARGINAL</b>	Está ubicado en la margen o contorno del dactilograma limita con el delta en su parte externa y las crestas van haciendo un recorrido ascendente para descender al lado opuesto de su inicio. <sup>19</sup>
	<b>NUCLEAR</b>	Las crestas se ubican en la región céntrica o núcleo del dactilograma la cual limita con la región basilar y marginal con un recorrido en forma descendente y ascendente.
	<b>BASILAR</b>	Constituido por crestas papilares que ubican en la última parte de la falange las cuales van elevándose hasta encontrarse con la región nuclear, por la parte inferior limita con el pliegue de flexión de la huella dactilar. <sup>20</sup>

## 5. Importancia de la biometría y la dactiloscopia en la actualidad

La biometría al igual que la dactiloscopia ha tenido un auge y avance, en Colombia es utilizada la dactiloscopia como método de identificación de delincuentes se hizo obligatorio para la expedición de la primera cédula de ciudadanía.

La Ley 906 del 2004 CPP en su artículo 251 establece como método de identificación la huella dactilar siendo utilizada como método de verificación de plena identidad de la persona vinculada y capturada dentro de proceso judicial para hacer efectiva y acertada la aplicabilidad de la justicia. El método de reconocimiento por huella dactilar cuenta en la actualidad con alto

<sup>19</sup>González, M. (2004). Introducción a la dactiloscopia como método de identificación de personas. Recuperado de <http://cienciaforense.com/Pages/EvidenciaFisica/Dactiloscopia.htm>

<sup>20</sup>Anónimo. Criminalística Legal. Dactiloscopia. Recuperado de <http://www.criminalisticalegal.com/dactiloscopia.php>

grado de credibilidad, efectividad y aceptada universalmente hasta ser utilizado en la investigación criminal aun por encima del métodos de reconocimiento de ADN.

La dactiloscopia no es única y exclusivamente para identificar delincuentes también sirve para identificar a todas las personas para así evitar suplantaciones, ya que las huellas que llevan los seres humanos en los dedos de las manos se evidencia cual es su nombre verdadero y su identidad.<sup>21</sup>

De igual manera la dactiloscopia sirve para identificar cadáveres en estado de descomposición o putrefacción, personas con enfermedades como la amnesia, identificación de victimas en desastres, extranjeros que circulen por el territorio Nacional sin ningún tipo de identificación o que no hablen el idioma del país donde se encuentren.

Al realizar un análisis detallado sobre las huellas encontradas en la escena del crimen se puede identificar y establecer que personas estuvieron presentes o fueron testigos presenciales del hecho materia de investigación, en algunos se puede establecer el autor material e intelectual del hecho punitivo.<sup>22</sup>

El auge y el grado de aceptabilidad que ha tenido el sistema biométrico dactilar ha sido tan significativo fue implementado por la Registraduría Nacional del Estado Civil desde el año 2009 en comicios electorales atípicos donde fue un éxito total, dicho sistema consta de un lector de huella el cual es instalado al ingreso de los puestos de votación esto con el fin de verificar la

---

<sup>21</sup>Valcárcel, A. (1949). La Dactiloscopia en su aplicación a los Seguros Sociales. Recuperado de [http://bvingesa.msc.es/bvingesa/es/catalogo\\_imagenes/grupo.cmd?path=1001350&responsabilidad\\_civil=on](http://bvingesa.msc.es/bvingesa/es/catalogo_imagenes/grupo.cmd?path=1001350&responsabilidad_civil=on)

<sup>22</sup>Iguaran, M. Manual único de criminalística de la Fiscalía General de la Nación. Recuperado de [http://www.fiscalia.gov.co/en/wp-content/uploads/2012/03/manual\\_de\\_criminalistica.pdf](http://www.fiscalia.gov.co/en/wp-content/uploads/2012/03/manual_de_criminalistica.pdf)

identidad de los votantes y constatar si la persona está habilitada para ejercer el derecho al voto, es por ello que será instalado en regiones del país donde el grado de fraude electoral por suplantación de votantes es significativo.

