



# **Introduccion a la Biometria por Huella Dactilar**

### PREGUNTAS MÁS FRECUENTES

#### **¿Qué es la biometría?**

La biometría es una técnica que consiste en identificar o verificar automáticamente la identidad de las personas, basándose en sus características físicas o sus pautas de comportamiento. Por ejemplo, el reconocimiento del iris, las características de la mano, las huellas dactilares o la voz.

#### **¿Cuál es el mejor método biométrico?**

Cada método tiene sus ventajas y desventajas, según la aplicación que se haga de él y las personas que utilicen los equipos. Ningún método es "el mejor". Aparte de la precisión y la seguridad de los equipos biométricos, hay que considerar también otros factores, como el confort, la facilidad de uso, la aceptación por parte del usuario, el mantenimiento y el costo.

#### **¿Conviene sustituir los códigos de acceso por biometría o utilizar ambos métodos para aumentar la seguridad?**

Como todo secreto, un código de acceso se puede revelar en el momento más inesperado. También es posible olvidarlo. El código de acceso puede traspasarse a otra persona debido a un descuido, robo o fraude. Por el contrario, las características físicas o las pautas de comportamiento de cada persona son únicas. Basta imaginarse que cada persona es una "llave" que no se puede copiar, ceder, perder ni robar. Como la biometría está unida indisolublemente a esta persona única, cualquier falsificación resultaría excesivamente costosa. Por último, no hay que olvidar un factor fundamental: se elimina la obligación de recordar códigos de acceso complejos.

#### **¿Existe la posibilidad de que me roben mi dispositivo biométrico y, con él, mi identidad?**

Está claro que es muy fácil robar una tarjeta, obtener fraudulentamente una clave o código de acceso o llegar a conocer un PIN. Pero las cosas se ponen muy difíciles con la biometría, precisamente porque cada ser humano es único. Si además de la técnica biométrica, se utiliza un código de acceso complementario, la seguridad se incrementará significativamente.

La biometría establece una relación muy segura entre la persona y el dispositivo identificador de proximidad, que el sistema utiliza para representar al individuo. De esta manera, resulta casi imposible robar la identidad. La seguridad de esta

relación dependerá de la coincidencia entre las características biométricas y el patrón. No obstante, si la integridad tiene algún punto débil, cualquier impostor podrá acceder a esa relación para intentar robar la identidad. Es cierto que la biometría reduce considerablemente los robos de identidad, pero no puede garantizar la eliminación absoluta de este riesgo.

**Tal y como están las cosas, también puede ocurrir que un delincuente corte el dedo a una persona para extraer fondos de un banco. ¿Ofrece alguna solución la biometría en estos casos?**

La mayoría de los sistemas biométricos son capaces de determinar si ese dedo pertenece a una persona viva o no. No obstante, esta posibilidad es bastante remota, porque el tejido orgánico, una vez separado del cuerpo, comienza a deteriorarse de inmediato y la biometría detecta esas alteraciones enseguida. Los delincuentes saben que disponen de muy poco tiempo para actuar y esto es un elemento disuasorio, al igual que el hecho de que recibirán sanciones mucho más graves por estos actos criminales.

**¿Qué ocurrirá si, por ejemplo, debido a un accidente, cambia temporalmente alguna característica física?**

El sistema biométrico no funcionará. Por ejemplo, en los sistemas de reconocimiento de huella dactilar, esto dependerá de cuántos patrones de dedos hayan sido guardados. Precisamente esta es una de las ventajas de este método en comparación con otros sistemas biométricos, que sólo pueden guardar una o dos características. Algunos sistemas están preparados para guardar los patrones de los diez dedos de las manos. Supongamos que una mano está lesionada. En ese caso, se utilizará cualquiera de los cinco dedos de la otra mano para la identificación. En el método de reconocimiento de iris, es probable que los usuarios ciegos no sean reconocidos. Tampoco podemos olvidar que hay usuarios que no desean utilizar la biometría. Para todas estas situaciones, se puede permitir el uso de un método alternativo. No obstante, hay que saber que algunos sistemas biométricos no admiten métodos alternativos. Tampoco debemos olvidar que dichos métodos serán más lentos y menos confortables.

