GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Guía sobre las tecnologías biométricas aplicadas a la seguridad

Con el patrocinio de:

Deloitte.

OBSERVATORIO DE LA **SEGURIDAD** DE LA **INFORMACIÓN**

Edición: Octubre 2011

La "Guía sobre las tecnologías biométricas aplicadas a la seguridad" ha sido elaborada por el Instituto Nacional de Tecnologías de la Comunicación (INTECO), a través de su Observatorio de la Seguridad de la Información:

Pablo Pérez San-José (dirección)

Eduardo Álvarez Alonso (coordinación)

Susana de la Fuente Rodríguez

Laura García Pérez

Cristina Gutiérrez Borge

El **Instituto Nacional de Tecnologías de la Comunicación (INTECO)**, sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología. La misión de INTECO es aportar valor e innovación a los ciudadanos, a las pymes, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional. Para ello, INTECO desarrollará actuaciones en las siguientes líneas: Seguridad, Accesibilidad, Calidad TIC y Formación.

El **Observatorio de la Seguridad de la Información** (**http://observatorio.inteco.es**) se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica, siendo un referente nacional e internacional al servicio de los ciudadanos, empresas, y administraciones españolas para describir, analizar, asesorar y difundir la cultura de la seguridad y la confianza de la Sociedad de la Información.

Deloitte (http://www.deloitte.es) presta servicios de auditoría, asesoramiento fiscal y legal, consultoría y asesoramiento en transacciones corporativas a entidades que operan en un elevado número de sectores de actividad. La firma aporta su experiencia y alto nivel profesional ayudando a sus clientes a alcanzar sus objetivos empresariales en cualquier lugar del mundo. Para ello cuenta con el apoyo de una red global de firmas miembro presentes en más de 140 países y con más de 170.000 profesionales que han asumido el compromiso de ser modelo de excelencia.

Deloitte cuenta con un grupo encargado de realizar servicios correspondientes a la gestión del riesgo informático que se denomina *Enterprise Risk Services* (ERS). Este grupo está formado por más de 200 profesionales, 8 socios en España y varios miles de especialistas a nivel mundial, dedicados exclusivamente a servicios de auditoría informática, seguridad informática, identificación y gestión de los riesgos de las operaciones asociados a los sistemas de información, así como a servicios enfocados a mantener el nivel de control interno requerido en la utilización de la tecnología.

Índice

1. ¿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 – y especialmente aquellas relacionadas con la seguridad – algunas de las cuales se expondrán a lo largo de la presente Guía.

Los primeros antecedentes de los que se tiene referencia sobre la biometría datan de hace más de mil años en China, donde los alfareros comenzaron a incluir sus huellas dactilares en los productos que realizaban como símbolo de distinción o firma, lo que les permitía diferenciarse del resto.

Sin embargo, no fue hasta finales del siglo XIX cuando Alphonse Bertillon - antropólogo francés que trabajó para la policía - comenzó a dar a la biometría el carácter de ciencia, profesionalizando su práctica. Basaba su teoría en que una cierta combinación de medidas del cuerpo humano era invariable en el tiempo, lo que permitió dar solución al problema de identificar a los criminales convictos a lo largo de toda su vida.

1. Taille. — 2. Envergure. — 3. Buste. — 4. Longueur de la tête. — 5. Largeur de la tête. — 6. Oreille droite. — 7. Pied gauche. — 8. Médius gauche. — 9. Coudée gauche.

El sistema de Bertillon o *"Antropometría"*, que incluía, entre otras, medidas como el largo y ancho de la cabeza o la longitud del pie izquierdo y del antebrazo, se comenzó a utilizar comúnmente a lo largo de todo el mundo. Sin embargo, su efectividad se puso en duda al presentarse algunos problemas en el uso de diferentes medidas y, especialmente, por las dificultades en la diferenciación de sujetos extremadamente similares como los gemelos.

Esta desacreditación hizo que Sir Edward Henry, Inspector General de la Policía de Bengala, buscase otras técnicas y se interesase por las investigaciones de Sir Francis Galton, el cual utilizaba la huella dactilar como método de identificación. Primero en Bengala y posteriormente en Londres (1901), Sir Edward Henry estableció su oficina de huella dactilar exitosamente y consiguió rápidamente la aceptación de la comunidad a nivel mundial. Así, los métodos utilizados en oriente desde siglos atrás fueron introducidos exitosamente en occidente.

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, detectándose multitud de rasgos biométricos diferentes a 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 las técnicas de identificación y seguridad en el futuro.

Esta Guía tiene como objetivo, de 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. De otro lado, tiene como finalidad no sólo **dar a conocer** estos métodos de identificación para **generar confianza** entre sus usuarios potenciales, 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.

2. Características y tipología de las tecnologías biométricas

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.

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:

- Captura: Se capturan los parámetros biométricos.
- Procesamiento: Se crea una plantilla con las características personales de los parámetros capturados.
- Inscripción: La plantilla procesada se guarda 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.