La identificación por huella dactilar es un método complementado con sistemas biométricos los cuales han sido instalados en puntos fronterizos para hacer seguimiento a migrantes, en aeropuertos para aumentar la seguridad, cajeros electrónicos este tipo de medidas es de gran importancia especialmente para aquellas personas que no saben leer ni escribir ya que pueden tener un sin número de servicios únicamente utilizando la huella.<sup>23</sup>

INTERPOL la organización policial más grande del mundo, esta mas allá de las fronteras administra un sistema de identificación dactilar llamado AFIS, cuenta con más de 146.000 registros de huellas dactilares, únicamente puede acceder cualquiera de los 188 países miembros con el fin de verificar, observa y enviar huellas dactilares de extranjeros arrestados y ciudadanos nacionales sospechosos de cometer delitos de carácter internacional, esto con el fin de tener identificados a todas aquellas personas que van por el mundo delinquiendo, resolver crímenes y para que la seguridad sea más segura y confiable.<sup>24</sup>

## 6. Sistema Biométrico y sus principales características

La palabra biometría se deriva del latín griego bio (vida) y metría (medida). La biometría es un sistema que utiliza para su funcionamiento una característica física del ser humano y es reconocido como una forma de identificación de personas, en este caso la huella dactilar.<sup>25</sup> Con

<sup>23</sup>Sánchez, C. (2011, 3 de noviembre). La experiencia Colombiana en identificación biométrica aplicada a las elecciones. Registraduría Nacional del Estado Civil - Biometría. *El Espectador*. Recuperado de [www.registraduria.gov.co](http://www.registraduria.gov.co)

<sup>24</sup> Till, E. Biometrías 2. Recuperado de [www.biometria.gov.ar/media/74948/biometrías2.pdf](http://www.biometria.gov.ar/media/74948/biometrías2.pdf)

<sup>25</sup> Anónimo. Recuperado de [http://www.kimaldi.com/area\\_de\\_conocimiento/biometria/que\\_es\\_la\\_biometria](http://www.kimaldi.com/area_de_conocimiento/biometria/que_es_la_biometria)

las características que se mencionan a continuación se evidencia la utilidad, practicidad y confiabilidad del sistema biométrico de acuerdo a las necesidades.

**Desempeño**, efectividad del sistema biométrico en la identificación de personas, con el fin primordial de comprobar la veracidad y exactitud del resultado obtenido, lo anterior asociado a los recursos y tecnologías aplicadas para alcanzar tal objetivo; **aceptabilidad**, aceptación que tiene el sistema biométrico para las personas que lo van a utilizar. El sistema debe prestar seguridad, confiabilidad, fácil utilización y no vulnerar el derecho a la intimidad, el reconocimiento de iris puede dejar en evidencia enfermedades que el usuario quiere mantener bajo reserva y la **fiabilidad**, dificultades que puede presentar el sistema biométrico al momento de ser vulnerado, debe reconocer características propias de personas vivas para evitar suplantaciones y sabotajes por parte de los operadores o usuarios que tengan acceso al dispositivo.<sup>26</sup>

## 7. Proceso de funcionamiento del sistema Biométrico

Dentro del funcionamiento de este sistema se encuentra la **captura**, como se almacenan los patrones o características a analizar, además se incluye un valor de calidad de la imagen y se registran datos personales del usuario; **proceso**, analiza los patrones o características y los convierte en un identificador numérico; **clasificación**, compara las características extraídas por el sistema de proceso con las almacenadas en el sistema. La salida da como resultado la similitud de la característica almacenada con la característica del sujeto en comparación y la **decisión**,

---

<sup>26</sup>Hernández, A. Bases teóricas y sistemas biométricos, Características sistema biométrico. Facultad de ingeniería biométrica informática. Recuperado de <http://redyseguridad.fi-p.unam.mx/proyectos/biometria/basesteoricas/caracteristicassistema.html>.

resultado de la comparación (características extraídas y las almacenadas) da como resultado positivo permite el acceso de lo contrario es denegado, afirma que el usuario es quien dice ser.<sup>27</sup>

Los errores que se pueden presentar en el sistema biométrico de huella dactilar es que en dicho proceso de reconocimiento se determine que la huella no corresponde al mismo dedo lo que se denomina falsa aceptación y la otra que el sistema determine que las dos huellas del mismo dedo no correspondan lo que se llamaría un falso rechazo.<sup>28</sup>



Recuperada de <https://www.google.com.co/search?q=proceso+de+funcionamiento+del+sistema+biometrico&bav=on.2>

Figura 5. Proceso funcionamiento del sistema Biométrico.

## 8. Proceso de autenticación e identificación biométrica

El proceso de autenticación es más rápido y realiza una comparación con un patrón ya guardado, este proceso se conoce como uno para uno (1:1). Para este proceso se debe conocer como primera medida la identidad de la persona a autenticar presentando un documento o tarjeta y da como resultado un valor positivo o negativo.