**Se dice que los métodos biométricos son muy complejos y costosos. ¿Es cierto?**

Puede parecer que un sistema biométrico para acceder a una vivienda será siempre costoso. Pero no hay que olvidar que estos sistemas no sólo se han perfeccionado y se ha reducido su costo de adquisición e instalación, sino que también contribuyen al ahorro en otras medidas de seguridad. Por eso, es importante que los especialistas en biometría realicen siempre una evaluación adecuada de los pro y los contra de su instalación en determinado lugar.

**¿Puede el sistema biométrico incumplir las normas relativas a la protección de la información y los derechos humanos?**

El uso de un dispositivo biométrico para verificar la identidad no afecta en absoluto la intimidad de la persona. Sin embargo, en determinadas circunstancias, el almacenamiento de información biométrica junto con otra clase de información personal sí puede estar sujeto a estas normas legislativas. En ese caso, la información se tendrá que procesar con los mismos controles que

se utilizan para cualquier otra información personal y quedará sujeta a las restricciones legales correspondientes.

Es importante saber que la tecnología biométrica ofrece la posibilidad de proteger la información personal y la intimidad de las personas, ya que exige una identificación directa y la autenticación de las personas que tienen acceso a ella. Por ejemplo, en el caso de expedientes de personal, informes médicos o actas policiales, con la biometría se puede proteger la intimidad de los interesados contra accesos no autorizados.

### **Aplicaciones en cualquier lugar en un instante**

#### **Verificación de personas para:**

Sistemas de control de acceso, tiempos y presencia (para la seguridad de edificios, aeropuertos, zonas de seguridad, etc.).

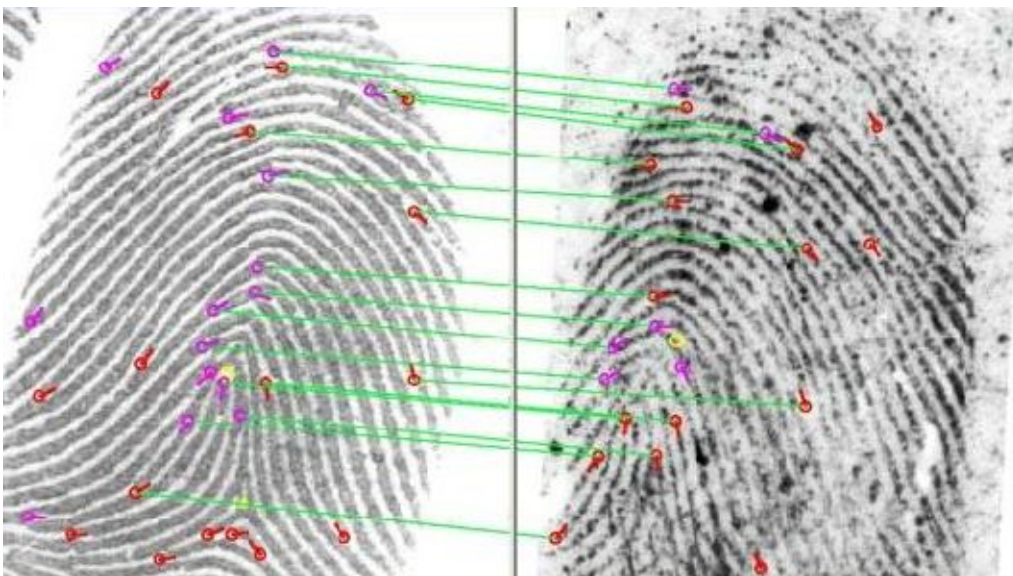
Control de tiempo y presencia.

Industria de servicios bancarios y financieros: tarjeta de seguridad inteligente, terminales de punto de venta, cajeros automáticos, comercio electrónico, etc.

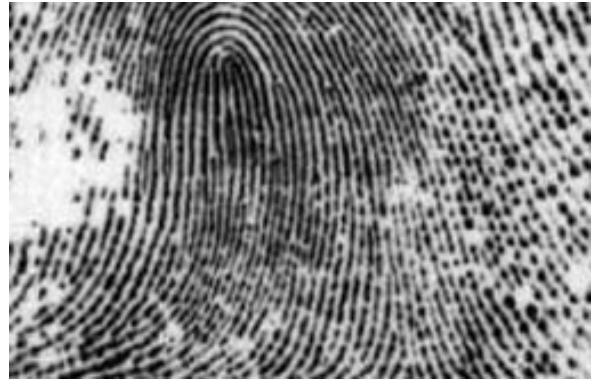
Industria: industria química y farmacéutica, industria alimentaria, industria de defensa, etc.