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 por parte 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.

- 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.

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.

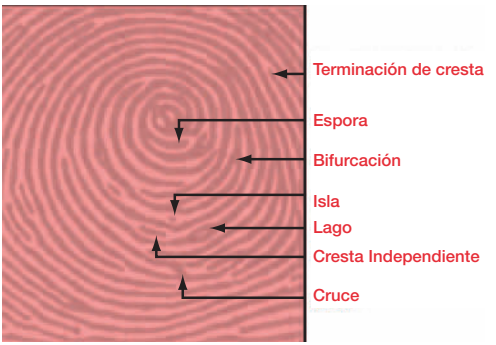
Huella dactilar

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 la mayoría de la población tiene huellas dactilares únicas e inalterables.

Es el rasgo biométrico más utilizado para autenticación y tiene la mayor gama de tecnologías de captura, con distintas características de funcionamiento. Asimismo, tiene como ventajas su alta tasa de precisión y que habitualmente los usuarios tienen conocimientos suficientes sobre su utilización.

Existen dos tipos de técnicas de búsqueda de coincidencias entre muestras 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.

El pequeño tamaño de los receptores, 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.

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.

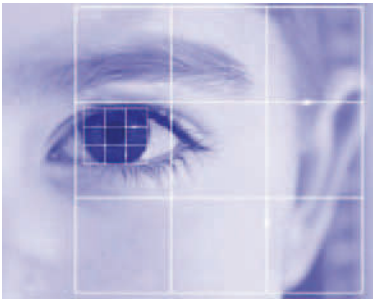
Entre los aspectos clave empleados para la comparación se encuentran mediciones como la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula.

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

Uno de los principales inconvenientes que presenta esta técnica es la escasa resistencia al fraude, pues una 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.

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.

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.

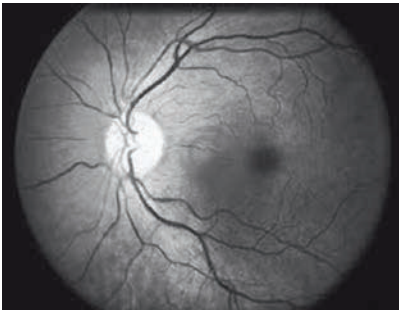
Las características extraídas incluyen las curvas de los dedos, su grosor y longitud, la altura y la anchura del dorso de la mano, las distancias entre las articulaciones y la estructura ósea en general. No se tienen en cuenta detalles superficiales, tales como huellas dactilares, líneas, cicatrices 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.

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.

Otras formas de biometría fisiológica

Existen además otras técnicas que analizan:

- Líneas de la palma de la mano
- Estructura de las venas de los dedos o las muñecas
- Forma de las orejas
- Piel, textura de la superficie dérmica
- ADN, patrones personales en el genoma humano

Estas técnicas son todavía extremadamente novedosas y su uso se reduce prácticamente en exclusividad al ámbito forense o de investigación. Esta falta de madurez hace que su implantación presente 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.

A pesar de estas limitaciones, se puede destacar, como ejemplo de caso de éxito en la implantación de estas técnicas más novedosas, la adopción del análisis de la estructura de las venas de las manos por parte de algunas entidades bancarias en Japón y República Checa para la identificación de sus clientes con escáneres integrados en cajeros automáticos.

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 realizada por una persona. Por tanto, incluyen la variable tiempo, ya que toda acción tiene un comienzo, un desarrollo y un final.

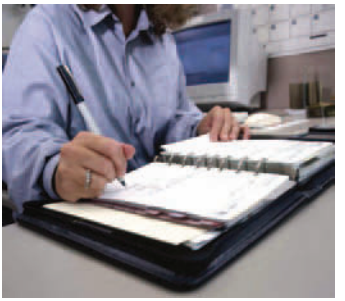
Reconocimiento de firma

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.

Reconocimiento de voz

Las aplicaciones de reconocimiento de voz usan redes neuronales para aprender a identificar voces. Los algoritmos deben medir y estimar la similitud 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 (integrados desde hace años en teléfonos y ordenadores personales) 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.

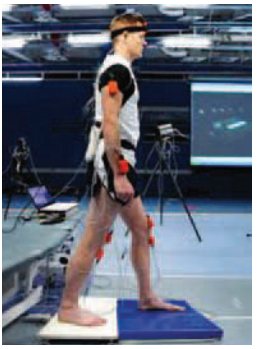
Reconocimiento de escritura de teclado

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 los costos de implantación se centrarían en el software.

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 encriptación o firmas digitales), la biometría está destinada a extenderse en muchos aspectos de nuestra vida diaria.

Las principales características de la biometría, que la distinguen de otros sistemas de autenticación –pudiéndose definir como sus puntos fuertes – son: i) puede asociarse a un individuo en concreto (por el contrario una contraseña podría ser usada por otra persona que no sea el usuario autorizado); ii) su comodidad, ya que no es necesario tener o recordar algo; iii) es altamente resistente al fraude.