<sup>27</sup>Morales, C. (2009). Biometría desde la perspectiva de la seguridad en la Tics. Recuperado de <http://es.scribd.com/doc/24156012/Biometria>

<sup>28</sup>Martínez, M. Vulnerabilidades en sistema biométrico de reconocimiento basado en huella dactilar: Ataques Hill – Climbing. Recuperado de <http://arantxa.ii.uam.es/~jms/pfesteleco/lecturas/20060926MarcosMartinezDiaz.pdf>



El proceso de identificación hace la comparación con unos patrones ya almacenados, este proceso se conoce como uno a muchos (1:N). Para este proceso no se requiere conocer la identidad del individuo como en el anterior, la muestra tomada del usuario es comparada una a una con los ya almacenados en la base de datos dando como resultado la identidad de la persona.<sup>29</sup>

#### 9. Efectividad de la huella dactilar frente a otros sistemas

Dentro de las múltiples ventajas y utilidades con las que cuenta el sistema biométrico de huella dactilar se encuentra:

Está catalogado como el más seguro, efectivo de 1.000 casos uno solo induce a error y el grado de aceptación es del 99%, esto frente a todos los demás sistemas existentes en el mercado.

El sistema biométrico dactilar en la identificación de personas, se tiene que la cantidad de información existente en una huella digital es significativa y valiosa, cada una de las huellas existentes en los diez dedos de las manos son totalmente diferentes al igual que en todas las personas, no se tiene la facilidad de descifrar un patrón de huella dactilar como una contraseña, las huellas no se tiene la facilidad de ser perdidas y olvidadas.<sup>30</sup>

Los sistemas biométricos analizan características físicas como reconocimiento de iris y retina, reconocimiento facial, reconocimiento geometría de la mano, reconocimiento de firma escrita, reconocimiento venas de las manos, reconocimiento palma de la mano y reconocimiento

---

<sup>29</sup>Anónimo. Autenticación e Identificación Biométrica, control de personal. Recuperado de <http://www.biodevices.com.ec/biometría>

<sup>30</sup>Fonseca, G. (2012, 31 de enero) Sistemas biométricos (web log post). Recuperado de <http://www.mentesinquietas.net/blog/archives/334>

de voz, los cuales presentan unas ventajas y desventajas las cuales se mencionaran a

continuación:

9.1. Reconocimiento facial: Se hace fotografiando la cara del individuo desde diferentes ángulos.

<b>VENTAJAS</b>	<b>DESVENTAJAS</b>
Sistema de reconocimiento es no invasivo por local que no requiere contacto con el autenticador.	Variación en el ángulo de la cabeza lo que no permite realizar el proceso de verificación.
Las personas pueden estar en movimiento cuando se encuentran frente al sistema biométrico.	Cambios de iluminación pueden llegar afectar el sistema biométrico.
Alta aceptabilidad ya que los usuarios no ven interrumpido su flujo de acceso y trabajo.	Los gestos expresivos pueden alterar el proceso de identificación.
Tipo de sistema biométrico es utilizado para entre humano entre varios individuos.	Obstrucción debido a lentes, gafas o sombreros que puedan cubrir parte de la cara.
Es un sistema no invasivo ya que únicamente se trata de una fotografía.	Unos de los mayores problemas es la utilización de máscaras, por lo que hace difícil ser detectado por el sistema de vigilancia.

Sánchez, D. Reconocimiento Biométrico. Reconocimiento facial. Revista decana independiente de seguridad, Seguritecnia. Recuperado de [http://www.bormart.es/articulo\\_seguritecnia.php?id=2166](http://www.bormart.es/articulo_seguritecnia.php?id=2166)

Fuentemayor, G. Avances en técnicas biométricas y sus aplicaciones en seguridad. Recuperado de <http://neutron.ing.ucv.ve/comunicaciones/Asignaturas/DifusionMultimedia/Tareas%202005-3/BIOMETRIA.doc>

Anónimo. Autenticación de reconocimiento facial. Recuperado de <http://www.umanick.com/index.php/tecnologia/reconocimiento-facial>

Martínez, M. Vulnerabilidades en sistema biométrico de reconocimiento basado en huella dactilar: Ataques Hill – Climbing. Recuperado de <http://arantxa.ii.uam.es/~jms/pfsteleco/lecturas/20060926MarcosMartinezDiaz.pdf>

9.2. Reconocimiento de voz: Se hace grabando el patrón de voz de una persona.

<b>VENTAJAS</b>	<b>DESVENTAJAS</b>
Puede ser confiable es una marca individual de una persona.	La voz puede ser grabada y reproducida después para engañar al sistema.
Es un sistema biométrico aceptado.	Puede ser alterada por la edad o enfermedades o afecciones como resfriado o en algunos casos el estado de ánimo hace que varía.
	Su baja distintividad y es muy fácil de ser imitada.