Sectores públicos: autoridades de inmigración, oficinas de bienestar social, imprentas del Estado de títulos y documentos nacionales de identidad, autoridades electorales, oficinas públicas, etc.

Procedimientos forenses preliminares.



En 1953 los jóvenes científicos ingleses Francis Crick y James Watson, entraron al bar “The Eagle” anunciando que habían encontrado “el secreto de la vida”. Su hallazgo: el ADN, información que hace posible identificar de forma exacta a los seres vivos y ha permitido los más grandes avances médicos de la historia.



Sin embargo, mucho antes de ese descubrimiento, durante siglos la huella digital fue la prueba más irrefutable para distinguir con exactitud la identidad de una persona, pues se trata de una característica física única en cada ser humano.

Formada por un patrón de crestas y valles, este es el sistema de reconocimiento biométrico más antiguo. Pese a ello, continúa implementándose en múltiples áreas que van desde la criminología hasta los documentos de identidad y ya comienza a integrarse a los sistemas de tecnología más avanzados, donde incluso se están desarrollando plataformas que permiten utilizar la huella digital electrónica para realizar complejos trámites a través de Internet.

### **Seña de la especie**

Las huellas dactilares son una característica física que sólo se presenta en los primates, en los humanos se forman a partir de la sexta semana de vida intrauterina y sus características no varían con la edad de la persona.

Además de crestas papilares y valles interpapilares, las rugosidades con formas arbitrarias que adopta la piel que cubre la yema de los dedos posee minucias, es decir, discontinuidades locales de las crestas.

Dado que el sudor se deposita en los surcos, al tocar alguna superficie, la marca única de cada persona queda impresa en el objeto, por lo que es posible obtener

## Tecnologías Biométricas de Identificación

una copia del negativo de una huella digital, superponiendo un polvo blanco de consistencia similar al talco, pues éste absorberá la grasa.

Si bien en criminología se ha utilizado la huella digital como prueba de la presencia de una persona en un determinado lugar durante el último siglo, su aplicación identificadora en otras áreas viene de mucho antes.

Ya en la antigua Babilonia, muchas de las transacciones comerciales quedaban grabadas en tablas de arcilla que se firmaban con la huella digital, práctica que también existía en Persia durante el Siglo XIV, época en la que oficiales del gobierno notaron que no había dos huellas dactilares iguales. Asimismo, la antigua legislación china establecía que para divorciarse era necesario un documento que expusiera siete motivos y fuera firmado con la impresión digital.

En la cultura occidental en tanto, las huellas dactilares comenzaron a ser utilizadas para validar documentos y contratos a partir del Siglo XIX, época en la que se registran las primeras investigaciones sistemáticas sobre el tema en Europa, lo que permitió masificar el uso de la identificación dactiloscópica en el campo civil y criminal.

En 1880 el cirujano inglés Henry Faulds, presentó un estudio sobre los surcos de la piel, inspirado en la presencia de marcas de dedos en piezas de cerámica prehistórica. En su trabajo, el médico propuso la importancia de huellas digitales como una forma para identificar personas, estableciendo un método de clasificación.

Al conocer sus investigaciones, Charles Darwin, quien ya tenía demasiados años como para abordar el desafío, decidió entregar la tarea a su primo, el científico inglés Francis Galton.

### **El Modelo de Galton**

Tras 12 años de arduo estudio, Francis Galton publicó el libro “Fingerprints”, donde estableció la individualidad y permanencia de huellas digitales, señalando que este rasgo poligénico no cambia a lo largo de la vida de un individuo y que no existen dos huellas dactilares exactamente iguales, por lo que postuló que serían una buena herramienta para identificar humanos.

En el libro, Galton estableció el primer sistema de clasificación para las huellas digitales, mostrando las características por las cuales pueden ser identificadas, índices que continúan utilizándose en la actualidad.