Las tecnologías biométricas que se han descrito en el capítulo anterior son utilizadas en diversos entornos y con diferentes finalidades.

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. Adicionalmente, existen líneas de investigación de cara a futuros usos que parecen especialmente prometedoras.

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).

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 de iris y el reconocimiento facial se presentan como alternativas 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).

Del mismo modo que se han instalado 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.

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.

Control de fronteras

La biometría puede ser utilizada para verificar identidades por parte de agentes fronterizos mediante el uso de dispositivos de lectura biométrica y contrastando esta información con sus bases de datos.

Los rasgos a analizar normalmente son la topografía facial y las huellas dactilares. Actualmente un gran número de administraciones públicas de todo el mundo está implantando la biometría en aduanas y aeropuertos para aumentar la seguridad y agilidad de los mismos.

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 están comenzando a implantar

sistemas biométricos para prevenir este delito, con el objetivo de evitar el gasto de fondos públicos de forma irregular. Un ejemplo concreto de ello es su uso en la gestión de los servicios sanitarios gubernamentales ofrecidos a domicilio en Estados Unidos. En este caso, se verifica biométricamente que el personal sanitario se ha presentado en las viviendas adecuadas y han ofrecido los servicios facturados.

Investigación de delitos

En ocasiones, las huellas recogidas de la escena de un delito, son posteriormente cotejadas a través del programa AFIS (*Automated Fingerprint Identification System*) o algún otro programa derivado del mismo.

Concretamente en España, se utiliza el sistema SAID (Sistema Automático de Identificación Dactilar), en el que se mantiene un registro de las huellas de individuos con antecedentes. No obstante, esta base de datos es totalmente independiente de la que almacena las huellas dactilares registradas en el proceso de obtención del Documento Nacional de Identidad, por lo que las Fuerzas de Seguridad solamente pueden utilizar en estos casos las huellas tomadas en escenarios de algún crimen o de personas con antecedentes.

Las huellas dactilares electrónicas se remiten, junto con los datos demográficos para identificar o verificar la identidad de la persona. Las búsquedas pueden tardar minutos, horas o días, dependiendo de la calidad de la información presentada y el tamaño de la base de datos en que se busca.

Este sistema procesa una o varias huellas dactilares desconocidas, buscando coincidencias automáticamente en una base de datos donde previamente se han almacenado todas las huellas sospechosas.

Otras Aplicaciones

Existen aplicaciones para tecnologías biométricas muy variadas y correspondientes a categorías diferentes de las ya mencionadas.

a) 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 su uso en la banca telefónica, que en los últimos años está creciendo en el mercado. Considerando que para realizar cualquier operación previamente se debe verificar la identidad de cada cliente en cada llamada, 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.

b) 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, hay colegios que ya utilizan la huella dactilar para el pago del menú en el comedor, eliminando problemas relacionados con la pérdida de tarjetas, olvido de números de identificación, transacciones manuales y cargos a cuentas erróneas.

c) Control parental

Hoy en día se pueden usar controles parentales mediante huella dactilar aplicados al acceso a redes sociales y a determinados sitios web, incluyendo las restricciones que los padres hayan determinado, por ejemplo, el filtrado de contenidos, la búsqueda de páginas o el uso ciertos servicios o a partir de ciertas horas.

d) Vigilancia

Las técnicas biométricas son utilizadas como medida de vigilancia para identificar criminales y sospechosos entre multitudes. Este caso

de uso requiere de rasgos biométricos que puedan ser adquiridos a una distancia media. La tecnología más utilizada es el reconocimiento facial, pero se están empezando a desarrollar sistemas que utilizan la forma de andar como rasgo biométrico.

e) Transacciones mediante dispositivos móviles

En la actualidad las técnicas biométricas se están comenzando a emplear en dispositivos móviles con el objetivo de proteger determinadas aplicaciones, realizar pagos o para la gestión de contraseñas. En este sentido cabe destacar la tecnología NFC (*Near Field Communication*) integrada en los *smartphones* de última generación y utilizada en combinación con biometría para la realización de pagos. Se prevé que esta será una de las principales líneas de investigación futura debido a su gran potencial.

4. Beneficios del uso de tecnologías biométricas

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

4.1. PARA LAS ENTIDADES USUARIAS

Las organizaciones deben suponer 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.

Aumento de la seguridad

Sin duda, una de las ventajas más importantes de la utilización de técnicas biométricas para la autenticación de usuarios es que garantizan 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 ajenas, 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.

Tanto el robo como la utilización por parte de varios usuarios de las mismas credenciales, suponen una grave brecha en la seguridad en las entidades que puede ser evitada. 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.

