Tecnologías biométricas aplicadas a la ciberseguridad

Una guía de aproximación para el empresario

INSTITUTO NACIONAL
DE CIBERSEGURIDAD

SPANISH NATIONAL
CIBERSECURITY INSTITUTE

10 incibe_
2006-2016
TRABAJANDO POR
LA CONFIANZA DIGITAL

Índice

Índice

¿Qué es la Biometría?

La **biometría** es un método de reconocimiento de personas basado en sus características fisiológicas o de comportamiento. Se trata de un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a sus congéneres por su aspecto físico, su voz, su forma de andar, etc.

En la actualidad, la tecnología ha permitido automatizar y perfeccionar estos procesos de reconocimiento biométrico, de forma que tienen multitud de aplicaciones y finalidades – especialmente aquellas relacionadas con la seguridad–, algunas de las cuales se expondrán a lo largo de la presente guía.

Ya a comienzo de los años 70, *Shearson Hamil,* una empresa de Wall Street, instaló *Identimat*, un sistema de identificación automática basado en huella dactilar que se utilizó para el control de acceso físico a instalaciones, siendo la primera solución biométrica de uso comercial.

Desde entonces se ha investigado mucho en el campo de la biometría, aplicándose a otros rasgos biométricos diferentes de la huella dactilar.

A día de hoy, el avance en el conocimiento de dichos rasgos y sus correspondientes ventajas e inconvenientes, unido a las posibilidades que ofrece la tecnología, hacen que la biometría se considere uno de los elementos clave en cuanto a técnicas de identificación y seguridad en el futuro.

Esta guía tiene como objetivo, por un lado, la descripción de las diferentes técnicas biométricas existentes, sus características, sus aplicaciones, sus beneficios y riesgos, así como la identificación de aquellos derechos y obligaciones de los diferentes actores del mundo de la biometría. Por otro lado, tiene como finalidad no solo **dar a conocer** estos métodos de identificación, sino además señalar qué **medidas y buenas prácticas** han de llevarse a cabo para que su uso sea seguro y respetuoso con la privacidad de los ciudadanos.

Las tecnologías biométricas se definen como métodos automáticos utilizados para reconocer a personas sobre la base del análisis de sus características físicas o de comportamiento.

Dependiendo de la técnica biométrica empleada, los parámetros considerados son diferentes: los surcos de la huella dactilar, la geometría de la mano, la voz, la imagen facial, etc. De estos parámetros se extrae un patrón único para cada persona, que será el que se utilice para posteriores comparaciones. Las tecnologías biométricas se aplican en dos fases: registro y autenticación.

Las características biométricas empleadas deben tener las siguientes propiedades:

- universalidad: todos los individuos las tienen
- singularidad o univocidad: distinguen a cada individuo
- permanencia en el tiempo y en distintas condiciones ambientales
- medibles de forma cuantitativa

Y las tecnologías para medir estas características deben proporcionar:

- rendimiento: nivel de exactitud
- aceptación: por parte del usuario
- resistencia al fraude y usurpación

Generalmente para poder ser usado los individuos deben registrar su identidad en el sistema por medio de la captura de una serie de parámetros biométricos. Este es el denominado **proceso de registro**, que se compone de tres fases distintas:

Figura 1: Proceso de registro

- **Captura** de los parámetros biométricos.
- **Procesamiento** creando una plantilla con las características personales de los parámetros capturados.
- **Inscripción** de la plantilla procesada guardándola en un medio de almacenamiento adecuado. Una vez que la inscripción está completa, el sistema puede autenticar a las personas mediante el uso de la plantilla.

2 Características y tipología de las Tecnologías Biométricas

A continuación, mediante el **proceso de autenticación** se captura una muestra biométrica del individuo que se comparará con las plantillas ya registradas. Esta autenticación puede realizarse de dos modos diferentes:

Identificación: consiste en la comparación de la muestra recogida del usuario frente a una base de datos de rasgos biométricos registrados previamente. No se precisa de identificación inicial del usuario, es decir, el único dato que se recoge en el momento de uso es la muestra biométrica, sin apoyo de un nombre de usuario o cualquier otro tipo de reconocimiento. Este método requiere de un proceso de cálculo complejo, puesto que se ha de comparar esta muestra con cada una de las anteriormente almacenadas para buscar una coincidencia.

Figura 2: Proceso de autentificación

Verificación: aquí, sin embargo, el primer paso del proceso es la identificación del usuario mediante algún nombre de usuario, tarjeta o algún otro método. De este modo se selecciona de la base de datos el patrón que anteriormente se ha registrado para dicho usuario. Posteriormente, el sistema recoge la característica biométrica y la compara con la que tiene almacenada. Es un proceso simple, al tener que comparar únicamente dos muestras, en el que el resultado es positivo o negativo.

Fundamentalmente se distinguen **dos grupos de tecnologías** biométricas en función de la metodología utilizada: aquellas que analizan **características fisiológicas** de las personas y aquellas que analizan su **comportamiento.**

Por otra parte dependiendo de qué tecnologías utilizan los **sistemas de identificación biométrica** se dividen en:

2 Características y tipología de las Tecnologías Biométricas

2.1 Tecnologías biométricas fisiológicas

Las tecnologías biométricas fisiológicas se caracterizan por considerar parámetros derivados de la medición directa de algún rasgo estrictamente físico del cuerpo humano a la hora de identificar personas.

2.1.1. Huella dactilar

La identificación basada en huella dactilar es la más antigua de las técnicas biométricas y ha sido utilizada en un gran número de aplicaciones debido a que se considera que las huellas dactilares son únicas e inalterables.

Es el rasgo biométrico más utilizado para autenticación. Se han desarrollado una amplia gama de tecnologías de captura, con distintas características de funcionamiento. Asimismo, tiene como ventajas su alta tasa de precisión y su facilidad de uso.

Existen dos tipos de técnicas de búsqueda de coincidencias entre muestras de huella dactilar:

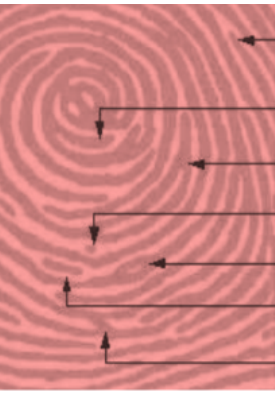


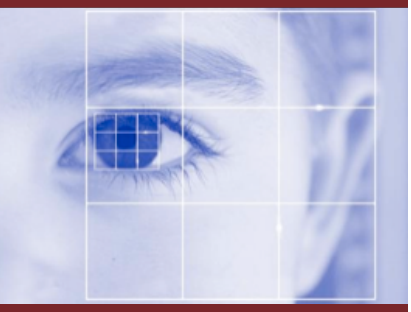
Figura 3: Minucias de huella dactilar

- **Basadas en minucias:** Esta técnica basa su mecanismo de autenticación en las «minucias», es decir, en determinadas formas fácilmente identificables existentes en la huella dactilar. Así, se registra el tipo de minucia y su posición dentro de la huella, estableciendo una serie de mediciones. De esta forma, el modelo o plantilla correspondiente a cada usuario es un esquema en el que se indican las minucias que se han de detectar, su posición y las distancias que separan unas de otras.