A fines del Siglo XIX, Juan Vucetich, jefe de la Oficina de Estadística de la Policía

## Tecnologías Biométricas de Identificación

de la Provincia de Buenos Aires, Argentina, simplificó el modelo de Galton creando el Sistema Dactiloscópico Argentino, que reduce la clasificación inicial de las huellas a sólo cuatro tipos. De este modo, en 1892 se aplicó la primera identificación criminal a través de este método, cuando mediante las huellas dactilares se logró incriminar a una mujer como la asesina de sus dos hijos, pues apoyó su mano ensangrentada en la puerta, lo que la delató.

Después de este hecho, las huellas digitales comenzaron a ser utilizadas para la identificación criminal en buena parte del mundo occidental, convirtiéndose en las décadas siguientes en el método más usado para identificar personas en todos los ámbitos.

En Estados Unidos, la Oficina Federal de Investigaciones (FBI) en 1946 ya había procesado más de 100 millones de tarjetas con huellas digitales en archivos mantenidos manualmente, cifra que se duplicó en los años '70.

A partir de 1978 la computación avanzó vertiginosamente en el campo de la informática, a raíz de lo cual el FBI comenzó a digitalizar millones de fichas dactilares clasificándolas mediante recuento de líneas. En 1989, basado en la misma tecnología, se planificó un nuevo sistema, denominado AFIS (Sistema automatizado para la identificación de impresiones dactilares, por su sigla en inglés), el cual permite una impresionante capacidad de búsqueda de fichas dactilares.

Esta herramienta es una gran base de datos, que se sustenta en un archivo dactiloscópico, alimentado mediante un escáner que toma fotografías digitales de las impresiones dactiloscópicas.

Para comparar y encontrar las imágenes de cada huella, la herramienta debe efectuar varios procesos y transformaciones de la imagen obtenida, para detectar vectores que se guardan en la base de datos del sistema, el cual mediante formulas matemáticas compara la similitud de los vectores y calcula el porcentaje de coincidencia entre huellas. Así mientras mayor sea la cantidad de puntos coincidentes entre una huella y otra, es más probable que pertenezca a la misma persona.

### **Más allá de la medicina**

Durante los últimos años los dibujos de las huellas dactilares de las manos y pies, han motivado numerosas investigaciones especializadas, que permiten asociar estos rasgos a algunas patologías. Así, las huellas de los recién nacidos se están estudiando para el diagnóstico precoz de anomalías cromosómicas.

La herencia de las huellas dactilares, al igual que los demás caracteres de herencia poligénica, también se ve influenciada por factores ambientales aunque, debido a la precocidad y rapidez del desarrollo de éstas, el fenotipo no cambia tras el nacimiento.

Las huellas dactilares se pueden detectar a partir de la sexta semana de gestación, llegando a su mayor desarrollo hacia la semana número 13 y su morfología final no se verá alterada durante el restante desarrollo prenatal y postnatal.

Dada su permanencia, los patrones de los dibujos de las huellas se pueden clasificar principalmente en tres grupos: arcos, lazos y espirales, cuyas alteraciones pueden dar cuenta de enfermedades tales como Trisomía 21, Trisomía 18 y Síndrome de Turner, entre otras.

Pero más allá de sus usos para identificación criminal y en medicina, en la actualidad y gracias a los pasos agigantados con que avanza la tecnología, las huellas digitales comienzan a ser utilizadas en vastas áreas, hecho que hace algunas décadas hubiese parecido un argumento de ciencia ficción.

De este modo, se espera que en un futuro cercano no necesitemos llevar un documento para demostrar nuestra identidad y que la impresión digital reemplace a las llaves de las casas, sirva para poner en marcha los automóviles, nos permita votar y baste con apoyar un dedo sobre un escáner para efectuar transacciones bancarias, demostrar quienes somos, de donde venimos y que antecedentes y créditos tenemos individualmente.

### **El poder de la Biométrica**

En la actualidad, la mayoría de los países del mundo utiliza las huellas digitales como sistema práctico y seguro de identificación. De la mano de las nuevas tecnologías, han surgido herramientas que permitirán otras formas de verificación para las personas.