Reducción de costes de mantenimiento

Si bien las técnicas tradicionales – como el uso de contraseñas o tarjetas de identificación – requieren una inversión muy baja en su implantación, no obstante, conllevan costes elevados asociados a su gestión diaria. Esta es la consecuencia de uno de los riesgos más evidentes asociados a este tipo de métodos de autenticación: la posibilidad de que las credenciales sean perdidas, robadas u olvidadas.

Sin embargo, en el caso de las tecnologías biométricas – donde la inversión inicial puede llegar a ser elevada en el caso de que sea necesario comprar dispositivos o software de adquisición y procesamiento de muestras – una vez la tecnología está en funcionamiento y sus usuarios acostumbrados a usarla, el coste de mantenimiento es muy reducido, ya que no se dan los riesgos anteriormente referidos.

Este beneficio es más notable en las tecnologías cuyo coste de implantación no es muy alto, como la huella dactilar, el reconocimiento de voz, el reconocimiento facial o el reconocimiento de escritura de teclado.

Aumento de la eficiencia

La realización de los diferentes procesos de autenticación, control de accesos e identificación mediante técnicas no biométricas supone, en ocasiones, una inversión excesiva de tiempo. A veces, aunque el proceso dure pocos segundos, si es realizado por un gran número de usuarios en un corto período de tiempo, puede resultar altamente ineficiente. Esto sucede, por ejemplo, en los accesos a grandes edificios de oficinas o en el control fronterizo de un aeropuerto en horas de máxima afluencia.

Mediante la elección de la tecnología biométrica más adecuada para los diferentes casos y la necesaria formación de los usuarios (unas nociones básicas de utilización) se puede aumentar considerablemente la eficiencia de los procesos con el consiguiente beneficio económico resultante para la entidad.

Reducción del fraude interno

Uno de los métodos más habituales de cometer fraude interno en empresas y en organismos públicos es la imputación de horas de trabajo inexistentes, en algunos casos no estando tan siquiera el empleado físicamente en las instalaciones de la entidad. Para ello, se pueden apoyar en compañeros que *"fichan"* en su lugar. Como consecuencia de ello, la empresa estaría remunerando al empleado por unas horas de trabajo que, en realidad, no ha realizado.

Esta situación acarrea pérdidas económicas así como posibles perjuicios a la imagen corporativa. El uso de tecnología biométrica para el control horario de los empleados puede ayudar a prevenir este tipo de fraude, verificando mediante diferentes métodos tanto el tiempo de trabajo imputado, como que el trabajador que registra su entrada es realmente quien dice ser.

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.

Oferta de nuevos servicios

El desarrollo de las líneas de investigación que actualmente se están llevando a cabo en torno a la biometría puede resultar en la oferta de nuevos servicios en un futuro cercano. Estos servicios abarcan diversas aplicaciones en el sector sanitario, el pago mediante dispositivos móviles, control parental, videovigilancia, etc.

4.2. PARA LOS USUARIOS FINALES

Los usuarios finales también se ven favorecidos por la implantación de tecnologías biométricas. A continuación se describen los principales beneficios que les reportan.

Aumento de la comodidad

La utilización de técnicas biométricas en procesos de identificación, autenticación y control de accesos suponen un aumento considerable de comodidad para los usuarios en la realización de estas tareas.

El empleo de tecnologías biométricas elimina la necesidad de recordar múltiples contraseñas que, por seguridad, se deben cambiar cada corto periodo de tiempo. En este sentido, el usuario tampoco se tendrá que poner en contacto, salvo excepciones, con el servicio de soporte informático o de atención al cliente para restaurar sus credenciales debido al olvido de contraseñas ni deberá extremar las precauciones para preservar la privacidad de las mismas. Del mismo modo, tampoco le resultará necesario llevar consigo ninguna tarjeta de identificación en todo momento ni existirá el riesgo de perderla o de que se dañe.

Reducción de tiempos de espera

La identificación y control de accesos realizados por métodos tradicionales suponen tiempos de espera que resultan molestos para el usuario. El uso efectivo de la biometría puede reducir considerablemente la espera y, por tanto, beneficiar al usuario. De este modo, en diferentes casos de éxito, se observa una reducción de espera en aeropuertos, tiendas, centros de ocio, entidades bancarias, etc.

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.

Mayor seguridad

Las tecnologías biométricas aportan un aumento de seguridad como consecuencia de los riesgos que mitigan. Esto redunda en beneficio para el usuario al reducir las posibilidades de que un tercero suplante su identidad para la comisión de algún delito o provocarle algún tipo de perjuicio.

La utilización de la biometría por parte de las administraciones públicas en la lucha contra el crimen también refuerza la sensación de seguridad de los ciudadanos.

Aumento de la privacidad

La seguridad de los datos de carácter personal de los ciudadanos en las múltiples transacciones que hacen uso de ellos, es otro de los aspectos reforzados por la aplicación de técnicas biométricas.

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.