No obstante, existen algunas dificultades asociadas a este método. Por un lado, no es sencillo extraer de forma precisa las mencionadas minucias cuando la calidad de la muestra no es buena. Por otro lado, no se tiene en cuenta el patrón global de crestas y surcos.

- **Basadas en correlación:** Mediante la utilización de esta técnica se analiza el patrón global seguido por la huella dactilar, es decir, el esquema general del conjunto de la huella en lugar de las minucias. Esta técnica requiere un registro preciso, pero su principal inconveniente es que se ve afectada por la traslación y la rotación de la imagen.

Figura 4: Patrones de huella dactilar



El pequeño tamaño de los lectores, su fácil integración (pudiendo ser incluidos de forma sencilla en teclados), y su usabilidad, así como los bajos costes asociados a los mismos, convierten a la huella dactilar en una tecnología muy útil para su implantación en oficinas y hogares.

No en vano, esta tecnología está siendo usada cada vez más en dispositivos móviles y portátiles, ya que es una tecnología perfecta para la autenticación sencilla de usuarios.

2.1.2. Reconocimiento facial

El reconocimiento facial es una técnica mediante la cual se reconoce a una persona a partir de una imagen o fotografía. Para ello, se utilizan programas de cálculo que analizan imágenes de rostros humanos.

Entre los aspectos clave empleados para la comparación se encuentran mediciones como la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula.

A diferencia de otros sistemas biométricos, el reconocimiento facial puede ser utilizado para la vigilancia general, habitualmente mediante cámaras de video.

Mejoras en los sistemas de reconocimiento facial han podido discernir entre personas reales y fotografías, sin embargo, cualquier persona puede modificar visualmente su cara de manera sencilla, como por ejemplo utilizando unas gafas de sol o dejándose crecer la barba.

Asimismo, debe considerarse que el rostro de las personas varía con la edad. Existen soluciones de software que utilizan esta tecnología para identificación de usuarios en dispositivos móviles y portátiles.

2.1.3. Reconocimiento de iris

Utiliza las características del iris humano con el fin de verificar la identidad de un individuo.

Los patrones de iris vienen marcados desde el nacimiento y rara vez cambian. Son extremadamente complejos, contienen una gran cantidad de información y tienen más de 200 propiedades únicas.

El escaneado del iris se lleva a cabo con una cámara de infrarrojos especializada —situada por lo general muy cerca de la persona— que ilumina el ojo realizando una fotografía de alta resolución. Este proceso dura sólo uno o dos segundos y proporciona los detalles del iris que se localizan, registran y almacenan para realizar futuras verificaciones.

Es importante señalar que no existe ningún riesgo para la salud, ya que al obtenerse la muestra mediante una cámara de infrarrojos, no hay peligro de que el ojo resulte dañado en el proceso.

El hecho de que los ojos derecho e izquierdo de cada persona sean diferentes y que los patrones sean difíciles de capturar, tienen como consecuencia que el reconocimiento de iris sea una de las tecnologías biométricas más resistentes al fraude.

2.1.4. Reconocimiento de la geometría de la mano

Esta tecnología utiliza la forma de la mano para confirmar la identidad del individuo. Para la captura de la muestra se emplean una serie de cámaras que toman imágenes en 3-D de la mano desde diferentes ángulos.

Las características extraídas incluyen las curvas de los dedos, su grosor y longitud, la altura y la anchura del dorso de la mano, las distancias entre las articulaciones y la estructura ósea en general. No se tienen en cuenta detalles superficiales, tales como huellas dactilares, líneas, cicatrices o suciedad, así como las uñas, que pueden variar de tamaño en un breve período de tiempo.

Si bien es cierto que la estructura de los huesos y las articulaciones de la mano son rasgos relativamente constantes, no obstante otras circunstancias, como una inflamación o una lesión, pueden variar la estructura básica de la mano dificultando la autenticación.

2.1.5. Reconocimiento de retina

El escáner biométrico de la retina se basa en la utilización del patrón de los vasos sanguíneos contenidos en la misma. El hecho de que cada patrón sea único (incluso en gemelos idénticos al ser independiente de factores genéticos) y que se mantenga invariable a lo largo del tiempo, la convierten en una técnica idónea para entornos de alta seguridad.

Pese a que su tasa de falsos positivos sea prácticamente nula, esta tecnología tiene un inconveniente considerable ya que es necesaria la total colaboración por parte del usuario al tratarse de un proceso que puede resultar incómodo. La toma de la muestra se realiza a partir de la pupila, lo que requiere que el usuario permanezca inmóvil y muy cerca del sensor durante la captura de la imagen. No obstante, el uso de una cámara de infrarrojos para la captura evita el riesgo de que el ojo pueda resultar dañado en el proceso.

2 Características y tipología de las Tecnologías Biométricas

2.1.6. Reconocimiento vascular

En la biometría vascular se extrae el patrón biométrico a partir de la geometría del árbol de venas del dedo (o de las muñecas). A diferencia de la huella dactilar el patrón biométrico es interno, por esta razón no deja rastro y sólo se puede conseguir en presencia de la persona. Es por tanto muy difícil el robo de identidad.

Debido a estas características es especialmente indicado para entornos de alta seguridad, así como en situaciones en que la superficie del dedo pueda estar en mal estado, erosionada o poco limpia.

2.1.7. Otras formas de biometría fisiológica

Existen además otras técnicas que analizan:

- líneas de la palma de la mano
- forma de las orejas
- piel, textura de la superficie dérmica
- ADN, patrones personales en el genoma humano;
- composición química del olor corporal.

Estas técnicas son todavía novedosas y su uso es muy reducido. Su implantación presenta mayores problemas que en el resto de los casos, ya sea por menor eficacia o por necesitar mayores esfuerzos en el procesamiento de la información.

2.2 Tecnologías biométricas de comportamiento

Las tecnologías biométricas de comportamiento se caracterizan por considerar en el proceso de identificación rasgos derivados de una acción (al escribir, al caminar, etc.) realizada por una persona. Por tanto, incluyen la variable tiempo, ya que toda acción tiene un comienzo, un desarrollo y un final.

2.2.1. Reconocimiento de firma

Esta técnica analiza la firma manuscrita para confirmar la identidad del usuario firmante.

Existen dos variantes a la hora de identificar a las personas según su firma:

- **Comparación simple:** se considera el grado de parecido entre dos firmas, la original y la que está siendo verificada.
- **Verificación dinámica:** se hace un análisis de la forma, la velocidad, la presión de la pluma/bolígrafo y la duración del proceso de firma. No se considera significativa la forma o el aspecto de la firma, sino los cambios en la velocidad y la presión que ocurren durante el proceso, ya que sólo el firmante original puede reproducir estas características.