Paduraru, C. Cuáles son las ventajas y desventajas de las biometrías. Recuperado de [http://www.ehowenespanol.com/cuales-son-ventajas-desventajas-biometrias-info\\_102877/](http://www.ehowenespanol.com/cuales-son-ventajas-desventajas-biometrias-info_102877/)

Martínez, M. Vulnerabilidades en sistema biométrico de reconocimiento basado en huella dactilar: Ataques Hill – Climbing. Recuperado de <http://arantxa.ii.uam.es/~jms/pfsteleco/lecturas/20060926MarcosMartinezDiaz.pdf>

9.3. Reconocimiento de iris-retina: El método de autenticación biométrica de iris utiliza técnicas de reconocimiento de patrones ya almacenados en una base de datos.

Este tipo de sistema utiliza la tecnología de cámaras que funciona con una fina iluminación infrarroja que reduce el reflejo que se haya podido producir en la convexa córnea y poder crear detalladas imágenes de las complejas estructuras del iris. Posteriormente estas imágenes son convertidas en plantillas digitales, para ser comparadas con un individuo.

El sistema biométrico de retina lo que hace es escanear la retina y los vasos sanguíneos, de la parte trasera del ojo. El usuario debe acercar el ojo al lector y fijar la mirada en un punto.

VENTAJAS	DESVENTAJAS
El iris tiene características únicas que no cambian con el tiempo.	Para obtener la medida exacta el patrón debe estar ubicado a una distancia considerable del escáner, lo cual significa incomodidad para los usuarios.
El reconocimiento de Iris es una Técnica donde el usuario puede realizar la verificación desde una distancia cómoda del escáner.	Este sistema es poco utilizado en el mercado por lo que no es de fácil adquisición.
El patrón de los vasos sanguíneos en la retina no cambia con el tiempo.	No tiene la facilidad de realizar búsqueda de un patrón con varios patrones ya almacenados.
El tiempo de verificación de retina es rápido.	Necesidad del desarrollo del algoritmo.
El sistema de análisis de retina es difícil de engañar, no existe la manera de hacer una réplica igual y cuando la persona fallece la retina se deteriora.	El reconocimiento de retina puede revelar enfermedades y afecciones la cuales pueden vulnerar el derecho a intimidad de los usuarios como hipertensión.
	El reconocimiento de retina la captura de este rango biométrico es compleja ya que se necesita voluntad y cooperación por parte del usuario ya que se requiere contacto con el sensor y su gran aceptabilidad es muy importante.
	El reconocimiento de iris tecnología muy

	<b>COSTOSA.</b>
<p>Fuentemayor, G. Avances en técnicas biométricas y sus aplicaciones en seguridad. Recuperado de <a href="http://neutron.ing.ucv.ve/comunicaciones/Asignaturas/DifusionMultimedia/Tareas%202005-3/BIOMETRIA.doc">http://neutron.ing.ucv.ve/comunicaciones/Asignaturas/DifusionMultimedia/Tareas%202005-3/BIOMETRIA.doc</a>                  Martínez, M. Vulnerabilidades en sistema biométrico de reconocimiento basado en huella dactilar: Ataques Hill – Climbing. Recuperado de <a href="http://arantxa.ii.uam.es/~jms/pfesteleco/lecturas/20060926MarcosMartinezDiaz.pdf">http://arantxa.ii.uam.es/~jms/pfesteleco/lecturas/20060926MarcosMartinezDiaz.pdf</a></p>	

9.4. Identificación de la geometría de la mano: Lo que hace este tipo de sistema biométrico es tomar una serie de medidas de mano, como forma, tamaño, anchura de los dedos y longitud.

<b>VENTAJAS</b>	<b>DESVENTAJAS</b>
Plantillas ocupan pequeñas cantidades de bytes.	Lectores son de relativo gran tamaño, lo que los hace fáciles de ser dañados.
Es un sistema no intrusivo.	Lectores son costosos.
Gran exactitud.	Variación de la morfología y geometría de la mano a lo largo de la vida.
Sencillo, no es costoso y no requiere de luz especial para ser utilizado.	Toma mucho espacio para registrar y se puede alterar con facilidad con la utilización de joyas o problemas de salud como artritis.