Familiarización con tecnología avanzada

El uso de tecnologías biométricas acerca en muchas ocasiones tecnología puntera, aplicada en sensores de última generación, a la ciudadanía. Pese a las reticencias que pueden mostrar los usuarios en un primer momento hacia una tecnología que no conocen, tras una pequeña fase de adaptación, su opinión sobre la misma suele mejorar por norma general. Como consecuencia, el uso de tecnología en el día a día del ciudadano se convierte en algo más sencillo y habitual.

4.3 COMPARATIVA CON OTROS SISTEMAS DE AUTENTICACIÓN E IDENTIFICACIÓN AUTOMÁTICA

Las tecnologías biométricas surgen como alternativa o complemento a las técnicas de identificación y autenticación ya 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:

- **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.

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

- **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.

- **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.

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

- **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.

- **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.

- **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.

- **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.

- **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.

- **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.

- **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.

A continuación se muestra una tabla ilustrativa identificando en qué aspectos destaca cada método de autenticación:

ASPECTO	BIOMETRÍA	CONTRASEÑAS /TARJETAS
Necesidad de secreto		
Posibilidad de robo		
Posibilidad de pérdida		
Registro inicial y posibilidad de regeneración		
Proceso de comparación		
Comodidad del usuario		
Vulnerabilidad ante el espionaje		
Vulnerabilidad a un ataque por fuerza bruta		
Medidas de prevención		
Autenticación de usuarios ‘reales’		
Coste de implantación		
Coste de mantenimiento		

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.

5. 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 actuales 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.

5.1. AMENAZAS

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.

Pérdida o robo de información biométrica

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. 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.

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.

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.

Incumplimiento de la normativa de protección de datos personales

> Es necesario tener en cuenta que la Agencia Española de Protección de Datos (AEPD) ha definido los datos biométricos como "aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión", tal y como se desprende de varios de sus informes jurídicos.

En consecuencia, podemos concluir que 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 Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y por su normativa de desarrollo, esto es, por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD (RDLOPD). A ello hay que sumar cierta legislación menor (Instrucciones, etc.), informes de la AEPD y algunas resoluciones judiciales.

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. A continuación se detallan algunas de los deberes y obligaciones más destacables:

- Inscribir los ficheros de datos personales en el Registro General de Protección de Datos de la AEPD o bien, tratándose de ficheros de titularidad pública, en el Registro de la Autoridad autonómica competente.

- Informar a los usuarios afectados en relación con el tratamiento de sus datos personales que se desea llevar a cabo.

- Solicitar y obtener el consentimiento de los usuarios afectados cuando sea necesario.

- Facilitar a los usuarios el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO).

- Cumplir con el principio de calidad de los datos personales y establecer el denominado "juicio de proporcionalidad", esto es, determinar en relación con el fin que se pretende alcanzar si la medida en cuestión resulta idónea, necesaria por no existir otra más moderada y guarda el necesario equilibrio por derivarse mayores beneficios.

- Regular adecuadamente el acceso a los datos biométricos por parte de terceros prestadores de servicios.

- Implantar las medidas de seguridad exigidas por el RDLOPD, tanto por el responsable del fichero de datos biométricos y, en su caso, por el encargado del tratamiento.

A la vista de todo lo anterior, no cabe duda de que un tratamiento inadecuado puede derivar en una infracción o incumplimiento de la normativa vigente en materia de protección de datos personales, con la consecuente exposición a sanciones pecuniarias y el deterioro de la imagen de la entidad. De hecho, las sanciones tipificadas en la LOPD van desde el mero apercibimiento en

los casos más leves, hasta multas que pueden alcanzar los 600.000 euros por infracción en los casos más graves, sin olvidar la posible reclamación de daños y perjuicios por parte del sujeto afectado ante la jurisdicción civil.

Por otro lado, en lo que respecta específicamente a las medidas de seguridad a adoptar, a pesar de que estos datos biométricos se han considerado, con carácter general, como "de nivel básico" de conformidad con el RDLOPD, siendo equiparables a una simple dirección o un número de teléfono, 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.

A este respecto, si bien en la inmensa mayoría de los casos a los sistemas y/o programas informáticos en virtud de los cuales se traten datos biométricos de personas físicas identificadas o identificables se les deberá aplicar las medidas de seguridad calificadas como de nivel básico por el RDLOPD (ver art. 81 y ss.), téngase en cuenta que en el caso de que los datos biométricos objeto de tratamiento en el sistema pudiesen además encontrarse eventualmente asociados o vinculados a la salud de los afectados (por ejemplo, a una discapacidad) o a otros datos especialmente protegidos, podría resultar también obligatoria la implantación de las medidas de seguridad de nivel medio y alto de conformidad con lo exigido en el referido RDLOPD.

En la siguiente tabla se compara el impacto en la privacidad en función del proceso de autenticación utilizado, el tipo de tecnología biométrica, el formato de la muestra y el tamaño de la base de datos donde se almacenan las muestras:

Impacto en la privacidad	Proceso	Tipo de tecnología	Muestra	Tipo de base de datos
Alto	Identificación	Fisiológico	Imagen biométrica	Bases de datos grandes/ centralizadas
Bajo	Verificación	De comportamiento	Muestra cifrada	Bases de datos pequeñas/ locales

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 ello es necesario realizar un análisis 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.