2.2.2. Reconocimiento de escritor

El objetivo del reconocimiento de escritor es averiguar o confirmar la identidad del autor de un determinado texto manuscrito valiéndose de un *software OCR* (o reconocimiento óptico de caracteres). Cada persona tiene una forma de escribir diferente, teniendo rasgos propios e inconfundibles para cada letra. Asimismo, cada persona tiene un grado de inclinación en la escritura y nivel de presión al escribir.

Uniendo todos estos datos, un *software* de reconocimiento de escritor puede ser capaz de detectar la persona que está escribiendo un texto manuscrito.

Pueden establecerse dos categorías de reconocimiento:

Los sistemas dinámicos ofrecen mejores tasas que los estáticos.

- **Estático:** en este modo, los usuarios escriben sobre papel; la imagen de la escritura así realizada se sube a un ordenador mediante un escáner o cámara de fotos para su posterior análisis. Esta modalidad también se conoce como *«off-line»*.
- **Dinámico:** en este modo, los usuarios escriben sobre una tableta digitalizadora, tablet, etc., que adquiere la escritura en tiempo real, simultáneamente durante su realización. Esta modalidad también recibe el nombre de *«on-line»*.

2.2.3. Reconocimiento de voz

Las aplicaciones de reconocimiento de voz usan sistemas de inteligencia artificial (en concreto redes neuronales) para aprender a identificar voces. Los algoritmos deben medir y estimar la similitud entre las muestras para devolver un resultado o una lista de posibles candidatos. La identificación se complica debido a factores como el ruido de fondo, por lo que siempre es necesario considerar un margen de error.

A pesar de que siguen existiendo dificultades para reconocer la forma natural de hablar de ciertos individuos, esta tecnología cuenta con la ventaja de que el dispositivo de adquisición es simplemente un micrófono por lo que no requiere de inversiones adicionales.

La utilización de este método está más extendida en sistemas de respuesta por voz y en centros de atención de llamadas telefónicas (call centers) que en el control de acceso físico a edificios o a redes y equipos informáticos.

2.2.4. Reconocimiento de escritura de teclado

Esta técnica se basa en el hecho de la existencia de un patrón de escritura en teclado que es permanente y propio de cada individuo. De este modo, se mide la fuerza de tecleo, la duración de la pulsación y el periodo de tiempo que pasa entre que se presiona una tecla y otra.

La principal ventaja de esta técnica es que la inversión necesaria en sensores es prácticamente nula, ya que los teclados de ordenador están presentes en múltiples aspectos de nuestra vida cotidiana y, además, están altamente aceptados por la población, que hace uso de ellos a diario. De este modo el coste de implantación se centraría en el software.

2.2.5. Reconocimiento de la forma de andar

Este método toma como referencia la forma de caminar de una persona. Este acto se graba y se somete a un proceso analítico que genera una plantilla biométrica única derivada de dicho comportamiento.

Esta tecnología está todavía en desarrollo y no ha alcanzado aún los niveles de rendimiento necesarios para ser implantada de manera similar al resto de tecnologías biométricas.

3 Usos y aplicaciones

Usada como forma única de autenticación o combinada con otras medidas (como tarjetas inteligentes, claves de cifrado o firmas digitales), la biometría está destinada a extenderse en muchos aspectos de nuestra vida diaria. En esta guía nos centraremos en aquellos aspectos relacionados con la ciberseguridad.

Los puntos fuertes de la biometría frente a otros mecanismos de autenticación son:

El contexto en el que se vaya a aplicar (colaborativo, a distancia, presencial, etc.) y la finalidad perseguida (control de accesos, control de presencia, control de identidad/personalidad, lucha contra el fraude, etc.) serán los elementos que determinen qué tecnología concreta es la más apropiada en cada caso.

3.1 Aplicaciones actuales de las tecnologías biométricas

En la actualidad las tecnologías biométricas se pueden utilizar en un amplio abanico de aplicaciones.

3.1.1. Control de accesos físicos y lógicos

Una de las aplicaciones en las que más extendido está el uso de la biometría es el control de accesos, ya sea éste físico (por ejemplo acceso a edificios o espacios restringidos) o lógico (acceso a sistemas, programas o equipos informáticos, móviles, tabletas).

Actualmente, la huella dactilar es la solución mayoritaria para este uso en España debido a su alto grado de madurez, que permite el establecimiento de precios competitivos, y a la usabilidad que ofrece.

No obstante, y aunque su presencia sea menor, el reconocimiento facial se presenta como alternativa a la huella dactilar en este tipo de aplicaciones.

En ocasiones, para el control de acceso a zonas de alta seguridad, se hace uso de una combinación de técnicas. Un ejemplo es el uso de una contraseña o tarjeta de identificación adicional a la huella dactilar, o la combinación de dos tecnologías biométricas, denominada biometría bimodal. Así, se pueden combinar dos factores de identificación: por un lado quién o cómo se es (biometría) y por otro lo que se sabe o se tiene (contraseñas y tarjetas, por ejemplo).

3 Usos y aplicaciones

Del mismo modo que se pueden instalar sensores en la entrada de edificios y salas de acceso restringido, cada vez más se integran sensores biométricos en los ordenadores corporativos de cara a gestionar la autenticación en sistemas y aplicaciones mediante tecnologías biométricas.

Biometría bimodal

combina factores de identificación de quién o cómo se es y de lo que se sabe o se tiene.

3.1.2. Control de presencia

Los métodos utilizados tradicionalmente para registrar a diario los horarios en los que los empleados acceden y abandonan sus respectivos puestos de trabajo suelen estar basados en el uso de un *PIN* o una tarjeta personal.

Uno de los principales inconvenientes que presentan estos métodos es la facilidad con la que se pueden cometer irregularidades, por ejemplo compartiendo con un compañero de trabajo el *PIN* o la tarjeta personal, ya que no se requiere ninguna verificación adicional.

El uso de cualquier técnica biométrica supone una forma eficaz de mitigar este riesgo por la imposibilidad de compartir los rasgos biométricos entre empleados.

Para este tipo de aplicaciones se utiliza habitualmente la huella dactilar, aunque también técnicas menos extendidas en el mercado como la geometría de la mano.

3.1.3. Lucha contra el fraude

El uso de estas tecnologías para realizar transacciones bancarias se encuentra bastante extendido, ya que se consideran más adecuadas que el uso de los métodos tradicionales al aportar mayores niveles de seguridad.

Sin embargo, su uso para la prevención de fraude no se limita a entidades privadas. Las Administraciones Públicas ya implantan sistemas biométricos para prevenir este delito, con el objetivo de evitar el gasto de fondos públicos de forma irregular.

3 Usos y aplicaciones

3.1.4. Otras aplicaciones

Existen otras aplicaciones de las tecnologías biométricas.