Fuentemayor, G. Avances en técnicas biométricas y sus aplicaciones en seguridad. Recuperado de <http://neutron.ing.ucv.ve/comunicaciones/Asignaturas/DifusionMultimedia/Tareas%202005-3/BIOMETRIA.doc>  
 Paduraru, C. Cuáles son las ventajas y desventajas de las biometrías. Recuperado de [http://www.ehowenespanol.com/cuales-son-ventajas-desventajas-biometrias-info\\_102877/](http://www.ehowenespanol.com/cuales-son-ventajas-desventajas-biometrias-info_102877/)

10.5 Reconocimiento de la Firma: Los elementos a tener en cuenta son presión de la pluma en el papel; movimientos que hace con la pluma y la velocidad de la firma.<sup>31</sup>

<b>VENTAJAS</b>	<b>DESVENTAJAS</b>
La firma es una sola para cada persona.	No es confiable debido a que la persona puede variar su firma dependiendo de la ocasión, por lo que al realizar la verificación con el sistema se debe firmar más de una vez.
Es Hardware que se utiliza es bastante sencillo.	Tiene un alto índice de falsificación.
Costo de implementación es bajo.	Bajo nivel de precisión.
Es un sistema con gran aceptabilidad y ha sido	La firma tiene una variación para una misma

<sup>31</sup>Paduraru, C. Cuáles son las ventajas y desventajas de las biometrías. Recuperado de [http://www.ehowenespanol.com/cuales-son-ventajas-desventajas-biometrias-info\\_102877/](http://www.ehowenespanol.com/cuales-son-ventajas-desventajas-biometrias-info_102877/)

utilizado desde el pasado.	persona con el pasar de los años por lo que hace difícil su identificación.
----------------------------	---

Fuentemayor, G. Avances en técnicas biométricas y sus aplicaciones en seguridad. Recuperado de <http://neutron.ing.ucv.ve/comunicaciones/Asignaturas/DifusionMultimedia/Tareas%202005-3/BIOMETRIA.doc>  
 Martínez, M. Vulnerabilidades en sistema biométrico de reconocimiento basado en huella dactilar: Ataques Hill – Climbing. Recuperado de <http://arantxa.ii.uam.es/~jms/pfsteleco/lecturas/20060926MarcosMartinezDiaz.pdf>

Algunos de los sistemas antes mencionados pueden combinarse para formar un sistema biométrico multimodal.

<b>Identificador Biométrico</b>	<b>Universalidad</b>	<b>Distintividad</b>	<b>Estabilidad</b>	<b>Evaluabilidad</b>	<b>Rendimiento</b>	<b>Aceptabilidad</b>	<b>Fraude</b>
<b>Huella Dactilar</b>	M	A	A	M	A	M	M
<b>Escáner de Retina</b>	A	A	M	B	A	B	B
<b>Iris</b>	A	A	A	M	A	B	B
<b>Firma</b>	B	B	B	A	B	A	A
<b>Geometría de la Mano</b>	M	M	M	A	M	M	M
<b>Rostro</b>	A	B	M	A	B	A	A

Martínez, M. Vulnerabilidades en sistema biométrico de reconocimiento basado en huella dactilar: Ataques Hill – Climbing. Recuperado de <http://arantxa.ii.uam.es/~jms/pfsteleco/lecturas/20060926MarcosMartinezDiaz.pdf>

Tabla 1. Comparación de los sistemas de reconocimiento Biométrico antes citados. Representan los niveles de Alto, Medio y Bajo. (A, M y B) Tabla extraída de Maltoni *et al.*, 2003). La cual fue modificada de acuerdo a las tecnologías requeridas para el presente trabajo.

10. Identificación de vulnerabilidades al control de acceso biométrico de huella dactilar

Lo primero que se busca al atacar un sistema biométrico es identificar los protocolos, sistema operativo y el personal que allí labora.

Se encontró una familia taiwanesa que desde hace cinco generaciones carecen de huellas, aun no se ha encontrado el motivo por el cual ocurre este fenómeno se cree que se debe a que carecen de la queratina 14 que se encuentra en la piel, sin esta proteína no se forman las huellas y la piel se hace frágil.

Esta familia sin huellas dactilares le ha causado grandes inconvenientes ya que no es posible tenerlos identificados y con el auge, aceptabilidad y seguridad que ha tenido el sistema biométrico dactilar para ellos el problema continua y persiste.<sup>32</sup>



Figura 6. Familia taiwanesa que carece de huella dactilar.

El sistema biométrico de huella dactilar presenta un grado de seguridad aceptable, vulnerabilidades y se enfrenta a una serie de ataques los cuales al ser ejecutados por parte de personas de mala fe puede llegar a desestabilizar la organización.