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.

Incidencias con el sistema

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.

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 usuario 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.

Alteración con ánimo fraudulento de los rasgos biométricos

Alteraciones en las huellas dactilares, en el vello facial, en las cuerdas vocales, etc. con el objetivo de evitar ser reconocido por un sistema biométrico. Es una práctica frecuente en los intentos de entrada ilegal en un país, tratando de eludir la identificación de un individuo reincidente.

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.

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.

Falta de aceptación cultural

Esta amenaza aparece en determinados grupos demográficos cuyas normas sociales o religiosas no favorecen la toma de muestras en determinadas téc-

nicas. 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.

5.2. VULNERABILIDADES

A continuación se listan algunas vulnerabilidades que afectan negativamente tanto a la implantación 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, etc. • 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.
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.

Tecnología biométrica	Vulnerabilidades
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.

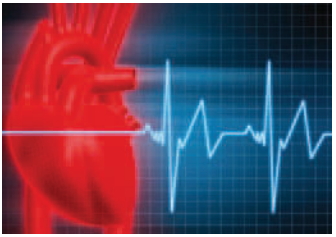
6. Buenas prácticas

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.

6.1. CATÁLOGO DE BUENAS PRÁCTICAS

La seguridad es fundamental en todos los elementos de un sistema biométrico. Es por ello que desde que se adquiere la muestra se deben aplicar los protocolos de seguridad pertinentes para garantizar la privacidad y evitar accesos no autorizados a la base de datos en que se guardan los registros biométricos.

Detección de vida



La detección de vida consiste en la capacidad de un sistema biométrico de detectar si la muestra adquirida proviene o no de un ser humano vivo, con el fin de evitar posibles intentos de fraude (como por ejemplo el uso de plantillas de goma que intenten simular una huella dactilar).

De este modo, el dispositivo biométrico comprobará uno o más de los siguientes factores, dependiendo de la tecnología empleada:

- Pulso cardíaco.
- Presión sanguínea.
- Detección de poros.
- Transpiración.
- Profundidad de la cara.
- Movimientos de la cabeza.
- Cambios de expresión facial.
- Movimiento del ojo.
- Dilatación de la pupila.
- Pigmentación del iris.
- Selección de palabras a pronunciar.

Esta técnica es uno de los principales métodos de los que dispone la biometría para combatir el fraude. No obstante, aún tiene bastante margen de mejora de cara al futuro.

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.

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.

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.

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.

Biometría en movimiento

La captura de muestras en movimiento es una forma de reducir la posible percepción de las técnicas de adquisición de información biométrica como intrusivas por parte de los usuarios y su reticencia a utilizarlas por este motivo. Este control no es válido para todas las técnicas pero ya se aplica, por ejemplo, en el reconocimiento facial y de iris.

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.

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.).

Igualmente, tal y como se ha venido estableciendo por la jurisprudencia reiterada, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales como las aquí analizadas viene determinada por una estricta observancia del citado principio de proporcionalidad.

7. Recomendaciones

A continuación se ha recogido un conjunto de consejos y recomendaciones para la investigación, implantación y uso de las tecnologías biométricas así como para su regulación.

7.1. FABRICANTES Y PROVEEDORES DE SERVICIOS

1. Apostar por la innovación en el desarrollo e implantación con el objetivo de fomentar las tecnologías biométricas.

2. Ofrecer sistemas de alta calidad, fomentando el éxito final que ayudará a la mejora de la imagen de la biometría en general.

3. Solventar las dudas de los clientes, informando de la importancia y la base tecnológica del sistema; de esta forma, el cliente podrá tomar una decisión informada sobre la tecnología a implantar.

4. Analizar al cliente para poder asesorarle en la tecnología idónea según sus necesidades y poder formar apropiadamente a los usuarios sobre su utilización.

5. Promover una unificación de algoritmos, cifrados y procesos de extracción de muestras, lo que favorecerá la interoperabilidad entre los sistemas implantados.

6. Mostrar las ventajas de estos productos y servicios y no exagerar sobre los defectos o inconvenientes de otras técnicas de la competencia ya que, como consecuencia de ello, se desprestigia a la biometría en general.

7. Solicitar permiso a los usuarios para tratar sus datos biométricos, siendo muy concreto y transparente sobre tratamiento y finalidad de su uso.

8. Garantizar especialmente la seguridad y confidencialidad de los datos cedidos para generar confianza en los usuarios del sistema.