1. Call-centers

Las tecnologías biométricas se perfilan como las más idóneas en el ámbito de las potenciales tecnologías a aplicar en los centros de atención de llamadas. Un ejemplo es aquellos negocios que requieren la autenticación de usuarios por vía telefónica. Así, el uso del reconocimiento por voz, resulta en un aumento de la seguridad y la rentabilidad al mismo tiempo, ya que atestigua que el interlocutor realmente es el cliente que dice ser y elimina la necesidad de contar con personal que atienda la llamada.

2. Medio de pago

El uso de la biometría en terminales de punto de venta (TPV) ha reducido el tiempo empleado en transacciones y ha reducido las posibilidades de errores o confusiones. Como ejemplo, es posible implantar el uso de la huella dactilar para el pago (pre-asociado a una cuenta bancaria), eliminando problemas relacionados con la pérdida de tarjetas, olvido de números de identificación, transacciones manuales y cargos a cuentas erróneas.

3. Control de navegación

Se pueden usar controles mediante huella dactilar aplicados al acceso a redes sociales y a determinados sitios web, incluyendo las restricciones que la empresa haya determinado, por ejemplo, el filtrado de contenidos, la búsqueda de páginas o el uso ciertos servicios.

4. Vigilancia

Las técnicas biométricas son utilizadas como medida de vigilancia. Este caso de uso requiere de rasgos biométricos que puedan ser adquiridos a una distancia media. Las tecnologías más utilizadas son el reconocimiento facial y la forma de andar como rasgo biométrico.

3.2 Aplicaciones en combinación con otras tecnologías

También están comenzando a desarrollarse aplicaciones en combinación con otras tecnologías.

Combinación biometría con *NFC*

Con el objetivo de proteger determinadas aplicaciones, autenticarse, realizar pagos o para la gestión de contraseñas ya se utilizan técnicas biométricas en dispositivos móviles. Por ejemplo con la tecnología *NFC (Near Field Communication)* integrada en los *smartphones* se pueden realizar pagos y existen aplicaciones que combinan esta tecnología con la biometría para comprobar la identidad del usuario.

Otra aplicación que combina ambas tecnologías es en entornos hospitalarios para administrar medicamentos. Con *NFC,* en una pulsera o similar, se determina qué medicamentos administrar y con biometría se identifica al paciente para evitar errores.

Match on card

Es una combinación de la biometría y las tarjetas inteligentes para proporcionar una autenticación de doble factor (algo que tienes y algo que eres). En el chip de la tarjeta inteligente se almacena de forma segura el patrón biométrico (generalmente la huella dactilar) y también tiene lugar la comparación. El sistema de autenticación debe proporcionar el dispositivo de captura (lector de huella).

4 Soluciones biométricas en dispositivos móviles

Para evitar que los sistemas biométricos acepten muestras falsas, deben incluir sistemas de verificación de vida.

Los *smartphones* ofrecen cada vez más funcionalidades y nos sirven para acceder a un creciente número de servicios. Esto los convierte en una potencial fuente de amenazas. Como hemos visto los dispositivos biométricos ofrecen un excelente nivel de seguridad en el proceso de autenticación, muy superior a la ofrecida por los códigos *PIN (Personal Identification Number)* que se han venido utilizando tradicionalmente.

Gran número de *smartphones* ya incluyen dispositivos de autenticación biométricos. Y no solo incorporando sensores de huella dactilar sino otras tecnologías biométricas también, y no solo para desbloquear el dispositivo si no para otras tareas como aprobar pagos y como parte de servicios de autenticación multi-factor.

En cualquier caso, la adaptación de la mayor parte de las tecnologías biométricas a los dispositivos móviles es aún complicada y llena de dificultades. A continuación se describirán las principales tecnologías biométricas implantadas en dispositivos móviles.

El rendimiento de las tecnologías biométricas generalmente se mide usando tasas de error y tasas de acierto, sin embargo la mayor parte de estas tecnologías tienen una vulnerabilidad consistente en la aceptación de muestras biométricas falsas como fotografías, dedos de goma, etc. Se trata de una vulnerabilidad muy importante puesto que permiten una autenticación falsa. Estos problemas pueden ser resueltos incluyendo módulos de detección de vida en el proceso de verificación para asegurarse de que la muestra presentada pertenece a una persona viva y la detección de vida es diferente en cada tecnología biométrica.

4.1 Reconocimiento de huellas dactilares en móviles

Existen dos métodos diferentes de reconocimiento de huellas dactilares en móviles:

- Usando la **cámara del dispositivo** para capturar una imagen de la huella dactilar y compararla con la introducida en el momento de la configuración del servicio
- integración de un **sensor de contacto,** en el dispositivo para usar autenticarse de forma tradicional, es decir situando el dedo en el lector

Con el primer método no es necesario contacto del dedo con el dispositivo. Para el segundo, sí. El primer método es más barato que el segundo para el usuario final, ya que para el segundo, el precio del dispositivo se verá afectado por incluir un sensor biométrico, si bien el grado de error de éste método es inferior al primero.

La razón es que la calidad de la imagen capturada a través de la cámara del teléfono no es lo suficientemente buena como para asegurar un margen de error lo suficientemente bajo. Además el nivel de luminosidad, del contraste y la calidad de la imagen pueden ser muy variables, lo que dificulta aún más este método de autenticación biométrico.

En cualquier caso, una vez entrenado el usuario para que la calidad de la captura de la huella digital sea buena, el nivel de error se reduce bastante. Sin embargo un método de detección de huellas difícil de usar conllevará que caiga en desuso.

4 Soluciones biométricas en dispositivos móviles

El segundo método propuesto tampoco se libra de los problemas. Aunque más preciso que el uso de la cámara fotográfica del dispositivo, el sensor biométrico también se ve muy influenciado por condiciones tales como la temperatura o la humedad, los dedos muy grasos o sucios, el polvo, etc. Además el tiempo de vida del sensor es inversamente proporcional al número de usos que se le dé.

Los sensores biométricos incorporados en dispositivos móviles comerciales han resultado ser fácilmente engañables, ya que no reconocen que el dedo esté «vivo».

4.2 Reconocimiento de escritura

Para el desbloqueo de un dispositivo móvil, existen tres modelos de implementación de este reconocimiento.

1. El primero es la inserción de un **patrón de unión de puntos.** Este método de desbloqueo es bastante común en dispositivo móviles y desde el punto de vista biométrico, lo que mide aquí el dispositivo para desbloquearse no es sólo el conocimiento del patrón sino la velocidad y el ritmo en que se dibuja el patrón de puntos.

2. El segundo método consiste en la **escritura de una firma en la pantalla de desbloqueo**. Para ello es necesario que el dispositivo móvil disponga de un lápiz stylus, como viene en los dispositivos de gama alta.