---

<sup>32</sup>Anónimo. No dejan huella. Recuperado de [http://www.soitu.es/soitu/2008/04/01/salud/1207067071\\_846773.html](http://www.soitu.es/soitu/2008/04/01/salud/1207067071_846773.html)

**Sabotaje** se pueden presentar a los **ataques al sensor**, cuando el individuo daña el sensor para impedir su normal funcionamiento y ahí es donde se aprovecha para su infiltración; **ataque a base de datos**, se requiere tener acceso al sistema, para eliminar, agregar o cambiar información que es de gran importancia para la comparación en el control de acceso.

**No actualizar la base de datos del sistema Biométrico** con la información de las personas que son contratadas para laborar dentro de la organización y de aquellas que son retiradas por terminación del contrato o situaciones diferentes a estas, es una de las fallas más constante ya que estas personas pueden seguir ingresando a la compañía y sustraer información valiosa o por el contrario aquellas personas que no son incluidas su ingreso se realiza de manera manual y allí es donde con más facilidad se presenta la suplantación ya que son personas que aún no son conocidas e identificadas en la organización, aunado se puede presentar **suplantación**, se manifiesta utilizando plantilla falsa de una huella dactilar latente o elaborada con goma, cera, gelatina, silicona, huellas dactilares adhesivas o de personas fallecidas. Para que el proceso de suplantación sea exitoso se requiere cooperación por parte de la persona a suplantar y que se conozca sobre el tipo de arquitectura del sistema biométrico. Aunque este tipo de suplantación se puede detectar y evitar instalando mecanismo de vida dentro del propio sensor de la huella dactilar.<sup>33</sup>

De igual manera se puede presentar algún tipo de **enfermedad común como la Dermatitis**, consiste en piel irritada o inflamada donde se puede alterar las líneas que forman las crestas papilares generando error en la lectura biométrica lo que hace complejo que las personas con ese tipo de problemas estén registradas en bases de datos.<sup>34</sup>

---

<sup>33</sup>Martínez, M. Vulnerabilidades en sistema biométrico de reconocimiento basado en huella dactilar: Ataques Hill – Climbing. Recuperado de <http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20060926MarcosMartinezDiaz.pdf>

<sup>34</sup>Anónimo. ( 2013, 2 de enero) Dermatitis produce error de lectura de huellas digitales. *Periódico vanguardia*. Recuperado de <http://www.vanguardia.com/vida-y-estilo/salud/189837-dermatitis-produce-error-de-lectura-de-las-huellas-digitales>

El **Trasplante de huellas por cirugía plástica**, es uno de los procedimientos más solicitados por las personas para evadir la justicia donde los médicos especialistas en cirugía plástica se ven expuestos a amenazas y ofertas económica incalculables, esto debido a los múltiples avances tecnológicos con el fin de identificar las personas, dicho procedimiento consiste en realizar un cambio de huellas dactilares de una a otra persona.<sup>35</sup>

Aunado a lo anterior existen otras situaciones que se presentan como vulnerabilidades la condición en la que debe estar el dedo al momento de tomar el registro no puede estar mojado o manchado, las altas temperaturas y la humedad puede afectar notablemente el lector y aquellas actividades laborales donde se manipulan químicos afectan las huellas dactilares.

11. Controles y buenas prácticas de prevención para minimizar el riesgo de suplantación o infiltración en sistema biométrico de huella dactilar.

**Detección de vida**, es aquella donde el lector biométrico debe estar en condiciones para detectar si la impresión dactilar que está intentado realizar el ingreso es de un ser humano vivo, esto con el objetivo de identificar una posible suplantación y posterior infiltración; **almacenamiento del patrón a verificar**, las huellas dactilares deben ser almacenadas por minucias no la huella completa, ya que será más difícil de reconstruirla en caso de ser robada la base de datos; **buena toma de huellas dactilar**, en caso de empresas donde sus empleados realicen trabajos con sustancias químicas, lo mejor será almacenar en la base de datos para posterior utilización las huellas dactilares de la mano que menos tenga contacto con estas sustancias, con esto se evitará a futuro situaciones relacionadas con cortes o un posible deterioro de la impresión dactilar;

---

<sup>35</sup>Pantaleón, D. Delincuencia Recurre a la Cirugía para evadir la justicia. *Periódico Listín Diario*. Recuperado de <http://www.listin.com.do/la-republica/2010/4/4/137207/Recurren-a-las-cirugias-para-evadir-a-la-justicia>



**adquirir sistemas tecnológicos de excelente calidad**, esto con el fin de evitar que el sistema al realizar las comparaciones de huellas dactilares arroje falsas alarmas o falsos positivos, al momento de presentarse este tipo de situaciones estos deben ser divulgados a todos los que pertenezcan a la cadena de responsabilidad para tomar las medidas y hacer el respectivo seguimiento, .<sup>36</sup>

---

<sup>36</sup> Instituto Nacional de Tecnologías de la Comunicación (INTECO). (2011). Guías sobre las tecnologías biométricas aplicadas a la seguridad. Recuperado de <http://www.inteco.es/file/ncKsGyFaqPdQ7ms3m2eDeA>.