Los datos biométricos, como las medidas del rostro, las huellas digitales y del iris, la forma de las orejas y las manos, la estatura, los mapas del iris y de la retina, el timbre y la modulación de la voz, a través de avanzados sistemas tecnológicos hacen posible identificar a las personas de forma cada vez más segura.

Las herramientas biométricas son sistemas automáticos de chequeo de patrones, que en pocos segundos pueden obtener una muestra del individuo, información que comparan con una base de datos para determinar si los documentos concuerdan o no a la identidad de una persona.

A diferencia de otros sistemas de seguridad, los datos biométricos no se pueden

robar o perder, porque forman parte del individuo, por lo que nadie los puede memorizar, ni tampoco es necesario recordarlos, como sucede con las claves y contraseñas.

En el caso de la fotografía biométrica, ésta se puede adjuntar en documentos como pasaportes o tarjetas y cada vez que se necesite verificar la identidad del portador de dicho documento, solo será necesario escanear su rostro.

De hecho, en algunos países ya se han comenzado a introducir información biométrica codificada en los pasaportes de sus ciudadanos. Es el caso de Suiza, país cuyos documentos cuentan con lectura óptica desde 2003 y se preparan para introducir en los pasaportes una pequeña pastilla con otros datos biométricos más exhaustivos, como información sobre la estructura facial de las personas, lo que se hará efectivo durante 2005, como un proyecto piloto que durará cinco años.

Con todo esto, se estima que la tecnología biométrica comenzará a imponerse como una exigencia a escala mundial en las próximas décadas, siendo masificado su uso especialmente en los lugares de trabajo.

Sin embargo, dadas las respectivas realidades locales de los países en vías de desarrollo, es muy probable que lo primero que se implemente sean los elementos detectores de la biometría de las huellas digitales, puesto que dichos lectores son más asequibles por su bajo costo.

Esta tecnología permite detectar modelos y formas presentes en la superficie de las yemas de los dedos y verificar la identidad de la persona a través de diversos enfoques: hay sistemas que funcionan como el proceso policial de coincidencia de huellas; otros utilizan dispositivos para describir los modelos y rasgos esquemáticos de las huellas, mientras que algunos manejan modelos tridimensionales basados en ultrasonido, que permiten incluso detectar si un dedo está vivo o muerto.

Chile ha estado a la vanguardia en este sentido. En septiembre de 2002, el Servicio de Registro Civil e Identificación incorporó a las cédulas un algoritmo matemático que permite codificar la información biométrica del dedo pulgar, sistema a través del cual es posible determinar biométricamente si el portador del documento es el titular, evitando así las suplantaciones de identidad. Dicha cédula posiciona a Chile como el primer país del mundo con la posibilidad de tener un documento oficial con capacidades transaccionales.

Pero la tecnología biométrica digital también ha ingresado con fuerza en los últimos años en otros ámbitos, permitiendo la compra de bonos para atención

médica, el control de acceso a algunas empresas e incluso ha comenzado a utilizarse en algunas casas comerciales, cuyas máquinas ofrecen el pago de cuentas en dinero efectivo, sin necesidad de utilizar sobres o formularios. Asimismo, está a la venta un mouse que detecta la huella dactilar y durante 2005 el sistema será implementado en un alto porcentaje de los cajeros automáticos. Dicha operación se realizará en línea con el Servicio de Registro Civil y será obligatoria para todos aquellos giros que sobrepasen un determinado monto, que aún está por definirse.

En este último ámbito, el uso de la huella digital permitirá que no sólo las personas con tarjetas puedan usar los cajeros, pues incluso alguien que no posea cuenta corriente, podrá girar dinero que le envíen al indicar un código más su huella digital.

Mientras que los avances científicos con sus aspectos interactivos y digitales afectan nuestra vida en los ámbitos más diversos, paulatinamente los sistemas de seguridad están evolucionando hacia un área que es la más simple y, a la vez, la más compleja de todas: buscan reconocer las marcas distintivas de nuestro cuerpo, las mismas que en la antigüedad se imprimían en la arcilla.

### La seguridad en un dedo. Casa segura.

Las técnicas de identificación a través de la huella dactilar pronto podrán expandirse hasta los hogares. Así, nadie podrá entrar a la casa si sus características no están previamente registradas.

La escena sería más o menos así: ni rejas, ni rondines con palos, ni fieros perros guardianes, ni vistosos y ruidosos sistemas de alarma que rodeen su casa. Sólo un pequeño lector de huellas dactilares le asegura que, a punta de tecnología, nadie será capaz de dar un paso al interior de su vivienda si no está plenamente identificado.

Así en vez de llaves que se pierden, son robadas, copiadas o adulteradas, cada habitante de la casa tendrá que poner su dedo índice, único e irrepitable, para que las puertas se vayan abriendo una a una como arte de magia. Una casa inteligente que reconoce a sus dueños.

Quien no tenga sus huellas previamente registradas no podrá entrar por más que lo intente, a no ser que alguien desde adentro le permita ingresar. Un sistema que parece simple a la vista, pero tan complejo en términos técnicos que es prácticamente invulnerable.

Lo que hay detrás de este sistema se llama biometría y se resume como la ciencia que estudia las características físicas que son únicas en la persona, como el reconocimiento de voz, el iris, los rasgos faciales y, lo más popular, las huellas digitales. Las ventajas de las yemas del dedo por sobre las otras técnicas biométricas son prácticas: la tecnología de implementación es más simple, notoriamente más barata y las huellas además son imborrables, cuantificables y tienen una tasa de seguridad cercana al 99.9998%.

Ojo que los sistemas biométricos incluyen un dispositivo de captación y un software biométrico que interpreta la muestra física y la transforma en una secuencia numérica. En el caso de reconocimiento de la huella digital, en ningún caso se extrae la imagen de la huella, sino una secuencia de números que la representan.

#### Casa segura

Aunque aún eran aplicados mayoritariamente en empresas, para el control de empleados o acceso a zonas restringidas de una compañía, la masificación de la tecnología biométrica y el abaratamiento de los lectores de huella digital hace que poco a poco vaya tomando terreno en los hogares, ya sea en casas o en el acceso a edificios.

Según algunos estudios, se cree que más del 60% de los robos cometidos en casas se producen por la puerta principal, mientras que el 27% de los delincuentes entra por las ventanas y un 11% por otras puertas.

Juan Daniel Reich, Senior Solutions Manager Telefónica Empresas, está seguro de que la biometría hogareña no se va a demorar mas en llegar. De hecho ve difícil que sigamos usando las actuales llaves de metal para entrar a una puerta en el futuro. "La pregunta interesante, como con toda tecnología nueva es cuándo se masificará, aunque la historia nos ha demostrado que las tecnologías se adoptan con relativa

rapidez en términos históricos", dice.

Cristian Sepúlveda, gerente de soluciones biométricas de NEC Chile, dice que actualmente en Asia, Estados Unidos y Europa, ya existen soluciones biométricas totalmente operativas para el mercado de casas, y especialmente en un contexto social de alta tecnología, donde impera el concepto de "high tech" o ultra tecnológico. Aquí el asunto es un poco diferente.

"Los controles de acceso biométricos tienen un costo variable en Chile, que fluctúa entre los 1.500 y 1.800 dólares, con lo cual la demanda viene preferentemente desde las empresas y no desde los hogares. No obstante los productos están disponibles y si alguien quiere pagar por ello puede implementarlo. De hecho, para residencias con un valor superior a las 4.500 UF, se recomienda por seguridad y control", dice.

De todas formas ya hay acercamientos un poco menos completos que soluciones biométricas globales, pero más baratas para instalar en el hogar. El primer paso a la biometría casera son las "cerraduras biométricas", que se venden fundamentalmente en Estados Unidos, Europa y países como México y que también se pueden encontrar en sitios de subasta en internet.

Las cerraduras tradicionales no son rival para los cacos de hoy en día, pero las biométricas sí. Falsificar una huella dactilar es muy difícil, falsificar el iris, imposible. Instalar una cerradura biométrica en casa es una garantía de seguridad, pero hay que tener en cuenta que el precio puede dispararse y que necesitan alimentación eléctrica para funcionar —normalmente pilas—. Una cerradura con lector de huellas dactilares cuesta alrededor de 450 euros, y hay que añadir la mano de obra del instalador. Las cerraduras de identificación a través de iris son mucho más caras.