3. El tercer modelo consiste en la **escritura mediante teclado virtual de un texto** (un código *PIN* largo) de manera que el dispositivo mida valores como el tiempo entre pulsaciones, el tiempo de pulsado, etc. Cada persona tiene una manera diferente de escribir en teclados virtuales y este es el método de identificación personal e intransferible.

Por supuesto este tipo de método de autenticación tiene algunas desventajas con respecto a otras técnicas biométricas, como una menor precisión, ya que los patrones de escritura pueden cambiar por una lesión, distracción o fatiga. La consecuencia es que este modelo biométrico debe ser re-entrenado periódicamente.

Los *smartphones* incorporan un buen número de sensores que permiten medir diferentes magnitudes como: la aceleración, los ángulos en que se encuentra el móvil, la presión, la proximidad, la localización, la orientación, etc. Por esta razón el reconocimiento de escritura debe ser combinado con otros métodos de reconocimiento biométrico como la manera en que el usuario coge el *smartphone*, la inclinación, los movimientos que hace el dispositivo al escribir el *PIN*, etc.

4 Soluciones biométricas en dispositivos móviles

4.3 Reconocimiento facial

Los dispositivos móviles de alta gama pueden ser entrenados para reconocer un rostro y desbloquearse cada vez que lo vean.

El *software* de reconocimiento facial ve el rostro como si fuera un mapa, anota puntos de referencia en la cara, como la distancia entre los ojos, el ancho de la nariz, la profundidad de la cuenca del ojo, la forma de los pómulos y el largo de la mandíbula. El móvil convierte estas medidas en un código numérico, igual que los escáneres de huellas dactilares. Este código numérico representa el «mapa» guardado de tu rostro, el cual usa el teléfono para comparar cuando intentes desbloquearlo.

Las técnicas de reconocimiento facial requieren una cierta cooperación por parte del usuario, ya que la cámara debe ser colocada justo en frente de la cara mientras se toma la foto.

Se trata de una técnica muy barata y está altamente aceptada por parte de los usuarios. Sin embargo el reconocimiento facial requiere un alto nivel de computación por parte del *Smartphone,* lo que puede, en ocasiones, ralentizar el dispositivo.

Además, estas técnicas son susceptibles a tres tipos de ataques:

- la foto del usuario legítimo, en vez de la propia persona
- el uso de una máscara con una fotografía del usuario legítimo
- la presentación de un video del usuario legítimo

Para solucionar estos posibles ataques, el software de reconocimiento facial utiliza técnicas dinámicas como:

Detección de parpadeo

Detección de movimiento de labios

4 Soluciones biométricas en dispositivos móviles

4.4 Reconocimiento de voz

El objetivo de esta técnica es que el *smartphone* sea capaz de determinar si la persona que ha pronunciado un determinado texto somos nosotros u otra persona, permitiendo así el desbloqueo del terminal.

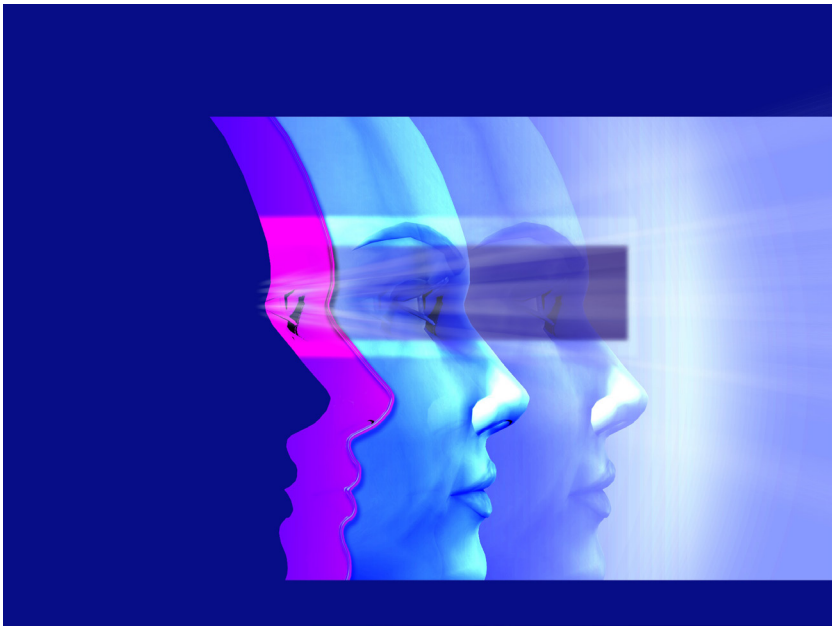
El proceso es algo más lento que la lectura de la huella dactilar y tiene el problema de que puede ser complicado desbloquear la pantalla si hay mucho ruido ambiente.

Además puede ralentizar el funcionamiento del dispositivo, ya que éste tiene que digitalizar lo que recibe por el micrófono y compararlo con la voz guardada durante el proceso de registro.

4.5 Otras técnicas

Existen muchas otras técnicas biométricas que están siendo investigadas para su implementación en dispositivos móviles:

- **Reconocimiento de manos.** Se trataría de realizar una foto a nuestra mano y que el dispositivo detectara que es nuestra mano antes de desbloquearse.
- **Reconocimiento de oreja.** Aquí se busca colocar el móvil en la oreja y por la forma de la misma cuando toca la pantalla, detectar que es la oreja del usuario legítimo.
- **Reconocimiento de iris.** El proceso consiste en fotografiar el ojo del usuario y mediante *software* hacer el reconocimiento de iris. El proceso es poco amigable para el usuario por lo que es difícil que este tipo de autenticación llegue a implantarse de forma masiva.



5 Soluciones biométricas en el catálogo de seguridad de INCIBE

INCIBE mantiene un catálogo de soluciones de ciberseguridad accesible a través de su portal web. Entre las soluciones de seguridad que se almacenan se incluyen soluciones biométricas de todo tipo.

El catálogo no incluye como tal una categoría de soluciones biométricas, pero se pueden encontrar soluciones biométricas en las categorías de:

- autenticación y certificación digital;
- contingencia y continuidad;
- control de contenidos confidenciales;
- gestión de control de acceso e identidad;
- seguridad en movilidad.

Dentro de este abanico de soluciones podemos encontrar plataformas de firma digital biométricas, dispositivos de almacenamiento que emplean tecnología biométricas, microcomputadores biométricos diseñados para la máxima seguridad en el trabajo diario, lectores biométricos de identidad y dispositivos biométricos de todo tipo (USB, teclados, etc).

Estas soluciones podrían permitir a la empresa, entre otras mejoras, un control biométrico de acceso a sus edificios, o el almacenamiento de datos seguro en dispositivos, de manera que sólo puedan ser leídos por las personas adecuadas, evitando así el peligro de fuga de información por pérdidas de dichos dispositivos de almacenamiento.

6 Beneficios del uso de tecnologías biométricas en la empresa

La implantación de tecnologías biométricas conlleva un conjunto de ventajas tanto para entidades públicas y privadas como para los usuarios finales.