## Conclusiones

1. Al analizar la Huella Dactilar como método de identificación se puede establecer que la biometría dactilar es una forma efectiva de conservar la privacidad, la plena identidad y proteger el sector la seguridad, empresarial, evitando suplantaciones e infiltraciones que traen como consecuencia fuga de información, pérdida recursos tangibles e intangibles entre otros.
2. Este tipo de sistema de reconocimiento dactilar es una de las técnicas más maduras, confiables y de fácil adquisición que puede llegar a presentar unas vulnerabilidades las cuales a tiempo se pueden prevenir realizando controles adecuados para mitigar el riesgo de ataques.
3. Dentro de las funciones principales de la dactiloscopia no es solamente identificar las personas para someterlas al castigo en caso de ejecutar una conducta delictiva, sino de recordarles que su responsabilidad puede ser demostrada.

## Bibliografía

Anónimo. (2007, 11 de diciembre). Historia de la dactiloscopia. Recuperado de

<http://www.dactiloscopia-dactiloscopia.blogspot.com/2007/12/dactiloscopia.html>.

Anónimo. No dejan huella. Recuperado de

[http://www.soitu.es/soitu/2008/04/01/salud/1207067071\\_846773.html](http://www.soitu.es/soitu/2008/04/01/salud/1207067071_846773.html)

Anónimo. (2013, 2 de enero) Dermatitis produce error de lectura de huellas digitales. *Periódico*

*vanguardia*. Recuperado de <http://www.vanguardia.com/vida-y-estilo/salud/189837-dermatitis-produce-error-de-lectura-de-las-huellas-digitales>

Anónimo. (2008, Mayo). Historia de la biometría. Recuperado de

[http://www.securetech.com.uy/servicios/info/biometria\\_5.htm](http://www.securetech.com.uy/servicios/info/biometria_5.htm).

Anónimo. Criminalística Legal. Dactiloscopia. Recuperado de

<http://www.criminalisticalegal.com/dactiloscopia.php>

Anónimo. Colegio de especialistas forenses. Dactiloscopia. Recuperado de

<http://coesfo.es.tl/Dactiloscop%EDa.htm>

Anónimo. Autenticación e Identificación Biométrica, control de personal. Recuperado de

<http://www.biodevices.com.ec/biometria>.

Anónimo. Autenticación de reconocimiento facial. Recuperado de

<http://www.umanick.com/index.php/tecnologia/reconocimiento-facial>

Anónimo. Historia de la Biometría. Recuperado de <http://www.biometria.gov.ar/acerca-de-la-biometria/historia-de-la-biometria.aspx>

Anónimo. Recuperado de

[http://www.kimaldi.com/area\\_de\\_conocimiento/biometria/que\\_es\\_la\\_biometria](http://www.kimaldi.com/area_de_conocimiento/biometria/que_es_la_biometria)

Carro, R. De las crestas Papilares (I). Recuperado de

[dialnet.unirioja.es/descarga/articulo/2869886.pdf](http://dialnet.unirioja.es/descarga/articulo/2869886.pdf).

Carro, R. (2009, 14 de mayo). El investigador: De las crestas papilares II. Recuperado de

<http://policiasenlared.blogspot.com/2009/05/de-las-crestas-papilares-ii.html>.

Chávez, C. (2008, 19 de julio). Huellas Dactilares. Recuperado de

<http://es.scribd.com/doc/3996151/Huellas-Dactilares>

Fonseca, G. (2012, 31 de enero) Sistemas biométricos. Recuperado de

<http://www.mentesinquietas.net/blog/archives/334>

Fuentemayor, G. Avances en técnicas biométricas y sus aplicaciones en seguridad. Recuperado de

<http://neutron.ing.ucv.ve/comunicaciones/Asignaturas/DifusionMultimedia/Tareas%202005-3/BIOMETRIA.doc>

González, M. (2004, enero). Introducción a la dactiloscopia como método de identificación de personas. Recuperado de <http://cienciaforense.com/Pages/EvidenciaFisica/Dactiloscopia.htm>

Instituto Nacional de Tecnologías de la Comunicación (INTECO). (2011). Guías sobre las tecnologías biométricas aplicadas a la seguridad. Recuperado de <http://www.inteco.es/file/ncKsGyFaqPdQ7ms3m2eDeA>.