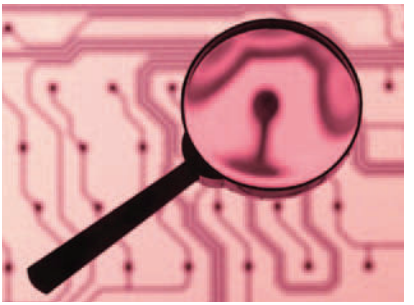
7.2 INVESTIGADORES

1. Adaptarse a los requerimientos de los usuarios finales con el objetivo de desarrollar líneas de investigación que puedan satisfacer las necesidades existentes.

2. Conocer la situación actual de la industria biométrica y evitar la elaboración de prototipos complejos en el ámbito comercial por su coste o utilidad.

3. Explorar diferentes opciones de mejora y abaratamiento de la tecnología para favorecer su desarrollo y expansión.

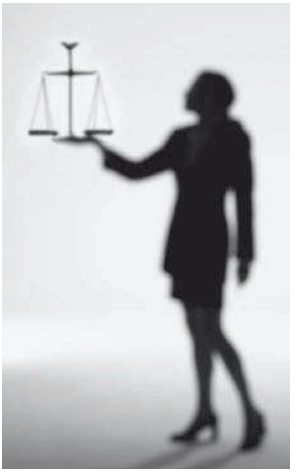
4. Realizar labor divulgativa de cara a fomentar que la ciudadanía se familiarice, comprenda y confíe en la biometría.



7.3. LEGISLADORES Y AGENTES DE ESTANDARIZACIÓN

1. Garantizar los derechos de privacidad de los ciudadanos, permitiendo al mismo tiempo el desarrollo de las tecnologías que ofrecen una mayor seguridad, como las biométricas.

2. Si bien la regulación actual en España, en materia de protección de datos es suficiente para regular el ámbito de la biometría, sin embargo, de cara a unificar criterios y atender a una especial sensibilidad de la población, podría ser conveniente desarrollar una regulación específica para la biometría



3. Evitar una normativa excesivamente rígida que impida o dificulte el uso de la biometría o que no se pueda adaptar fácilmente a los futuros desarrollos.

4. Desarrollar un análisis profundo de los riesgos y beneficios de la biometría antes de redactar y promulgar la normativa de desarrollo.

5. Avanzar en la regulación legislativa relativa a la suplantación de identidad (una de las mayores amenazas identificadas).

6. Fomentar la creación de un estándar único para cada tecnología que facilite la interoperabilidad.

7.4. ENTIDADES IMPLANTADORAS

1. Apostar por la implantación de tecnologías de calidad, esto es, ante las diferentes tecnologías existentes en el mercado, primar aquellas que ofrezcan mayor fiabilidad y, consecuentemente, mejores resultados.

2. Informarse adecuadamente de cara a hacer un uso correcto de las técnicas biométricas a implantar en la organización.

3. Ofrecer colaboración a los usuarios finales; la cooperación con ellos es el gran factor en el éxito de las implantaciones de tecnologías biométricas.

4. Ser consciente de que los datos biométricos son de carácter personal: es por ello que están regulados por la Ley Orgánica de Protección de Datos y se deben proteger como tales.

5. Solicitar siempre el consentimiento de recogida y uso de datos biométricos. La empresa que quiera recopilar y emplear dichos datos ha

de obtener el consentimiento del usuario, informándole previamente de su finalidad y tratamiento. De este modo no sólo se cumplirá con la legislación, sino que una actuación transparente ayudará a mejorar los niveles de aceptación por la ciudadanía, la usabilidad, y, por tanto, la efectividad de estas tecnologías.

6. Facilitar el ejercicio de los derechos ARCO de los usuarios sobre sus datos personales, dándoles a conocer la posibilidad de obtener información, modificar, suprimir y oponerse al tratamiento de dichos datos.

7.5. USUARIOS FINALES

1. Exigir los niveles de seguridad apropiados para proteger sus datos biométricos a las empresas que los recojan, empleen y almacenen.

2. Dar el consentimiento sólo tras ser informado y conocer el uso concreto que se va a dar a los datos biométricos solicitados.

3. Perder el miedo a las tecnologías biométricas. Solo a partir de una información rigurosa y un verdadero conocimiento de las mismas, podrán desterrarse suposiciones y falsedades, y se generará una mayor confianza en ellas, normalizándose su uso.

8. Glosario de términos relacionados con la biometría

A continuación se explican diferentes términos biométricos empleados en la realización de esta guía o que son utilizados especialmente en esta materia:

- **AFIS**: Sistema biométrico que compara un registro de huellas dactilares con los registros de una base de datos para determinar la identidad de un individuo. El sistema AFIS se utiliza, especialmente, en labores policiales. En España se conoce como Sistema Automático de Identificación Dactilar.

- **Algoritmo**: Secuencia de instrucciones que indica a un sistema cómo resolver un problema en especial. Un sistema biométrico utiliza múltiples algoritmos; por ejemplo, para el procesamiento de imágenes, la generación de plantillas, comparaciones, etc.

- **Amenaza**: Hecho o acción, intencional o no, que puede comprometer la seguridad e integridad de un sistema.