Aunque las medidas biométricas están relacionadas con la ciberseguridad, gran parte de sus beneficios afectan a la vida diaria de usuarios y empleados:

- reducción de costes de mantenimiento de los sistemas de autenticación
- aumento de la eficiencia
- control horario
- mejora de la imagen corporativa...

Sin embargo desde el punto de la ciberseguridad las medidas biométricas también aportan gran cantidad de beneficios:

6.1 Para las organizaciones y usuarios finales

Las organizaciones deben ser el principal motor que promueva e invierta en el desarrollo de las tecnologías biométricas. Para que esto ocurra, los beneficios potenciales a obtener con su implantación han de ser claros y relevantes. A continuación se describen los más destacados.

6.1.1. Aumento de la seguridad en el control de accesos

Sin duda, una de las ventajas más importantes para las empresas de la utilización de técnicas biométricas es para la autenticación de empleados, garantizando así que la persona es quien dice ser, es decir, que los rasgos biométricos se encuentran exclusivamente ligados a su legítimo usuario.

Mediante el robo de credenciales o tarjetas identificativas, un individuo puede acceder a zonas restringidas o realizar operaciones no permitidas, inculpando a terceros. Asimismo, es posible que estas credenciales se compartan voluntariamente entre empleados.

A través de la implementación de sistemas biométricos, se aumenta la seguridad reduciendo la probabilidad de que alguien no autorizado acceda a zonas o a aplicaciones restringidas.

6.1.2. Mejora de imagen corporativa

La implantación de tecnologías biométricas contribuye a que una empresa sea más eficiente, más segura y reduzca el fraude interno. Es por ello que, sumado a todas las ventajas descritas anteriormente, se produce una importante mejora en la opinión general sobre la compañía. Así mismo, se asociaría la entidad con la innovación, la inversión en investigación y desarrollo y la apuesta por tecnología puntera.

6.1.3. Posibilidad de tramitaciones remotas

Es posible emplear técnicas biométricas como forma de verificación en operaciones no presenciales de forma altamente fiable, pudiendo superar a las firmas electrónicas actuales. De esta forma se pueden reducir los traslados y trámites innecesarios e inconvenientes para el usuario final.

6 Beneficios del uso de tecnologías biométricas en la empresa

6.1.4. Aumento de la privacidad

Utilizando técnicas biométricas se incrementa la seguridad de la transmisión de los datos de carácter personal de los clientes al cifrarlos utilizando una clave única y personal del propio cliente.

Es la consecuencia de la notable dificultad que supone la falsificación de rasgos biométricos con el objetivo de acceder a la información personal de un usuario final o cliente.

6.2 Comparativa con otros sistemas de autenticación e identificación automática

Las tecnologías biométricas surgen como alternativa o complemento a las técnicas de identificación y autenticación existentes. Por ello es posible establecer una comparación directa entre ambas, destacando beneficios que resultan del uso de biometría junto con aspectos en los que las técnicas tradicionales son superiores.

Se han de considerar los siguientes aspectos:

1. **Necesidad de secreto:** las contraseñas han de ocultarse y las tarjetas no deben de estar al alcance de terceros, mientras que la biometría no requiere de estas medidas de protección que son exclusivamente dependientes del usuario.

2. **Posibilidad de robo:** las tarjetas y contraseñas pueden ser robadas. Sin embargo, robar un rasgo biométrico es extremadamente complejo.

3. **Posibilidad de pérdida:** las contraseñas son fácilmente olvidables y las tarjetas se pueden perder. Los rasgos biométricos permanecen invariables salvo en contadas excepciones y siempre están con el sujeto a quien identifican.

4. **Registro inicial y posibilidad de regeneración:** la facilidad con la que se puede enviar una contraseña o tarjeta nueva contrasta con la complejidad que supone el registro en un sistema biométrico, ya que requiere de la presencia física del individuo en esta fase. Hay que añadir que los rasgos biométricos son por definición limitados, mientras que la generación de contraseñas es ilimitada, lo cual es una ventaja.

5. **Proceso de comparación:** la comparación de dos contraseñas es un proceso sencillo. Sin embargo, comparar dos rasgos biométricos requiere de mayor capacidad computacional.

6. **Comodidad del usuario:** el usuario ha de memorizar una o múltiples contraseñas y, en el caso de que use una tarjeta, ha de llevarse siempre consigo. Utilizando tecnología biométrica no se necesita realizar estos esfuerzos.

6 Beneficios del uso de tecnologías biométricas en la empresa

7. Vulnerabilidad ante el espionaje: una discreta vigilancia de nuestra actividad podría servir para obtener nuestra contraseña o robar nuestra tarjeta. Ese método no es válido ante los sistemas biométricos.

8. Vulnerabilidad a un ataque por fuerza bruta: las contraseñas tienen una longitud de varios caracteres. Por su parte, una muestra biométrica emplea cientos de bytes, lo que complica mucho los ataques por fuerza bruta.

9. Medidas de prevención: los ataques contra sistemas protegidos por contraseña o tarjeta se producen desde hace años, y las medidas de prevención contra ellos ya se encuentran maduras. Por el contrario, los ataques a los sistemas biométricos son un área en la que estas medidas de prevención se están generando en estos momentos.

10. Autenticación de usuarios «reales»: la autenticación de usuarios mediante contraseña o tarjeta y su efectividad, dependen absolutamente de la voluntad del usuario a la hora de hacerlas personales e intransferibles. La biometría está altamente relacionada con el propio usuario pues no puede ser prestada ni compartida.

11. Coste de implantación: en el momento de la implantación, el hecho de instaurar un sistema de contraseñas tiene un coste bajo, mientras que en el caso de un sistema basado en muestras biométricas es más costoso.

12. Coste de mantenimiento: el coste de mantenimiento de un sistema biométrico, una vez está implantado con éxito, es menor al de un sistema de contraseña o tarjeta ya que no conlleva gastos de gestión asociados a la pérdida u olvido de credenciales.

6 Beneficios del uso de tecnologías biométricas en la empresa

La siguiente tabla identifica los aspectos en los que destaca cada método de autenticación:

Aspecto	Biometría	Contraseñas/ tarjetas
Necesidad de secreto	✔	
Posibilidad de robo (baja)	✔	
Posibilidad de pérdida (baja)	✔	
Registro inicial y posibilidad de regeneración		✔
Proceso de comparación (fácil)		✔
Comodidad del usuario	✔	
Vulnerabilidad ante el espionaje (baja)	✔	
Vulnerabilidad a un ataque por fuerza bruta (baja)	✔	
Medidas de prevención		✔
Autentificación de usuarios "reales"	✔	
Coste de implantación (bajo)		✔
Coste de mantenimiento (bajo)	✔	

Tabla 1: comparativa de sistemas de autentificación

Ante las diferencias de ambos métodos, hay que resaltar el hecho de que se complementan de forma óptima, especialmente en entornos de máxima seguridad donde la autenticación sea un proceso crítico. De este modo, su uso combinado mejora notablemente la seguridad.