Hernández, A. Bases teóricas y sistemas biométricos, Facultad de ingeniería biométrica informática. Recuperado de <http://redyseguridad.fi-p.unam.mx/proyectos/biometria/basesteoricas/caracteristicassistema.html>.

Iguaran, M. Manual único de criminalística de la Fiscalía General de la Nación. Recuperado de [http://www.fiscalia.gov.co/en/wp-content/uploads/2012/03/manual\\_de\\_criminalistica.pdf](http://www.fiscalia.gov.co/en/wp-content/uploads/2012/03/manual_de_criminalistica.pdf)

Jiménez, V. (2011. 9 de diciembre). Crestas Papilares. Recuperado de <http://es.scribd.com/doc/64679879/CRESTAS-PAPILARES>

Leaño, E. (1982). Curso de dactiloscopia clasificación de y archivo Sistema Henry. Registraduría Nacional del Estado Civil División de Identificación. Pág.21

Martínez, J. Sistemas de Clasificación dactiloscópica. Recuperado de [http://www.getocolombia.com/Archive/MANUAL%20SISTEMA%20HENRY%20CANA DIENSE%20\(YA\).pdf](http://www.getocolombia.com/Archive/MANUAL%20SISTEMA%20HENRY%20CANA DIENSE%20(YA).pdf)

Martínez, M. Vulnerabilidades en sistema biométrico de reconocimiento basado en huella dactilar: Ataques Hill – Climbing. Recuperado de

<http://arantxa.ii.uam.es/~jms/pfsteleco/lecturas/20060926MarcosMartinezDiaz.pdf>

Maza, M. Manual de Criminalística. Recuperado de

[http://clasev.net/v2/pluginfile.php/11083/mod\\_resource/content/0/INTRODUCCION\\_A\\_LA\\_DACTILOSCOPIA.pdf](http://clasev.net/v2/pluginfile.php/11083/mod_resource/content/0/INTRODUCCION_A_LA_DACTILOSCOPIA.pdf)

Mendoza, M. (2006). Post grado de criminalística Instituto de Trabajos Superiores Policía Nacional de Nicaragua. Recuperado

de <http://www.policia.gob.ni/cedoc/sector/acapol/postgrado/8%20CaracteristicaDactilares.pdf>

Morales, D. y Ruiz, J. Sistemas biométricos: Matching de huellas dactilares mediante transformada de Houg generalizada. Recuperado de

[http://www2.ing.puc.cl/~iing/ed429/sistemas\\_biometricos.htm](http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm)

Morales, C. (2009, 16 de diciembre). Biometría desde la perspectiva de la seguridad en la Tics. Recuperado de <http://es.scribd.com/doc/24156012/Biometria>.

Paduraru, C. Cuáles son las ventajas y desventajas de las biometrías. Recuperado de

[http://www.ehowenespanol.com/cuales-son-ventajas-desventajas-biometrias-info\\_102877/](http://www.ehowenespanol.com/cuales-son-ventajas-desventajas-biometrias-info_102877/).

Pantaleón, D. Delincuencia Recurre a la Cirugía para evadir la justicia. *Listin Diario*. Recuperado de <http://www.listin.com.do/la-republica/2010/4/4/137207/Recurren-a-las-cirugias-para-evadir-a-la-justicia>

Paños, S. (2010, 9 de junio). Historia de la biometría, presentación. Recuperado de

<http://www.slideshare.net/serweb/presentacion-biometra#btnNext>.

Sánchez, C. (2011, 3 de noviembre). La experiencia Colombiana en identificación biométrica

aplicada a las elecciones. Registraduría Nacional del Estado Civil - Biometría. *El Espectador*.

Recuperado de [www.registraduria.gov.co](http://www.registraduria.gov.co)

Sánchez, D. Reconocimiento Biométrico. Reconocimiento facial. Revista decana independiente

de seguridad, Seguritecnia. Recuperado de

[http://www.bormart.es/articulo\\_seguritecnia.php?id=2166](http://www.bormart.es/articulo_seguritecnia.php?id=2166)

Till, E. Biometrías 2. Recuperado de [www.biometria.gov.ar/media/74948/biometrias2.pdf](http://www.biometria.gov.ar/media/74948/biometrias2.pdf)

Valcárcel A. (1949). La Dactiloscopia en su aplicación a los Seguros Sociales. Recuperado de

[http://bvingesa.msc.es/bvingesa/es/catalogo\\_imagenes/grupo.cmd?path=1001350&responsabilidad\\_civil=on](http://bvingesa.msc.es/bvingesa/es/catalogo_imagenes/grupo.cmd?path=1001350&responsabilidad_civil=on)