- **Autenticación**: Proceso para comprobar la veracidad de alguna declaración, en el caso que se expone en esta guía se trata de la confirmación de una identidad.

- **Búsqueda de coincidencias**: Proceso que incluye la comparación de una muestra biométrica con una plantilla almacenada anteriormente y el cálculo del grado de semejanza. Los sistemas toman las decisiones basándose en el nivel de semejanza resultante y en relación a los límites de semejanza mínimos establecidos para dar por válida la identificación.

- **Captura**: Obtención de una muestra biométrica de un individuo por medio de un sensor.

- **Coincidencia**: Decisión según la cual una muestra biométrica y una plantilla almacenada provienen de la misma persona, basada en el alto grado de semejanza.

- **Comparación**: Proceso de cotejo de una muestra biométrica con otras almacenadas con anterioridad, con el fin de tomar una decisión sobre identificación o verificación.

- **Encriptación**: Transformación de datos mediante un algoritmo criptográfico para producir texto cifrado, es decir, esconder la información que contienen los datos.

- **Extracción**: Conversión de una muestra capturada en datos biométricos para que puedan ser comparados con las plantillas de referencia.

- **Impostor**: Sujeto que intenta hacer coincidir su muestra biométrica con la de otra persona.

- **Minucias**: Características de las crestas de fricción que se utilizan para identificar una imagen de huella dactilar. Las minucias son los puntos donde las crestas de fricción comienzan, terminan o se dividen en dos o más crestas. En muchos sistemas de huellas dactilares se realizan comparaciones de las minucias en lugar de las imágenes en su conjunto.

- **Muestra**: Información biométrica presentada por el usuario y capturada por el sistema.

- **PIN** *(Personal Identification Number)*: número de identificación personal que puede ser utilizado para declarar o verificar una identidad.

- **Plantilla**: Representación digital de las características distintivas de un individuo que contiene la información extraída de una muestra biométrica. Las plantillas se utilizan durante la autenticación biométrica como base de comparación.

- **Precisión**: Término utilizado para describir cuál es el rendimiento de un sistema biométrico. La estadística real que determina dicho rendimiento varía según la tarea a realizar (verificación o identificación).

- **Reconocimiento:** Término utilizado en la descripción de sistemas biométricos (por ejemplo, reconocimiento de rostro o reconocimiento de iris) en relación con su función principal. El término "reconocimiento" no implica necesariamente verificación o identificación.

- **Registro:** Captura inicial de una muestra biométrica de un usuario, procesamiento de la misma e inscripción de la referencia en la base de datos del sistema biométrico para su posterior comparación.

- **Rendimiento:** forma de medir las características (precisión, velocidad, etc.) de un sistema o algoritmo biométrico.

- **Sensor:** Dispositivo que convierte los datos biométricos de entrada en una señal digital y transmite esta información al dispositivo de procesamiento.

- **Sistema biométrico bimodal**: Sistema en el que se utilizan dos rasgos biométricos de distinta naturaleza.

- **Suplantación**: Habilidad para engañar a un sensor biométrico y hacer que reconozca a un usuario ilegítimo como legítimo (verificación) o que no encuentre la identificación de una persona que es parte de la base de datos.

- **Tasa de error de adquisición** (*Failure To Acquire Rate*): Porcentaje de veces que el sistema no es capaz de capturar una muestra de calidad suficiente para ser procesada.

- **Tasa de error de registro** *(Failure To Enrol Rate)***:** Porcentaje de la población para el cual el sistema biométrico no es capaz de generar muestras de calidad suficiente.

- **Tasa de falso negativo** *(False Rejection Rate)*: Porcentaje de veces que el sistema no vincula a un individuo con su propia plantilla biométrica existente.

- **Tasa de falso positivo** (*False Acceptance Rate*): Porcentaje de veces que un sistema vincula erróneamente a un individuo con la información biométrica existente de otra persona.

- **Umbral**: valor numérico usado como límite para decidir si el resultado de una comparativa es considerado una coincidencia o no.

- **Vulnerabilidad**: Potencialidad de verse comprometido un sistema por una actividad fraudulenta, defecto de diseño, error de uso, accidente, fallo en el hardware, o condición ambiental externa.

OBSERVATORIO INTECO

Síguenos a traves de:

Web **http://observatorio.inteco.es**

Perfil Facebook ObservaINTECO
http://www.facebook.com/ObservaINTECO

Perfil Twitter ObservaINTECO:
http://www.twitter.com/ObservaINTECO

Perfil Scribd ObservaINTECO:
http://www.scribd.com/ObservaINTECO

Canal Youtube ObservaINTECO:
http://www.youtube.com/ObservaINTECO

Blog del Observatorio de la Seguridad de la Información:
http://www.inteco.es/blogs/inteco/Seguridad/BlogSeguridad

Envíanos tus consultas y comentarios a:

observatorio@inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación

Con el patrocinio de:

Deloitte.