7 Gestión de riesgos en biometría

La implantación y el empleo de tecnologías biométricas están expuestos a una serie de riesgos, algunos específicos y otros compartidos con las demás tecnologías y técnicas de identificación. En este capítulo se identifican las amenazas y vulnerabilidades que pueden comprometer la seguridad o la confianza en los sistemas biométricos.

Además algunos sistemas biométricos cuentan con ciertas limitaciones, tales como no ser capaces de satisfacer las cada vez mayores demandas de carga de trabajo o contar con dificultades de interoperabilidad entre sistemas. Estas carencias demuestran la necesidad de un mayor desarrollo y la aplicación de medidas de seguridad.

7.1 Consideraciones a tener en cuenta ante la implantación de medidas biométricas

Las tecnologías biométricas, como el resto de tecnologías, están expuestas a una serie de amenazas. Estas pueden ser exclusivas o compartidas con otras tecnologías de autenticación. Las más relevantes se desarrollan a continuación.

7.1.1. Pérdida o robo de información biométrica

A diferencia de las contraseñas o las tarjetas personales, los rasgos biométricos son invariables (como regla general), por lo que su número es limitado a lo largo del tiempo, sin posibilidad de renovación y, en consecuencia, su confidencialidad es esencial.

El robo de información es especialmente sensible en el caso de la biometría al tratarse de información exclusiva y extremadamente ligada al individuo, por lo que el robo de la misma supone un incidente de seguridad grave.

7.1.2. Suplantación de identidad

Se trata del uso de información biométrica robada o falsificada con el propósito de acceder a espacios o aplicaciones restringidas, falsificar el control de presencia, enmascarar o suplantar una personalidad, etc. Es de especial gravedad cuando se utiliza para cometer un crimen ya que su repudio resulta complicado.

7.1.3. Sabotaje

Pueden darse ataques al sensor de forma consciente para tratar de impedir su funcionamiento. Frecuentemente, la causa de estos ataques es una expresión del desacuerdo o descontento con la implantación de biometría precisamente debido a la alta fiabilidad que ofrece el sistema a la hora evitar conductas fraudulentas y accesos no autorizados.

7.1.4. Incumplimiento de la normativa de protección de datos personales

Los rasgos biométricos se consideran datos de carácter personal a todos los efectos legales por lo que su tratamiento se encuentra sometido al cumplimiento de las distintas exigencias de carácter jurídico, técnico, físico y organizativo previstas, principalmente por la Ley de Protección de Datos de Carácter Personal (LOPD) [2] y por su normativa de desarrollo (RDLOPD) [3].

Los datos biométricos se han considerado, con carácter general, como “de nivel básico”, siendo equiparables a una simple dirección o un número de teléfono, pero siempre es aconsejable tratar estos datos con la máxima cautela y protección posible, ya que en muchos casos el usuario final los percibe como de una alta sensibilidad, precisamente por tratarse de rasgos intrínsecamente ligados a su persona.

7 Gestión de riesgos en biometría

La LOPD establece una serie de obligaciones y principios de obligado cumplimiento para todas aquellas entidades o empresas, tanto del sector público como privado, que traten datos de carácter personal para el desarrollo de su actividad. Un tratamiento inadecuado puede derivar en riesgos para la privacidad de los datos personales almacenados además de los derivados de la infracción e incumplimiento de la normativa vigente.

7.1.5. Idoneidad de la implantación

Existe el riesgo de creer erróneamente que un sistema biométrico garantiza la seguridad total y que es la solución a cualquier problema de seguridad. La implantación de tecnologías biométricas supone un alto coste económico y una implicación de personal específicamente dedicado a ello durante la fase inicial. Por esta razón es necesario realizar un análisis previo para evaluar la verdadera necesidad, escenario adecuado de implantación y el beneficio logrado frente al coste incurrido, ya que es posible que ésta no sea la solución más adecuada para todos los casos.

7.1.6. Calidad de la tecnología

Si la calidad de la tecnología implantada no alcanza los niveles recomendables, podría acarrear graves brechas de seguridad así como un deterioro notable de la percepción de las tecnologías debido a su mal funcionamiento. Los elementos que se deben tener en cuenta al respecto son: la calidad del sensor, la eficiencia del algoritmo de comparación, la encriptación del almacenamiento de muestras obtenidas y la interoperabilidad con otros sistemas.

7.1.7. Incidencias con el sistema

Como todo sistema electrónico/informático, los sistemas de autenticación biométricos son susceptibles de fallos eléctricos, caída de las líneas de comunicación, del propio sistema o de los sistemas de soporte (por ejemplo suministro eléctrico o sistema de comunicaciones), ataques informáticos, etc. Estos problemas afectan de forma similar que al resto de tecnologías.

7.1.8. Indisponibilidad de sensor

Si el acceso o la autenticación se realizan exclusivamente mediante biometría, es decir, no existe un método alternativo como puede ser el uso de contraseñas o tarjetas personales, el fallo o ausencia del dispositivo de adquisición de muestras supone la imposibilidad de autenticación o acceso. Un ejemplo de esta situación es un empleado que tenga que acceder de forma urgente al correo electrónico desde fuera de la oficina mediante huella dactilar pero no disponga de sensor en su ordenador.

7.1.9. Variación involuntaria en los rasgos biométricos

Los cambios en los rasgos biométricos, como variaciones de la voz, vello facial o el peinado también suceden de forma natural. En estos casos, el usuario no tiene intención de engañar al sistema. No obstante, estos cambios pueden dificultar el proceso de identificación y generar, incluso, una percepción negativa para el usuario.

7.1.10. Experiencia de uso negativa (usabilidad)

Un mal uso involuntario del sensor realizado por una persona sin los conocimientos adecuados puede tener como consecuencia la desconfianza del usuario en la tecnología y el aumento de la tasa de error de la misma.

7.1.11. Falta de aceptación cultural

Esta amenaza aparece en determinados grupos demográficos cuyas normas sociales o religiosas no favorecen la toma de muestras en determinadas técnicas. Por ejemplo, en algunas culturas el reconocimiento facial no es válido ya que no todos los ciudadanos llevan el rostro al descubierto; en otras la lectura de la huella dactilar se considera una práctica antihigiénica, etc.

7.2 Vulnerabilidades

A continuación se listan algunas vulnerabilidades que afectan negativamente tanto a la implantación y operación de sistemas de reconocimiento biométrico como a su propio rendimiento. Estas vulnerabilidades se dividen según sean comunes a todas las técnicas biométricas o específicas de alguna de ellas.

Tecnología biométrica	Vulnerabilidades
Vulnerabilidades comunes a todas las tecnologías biométricas	■ calidad baja de los dispositivos de captura ■ ubicación inadecuada del dispositivo de captura ■ desconocimiento de la calidad o del abanico de productos y utilidades disponibles ■ falta de conocimientos técnicos del personal ■ falta de recursos (tanto de personal como económicos) ■ escasa concienciación en materia de seguridad ■ percepción de ausencia de privacidad por parte de los usuarios
Huella dactilar	■ condición del dedo en el momento de tomar la muestra: mojado, seco, manchado... ■ condiciones climatológicas que afectan al lector: humedad, temperatura, etc. ■ condiciones de la huella: cortes, heridas o inflamaciones ■ actividad laboral: trabajos que puedan afectar a la huella, por ejemplo el uso habitual de productos químicos que puedan deteriorarla

Tabla 2: Vulnerabilidades de las tecnologías biométricas

7 Gestión de riesgos en biometría

Tecnología biométrica	Vulnerabilidades
Reconocimiento de voz	■ enfermedades de la voz: bronquitis, faringitis, gripe, laringitis, afonías, etc. ■ variación entre el dispositivo de registro y el usado en la captura de muestras ■ variación entre entornos de registro y captura de muestras (por ejemplo: interior y exterior) ■ volumen del habla
Reconocimiento facial	■ variación en el aspecto facial: peinado, vello, gafas, sombrero, etc. ■ condiciones de luminosidad ■ variación en el peso ■ uso de vestimenta que puede dificultar la localización o visión de la cara (pañuelos, bufandas, etc.)
Escáner de iris y retina	■ excesivo movimiento ocular o de la cabeza ■ enfermedades oculares ■ uso de gafas ■ problemas debidos al uso de lentes de contacto (iris)
Geometría de la mano	■ uso de joyería, bisutería o abalorios ■ uso de vendajes o guantes ■ condiciones de la mano: inflamaciones en las articulaciones, heridas, etc.
Escáner de firma	■ velocidad de la firma: excesivamente rápida o lenta ■ diferente postura del sujeto durante la firma: sentado o de pie ■ firma no consistente: el sujeto varía su firma

Tabla 2: Vulnerabilidades de las tecnologías biométricas

8 Buenas prácticas en el empleo de sistemas biométricos

Con el objetivo de reducir los riesgos asociados al empleo de biometría y hacer una adecuada gestión de los mismos, han de aplicarse una serie de controles mitigantes y buenas prácticas de seguridad.

8.1 Reforzar la seguridad del sistema

La seguridad es fundamental en todos los elementos de un sistema biométrico. Es por ello que se debe garantizar la privacidad y evitar accesos no autorizados a la base de datos en que se guardan los registros biométricos.

8.2 Almacenamiento de muestras

En el proceso de registro previo al uso de tecnologías biométricas han de almacenarse las muestras aportadas por los usuarios. Así, existe la posibilidad de almacenar una parte de la muestra o multitud de referencias en lugar de la muestra íntegra. Esto se hace para prevenir su utilización fraudulenta en caso de pérdida o robo. Un ejemplo es el almacenamiento de minucias de huellas dactilares, en lugar de la huella completa. De esta forma resulta imposible la recreación de la huella a partir de una minucia, en caso de que esta sea robada.

8.3 Autenticación de doble factor

Con el objetivo de evitar el fraude se recomienda el uso de dos factores en el proceso de autenticación. Para ello se puede utilizar biometría bimodal (dos técnicas biométricas diferentes, por ejemplo huella dactilar e iris) o combinar la biometría con el uso de contraseña y/o tarjetas de identificación.

8.4 Realizar una buena adaptación

No todas las empresas son iguales, por ello la adaptación a las circunstancias de cada caso es esencial para evitar futuros problemas. Por ejemplo, si una empresa va a incorporar un control de accesos en base a la huella dactilar y cuenta con empleados que realizan trabajos manuales o utilizan productos abrasivos, puede ser aconsejable registrar las huellas de la mano que menos utilicen (izquierda en el caso de los diestros y derecha en el caso de los zurdos) y de los dedos que menos se utilicen (generalmente anular y meñique). Con esta simple adaptación, se podrán evitar en buena medida futuros problemas relacionados con cortes o deterioros en la huella.

8.5 Adquisición de tecnología de calidad

La obtención de muestras adecuadas y la realización de comparativas fiables es importante para evitar falsos positivos, falsos negativos y altas tasas de error, y esto depende en gran medida de la calidad y fiabilidad de los sistemas utilizados. Una elección adecuada previene el fraude y la reticencia de los usuarios.

8 Buenas prácticas en el empleo de los sistemas biométricos

8.6 Formación de los usuarios

Un factor clave en el éxito de las tecnologías biométricas es que sus usuarios las utilicen correctamente. Para la consecución de este objetivo se puede ofrecer una fase inicial de formación que, por norma general, no será excesivamente larga y en la que se informe de lo que son las tecnologías biométricas y se aporten unas breves instrucciones y recomendaciones sobre su uso. En este sentido, los acuerdos con los representantes de los trabajadores previos a la implantación de las tecnologías favorecen este proceso.

8.7 Cumplimiento normativo

A la hora de implantar este tipo de tecnologías biométricas aplicadas a la seguridad, resulta de vital importancia el evaluar previamente las ventajas e inconvenientes posibles que, desde un punto de vista jurídico, puede suponer la implantación de dicho sistema en relación con la vida privada de las personas afectadas, así como tener en cuenta posibles sistemas o soluciones alternativas que puedan suponer una menor intrusión contra los derechos de los interesados.

A este respecto, destacar que en todo caso los datos biométricos que, en su caso, pudiesen ser sometidos a tratamiento a través de dichos sistemas deberían ser siempre adecuados, pertinentes y no excesivos en comparación con la finalidad del proceso (por ejemplo: control horario, control de accesos, control de presencia, etc.).

9 Referencias

1. Cuerpo Nacional de Policía, Sistema Automático de Identificación Dactilar – SAID
http://www.policia.es/org_central/cientifica/servicios/id_identificacion.html

2. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, LOPD
https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

3. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal RLOPD
https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

4. Agencia española de protección de datos, AGPD,
http://www.agpd.es/

5. CERTSI, Blog, «La problemática de la biometría como medio de autenticación»
https://www.certsi.es/blog/problematica-biometria-autenticacion

6. CERTSI, Blog, «Patrones biométricos y autenticación dinámica»
https://www.certsi.es/blog/autenticacion-dinamica

7. Modi, Shimon K., Artech House, 2011
«Biometrics in Identity Management: Concepts to Applications»

8. Janin, A.K, et al, Springer, 2011,
«Introducction to biometrics»

9. A. K. Jain, R. Bolle and S. Pankanti (eds.),
«Biometrics: Personal Identification in a Networked Society»
Kluwer Academic Press, 1999.

10. M. Tapiador y J. A. Sigüenza (coord.)
«Técnicas biométricas aplicadas a la Seguridad»
Ra-Ma, 2005.

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL