El uso de la biometría en la prestación de servicios sociales: *buenas prácticas*

Javier Preciozzi

BID

El uso de la biometría en la prestación de servicios sociales:
buenas prácticas

Agradecimientos:
El autor agradece a Cristina Pombo, Arturo Muente, Alex Bagolle, Ariel Nowersztern y Natalia González Alarcón, quienes proporcionaron comentarios e insumos relevantes para el desarrollo de este documento. Igualmente, a Patricia Ardila por su labor de edición y a Alejandro Scaff por el diseño.

https://www.iadb.org/

CONTENIDO

Acerca de este material

>Presentación

En los últimos años, el uso de sistemas biométricos se ha expandido de manera significativa en los escenarios más variados en todo el mundo. Noticieros y diarios a menudo incluyen noticias sobre sus diversos usos: desde el pago automático en el momento de comprar una bebida, hasta la detección de personas requeridas en aeropuertos o lugares públicos. Ahora bien, este incremento ha traído aparejada una enorme preocupación por la forma en que se los emplea: sistemas de reconocimiento facial que procesan rostros sin el consentimiento de las personas filmadas o fotografiadas, sistemas de identidad nacional cuyo uso sistemático genera perjuicios a la población e incluso sistemas biométricos con sesgos evidentes a la hora de procesar los datos por sexo, raza y edad. En todos los casos, la crítica principal es que los dueños de los datos —los individuos mismos— no tienen control sobre estos.

Este documento hace parte de una serie de materiales producidos por la iniciativa fAIr LAC sobre el uso de la inteligencia artificial en la prestación de servicios sociales. El propósito no es generar un debate sobre el uso o no de sistemas biométricos, sino ofrecer una serie de herramientas para entender cuándo, cómo y de qué forma su implementación en proyectos de prestación de servicios sociales tiene sentido y, en caso de utilizarse, cuáles son las precauciones que se deben tomar para proteger a la ciudadanía.

>Iniciativa fAIr LAC

El Banco Interamericano de Desarrollo (BID), en colaboración con socios y aliados estratégicos, lidera la iniciativa fAIr LAC mediante la cual se busca promover la adopción responsable de la inteligencia artificial (IA) en los sistemas de toma de decisiones. Con ello se busca mejorar la prestación de servicios sociales y crear oportunidades de desarrollo en aras de atenuar la desigualdad social. Este documento se enmarca en esta iniciativa, cuyo objetivo es poner a disposición de los equipos técnicos y de los responsables por la toma de decisiones un conjunto de guías relacionadas con el uso de los sistemas biométricos en sistemas vinculados con los servicios sociales.

>¿Por qué este documento?

Uno de los puntos débiles de la expansión acelerada del uso de sistemas biométricos es que esta se ha producido sin que se realice un análisis profundo sobre su aplicabilidad y sin que se hayan adoptado criterios mínimos para asegurar que dichas iniciativas sean exitosas en un contexto de protección de derechos y libertades. Si bien es cierto que abunda la literatura sobre los sistemas biométricos, y sobre los problemas que su uso incorrecto puede generar, no se dispone de un material de referencia sencillo y serio que permita entender cómo, cuándo y de qué forma se deben llevar adelante proyectos que incluyan sistemas biométricos. Ese es precisamente el objetivo del presente documento.

>¿A quién está dirigido?

Este documento está dirigido a dos tipos de público: en primer lugar a los equipos técnicos responsables del diseño, implementación y ejecución de sistemas biométricos en el ámbito

de la prestación de servicios sociales y, en segundo lugar, a un público no especializado pero interesado en conocer los conceptos básicos de los sistemas biométricos, y en particular a las personas responsables por la toma de decisiones en los ámbitos público y privado.

En razón de este carácter dual, el documento ha sido estructurado de manera tal que su contenido general pueda ser aprovechado por personas no especializadas, pero también por individuos con formación técnica para los cuales se han incluido recuadros con contenido avanzado más detallado. De este modo se espera cumplir con el objetivo de que esta guía se constituya en un material de referencia tanto para las personas responsables por la toma de decisiones como para los especialistas.

Resumen Ejecutivo

El uso generalizado de los sistemas biométricos en la sociedad exige el abordaje de dos asuntos fundamentales: (1) su aplicabilidad —si se justifican en un determinado campo de actividad o si existen alternativas más eficaces, efectivas y eficientes en función de los costos— y (2) las preocupaciones que de ello se desprenden como resultado de la captura de información personal. Tales preocupaciones se relacionan con su uso sin el conocimiento y el consentimiento de sus titulares, así como con los sesgos que estos sistemas puedan reproducir a partir de los prejuicios que permean las sociedades, afectando a unos grupos más que a otros. Surge entonces la imperiosa necesidad de tomar medidas que garanticen los derechos y la protección de todos los ciudadanos, para lo cual se requiere entender cómo funcionan estos sistemas y así aprovechar su uso sin afectar los intereses de aquellos a quienes se busca favorecer, en especial —aunque no exclusivamente— en la prestación de servicios del Estado.

El objetivo de un sistema biométrico es reconocer automáticamente a una persona por lo que es, y no por lo que sabe (una contraseña) o posee (una tarjeta). Su utilización puede considerarse para cualquier sistema o proceso que requiera el reconocimiento, identificación o autenticación de la identidad de una persona.

Los datos biométricos son considerados datos sensibles, y por lo tanto su manejo debe seguir prácticas de confidencialidad y seguridad muy estrictas. En el momento de definir el posible uso de un sistema biométrico, es conveniente considerar si es realmente necesario, y si no hay otras alternativas de identificación más adecuadas. Lo mismo en lo que se refiere a determinar sus ventajas y desventajas frente a otros mecanismos de identificación.

Una vez tomada la decisión de utilizar un sistema biométrico, es importante responder a una serie de preguntas que ayuden a definir la solución más adecuada: qué tipo de biometría utilizar, en qué contexto va a funcionar, y cómo se garantizará la privacidad y la protección de los datos biométricos. Entre otras consideraciones, se deben tener en cuenta aspectos tales como la edad de la población objetivo, el tiempo de uso del sistema, la actualización de los datos biométricos, el lugar de la aplicación y otros elementos de índole cultural.

Asimismo, se debe tener en cuenta que la biometría es solo un componente de un sistema de identificación más amplio que exige considerar otro conjunto de elementos humanos, así como de infraestructura, gobernanza y funcionamiento operativo.

A continuación, se resumen los puntos críticos de un sistema biométrico.

Proceso de enrolamiento y calidad de los datos. El proceso de enrolamiento es el mecanismo mediante el cual se capturan los datos biométricos y se los asigna a una persona en particular. Dado que en el momento de identificar a una persona estos datos biométricos almacenados serán utilizados para compararlos con nuevas muestras, su calidad es de vital importancia. Si durante el enrolamiento la calidad de la captura de los datos es deficiente, es posible que a la postre esto se traduzca en el deterioro de la calidad de todo el sistema

biométrico. Por esa razón se debe dar especial importancia al proceso de enrolamiento y a la calidad del dato obtenido.

Errores específicos a los sistemas biométricos. Existen factores que dificultan el reconocimiento de las personas mediante el uso de sistemas biométricos. Por un lado, están los cambios naturales en los individuos como son el envejecimiento y las fluctuaciones de peso, entre otros. Asimismo, es posible que personas distintas tengan características muy similares, como es el caso de los gemelos. Si bien es cierto que algunos rasgos biométricos son más estables que otros, ninguno es inmune a errores originados en los factores mencionados. A esto se agrega el hecho de que, como para obtener la muestra biométrica se requiere algún tipo de sensor (cámara fotográfica, escáner de huellas dactilares o de iris, etc.), las distintas capturas presentarán diferencias, aunque el rasgo biométrico sea el mismo. Esto hace que la comparación nunca sea exacta.

Punto de funcionamiento (umbral de aceptación). El reconocimiento biométrico se realiza mediante la comparación de muestras de la persona (iris, huella dactilar, rostro). Esto presenta desafíos significativos, dado que los sistemas no son perfectos. Dos muestras de la misma característica de una persona nunca serán iguales puesto que los procesos de captura y extracción no se realizan en las mismas condiciones. Los sistemas biométricos comparan las muestras y devuelven un puntaje que determinará cuán parecidas son. Con base en esa medida, el sistema debe decidir si las muestras corresponden o no a la misma persona, para lo cual se define un umbral: si el puntaje es mayor al umbral, se acepta; si es menor, se rechaza. Determinar un umbral de desempeño es crucial para el funcionamiento del sistema biométrico.

Dado que los datos no son perfectos, una vez definido el umbral se generan dos tipos de errores: falsas aceptaciones (se acepta a una persona que no es) y falsos rechazos (se rechaza a la persona correcta). Si se fija un umbral bajo, el sistema aceptará muchas identidades erróneas, lo cual puede evitarse estableciendo un umbral más alto. Sin embargo, un umbral más alto presentará problemas para validar identidades cuya muestra obtenida difiera de la previamente almacenada.

Una vez seleccionado el umbral, se tendrá un **punto de funcionamiento**, el cual determinará la tasa de falsos positivos y negativos del sistema. La determinación de este punto tiene un impacto definitivo en el sistema final, ya que puede conducir o bien a rechazar o bien a aceptar de manera incorrecta el acceso a un determinado servicio.

Seguridad del sistema. Es usual que en las regulaciones de protección de datos se considere a los datos biométricos como “sensibles”, es decir, sujetos a un tratamiento especial. En su calidad de sistemas de información, los sistemas biométricos pueden sufrir los mismos ataques de los cuales son víctimas otros sistemas de esa índole. Sin embargo, existe un conjunto de amenazas propias que se presentan durante las etapas de captura, comparación y almacenamiento de muestras. El tipo de ataque más común es el intento de suplantación de identidad mediante la presentación de una copia de la muestra biométrica (una huella dactilar de silicona, una careta con la cara de otra persona, etc.). Para cada uno de estos casos, existen mecanismos de detección (*anti-spoofing*) que deben ser tenidos en cuenta.

Privacidad y ética. La forma de dar garantías a una población cuyos datos biométricos están siendo empleados de manera adecuada es mediante la formulación de políticas sólidas de manejo de datos personales dotadas de protocolos claros de uso y transparencia. A la hora de desplegar sistemas biométricos, el cumplimiento del marco legal es un elemento de suma importancia. Es por esto que existe un conjunto de estándares y normativas que se debe tener en cuenta en el momento de diseñar una solución de biometría. Asimismo, y dado que los sistemas biométricos pueden sufrir de sesgos no deseados, es importante evitar una discriminación posible por sexo, edad y/o raza.

En suma, todos los elementos críticos arriba mencionados deberán orientar las decisiones en el momento de adquirir y emplear los sistemas biométricos, una vez que se hayan discutido las ventajas de su aplicabilidad en los distintos sectores, así como los estándares de funcionamiento y las medidas que garanticen que dichas iniciativas sean exitosas en el ámbito de la prestación de servicios y en un contexto de protección de derechos y libertades.

Parte I.
Conceptos básicos de un sistema biométrico

Parte I. Conceptos básicos de un sistema biométrico

1.1 ¿Qué hace un sistema biométrico?: generalidades

Un sistema biométrico reconoce a una persona utilizando para ello sus características físicas[1]. El uso de estas características como mecanismo de reconocimiento es lo que distingue a los sistemas biométricos de otros que se basan en datos como usuario y contraseña, PIN, etc.

> *Definición:* Una **característica biométrica**[2] es una característica biológica o conductual de un individuo de la cual se puede extraer información que permita su reconocimiento (ISO/IEC 2382)[3].

Un **sistema biométrico** es entonces un sistema de reconocimiento de personas que utiliza información biométrica.

> *Definición:* El objetivo de un **sistema biométrico** es el reconocimiento de individuos con base en sus características biológicas o conductuales (ISO/IEC 2382).

¿En qué se diferencia de otros sistemas de reconocimiento?

Para establecer la diferencia entre el sistema de identificación biométrico y otros de uso común se emplearán casos ilustrativos. Tómese como ejemplo un sitio web cuyo modo de acceso a los servicios que presta requiera el ingreso de usuario y contraseña. En esta instancia se está reconociendo al usuario bajo el supuesto de que si la persona que está queriendo ingresar con un usuario determinado conoce la contraseña asociada a aquel, entonces se trata del individuo correcto y el sistema le permite la entrada. Aquí el mecanismo de reconocimiento se basa en lo que la persona **sabe**. Ahora, cuando se retira dinero de un cajero automático, el sistema también realiza un proceso de reconocimiento, aunque esta vez mediante la posesión de la tarjeta correspondiente y su PIN asociado. Aquí el proceso de reconocimiento se realiza a partir de lo que la persona sabe (el PIN) pero también por lo que **posee** (la tarjeta). Finalmente, cuando alguien pasa por un control migratorio automático (eGates), allí se le toma una fotografía que se compara con la almacenada en su pasaporte electrónico. El reconocimiento aquí se realiza a partir de lo que la persona posee (el pasaporte) pero también de lo que **es**, ya que se toma su fotografía en tiempo real. Esta última modalidad, en la cual el reconocimiento ocurre a partir de lo que la persona es, se conoce como **reconocimiento biométrico**.

1 También es usual considerar como características biométricas aquellos elementos de información conductual de la persona: su modo de caminar, su manera de escribir en el teclado, etc.
2 En la literatura se suele utilizar también el término "rasgo biométrico". Aquí se empleará **característica biométrica**, que es el término utilizado en el estándar ISO/IEC 2382.
3 Infortunadamente, el estándar de vocabulario ISO/IEC 2382 solo está disponible en inglés. La traducción corre por cuenta del autor.

Estos distintos tipos de reconocimiento (lo que la persona sabe, lo que la persona posee o lo que la persona es) pueden combinarse entre sí. Por ejemplo, para retirar dinero del cajero se requiere no solo tener la tarjeta sino conocer el PIN, o verificar con la huella dactilar o reconocimiento facial. A esta combinación se la conoce como autenticación de doble factor (2FA por las siglas en inglés de *two-factor authentication*).

Definición: El **reconocimiento biométrico** es el reconocimiento automático de individuos con base en sus características biológicas y conductuales, es decir, en sus características biométricas (ISO/IEC 2382).

1.2 Operaciones básicas de un sistema biométrico

El objetivo de un sistema biométrico es reconocer a una persona a través de sus características biométricas. Lo usual es tener una base de datos biométricos de distintas personas. Todo sistema biométrico debe tener entonces un mecanismo para recolectar y almacenar los datos biométricos de un individuo para que puedan ser utilizados en el futuro. Los datos biométricos pueden estar acompañados de otros datos (nombres, apellidos, etc.) que, mediante la generación de algún tipo de identificador, hacen que ese registro sea único. Este proceso se conoce como **enrolamiento**, el cual es crucial para el correcto funcionamiento de un sistema biométrico, como se verá a continuación.

>Enrolamiento

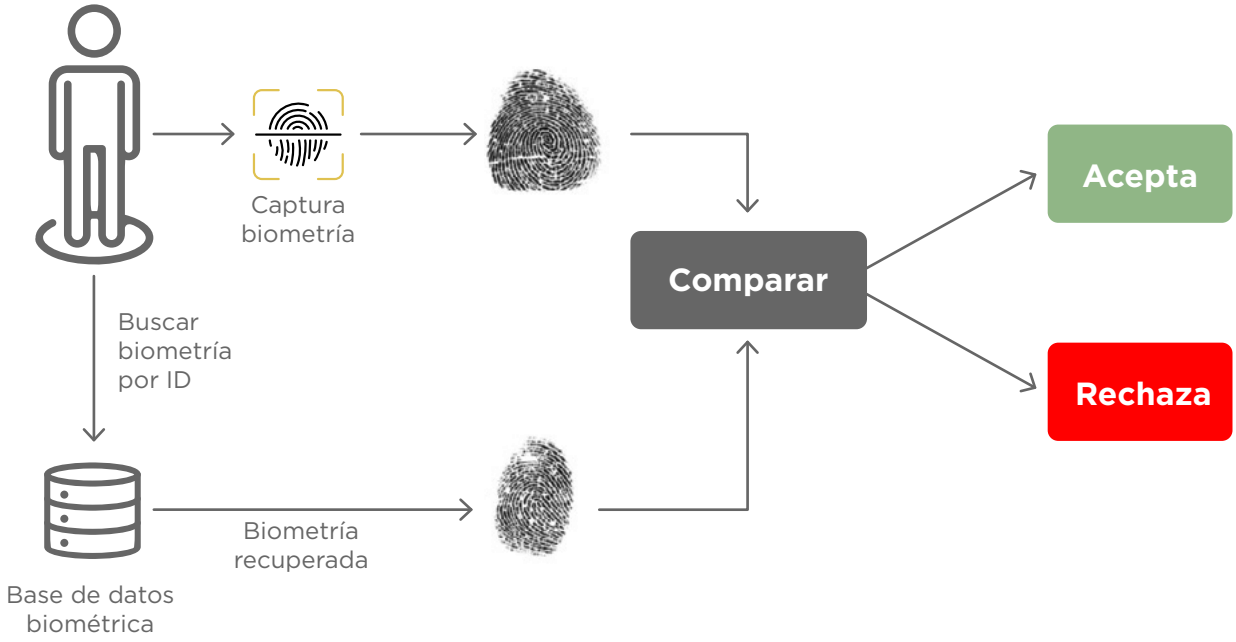
El enrolamiento es el registro de las características biométricas capturadas para una persona dada, con algún tipo de identificador que lo represente de forma unívoca en el sistema. Por ejemplo, en un sistema de identificación nacional ciudadana, este identificador será el número de identidad nacional.

Cabe señalar que un sistema biométrico no solo está constituido por el software y hardware que lo implementan, sino también por la base de datos biométricos asociada. Por esta razón, el proceso de enrolamiento es clave para obtener un sistema confiable cuyas tasas de error sean bajas. Este proceso debe garantizar que las muestras biométricas capturadas sean de la mejor calidad posible. Como se verá más adelante, los sensores de captura de datos biométricos cuentan por lo general con funciones de análisis de calidad. Esto es muy útil, ya que permite controlar la calidad de las muestras adquiridas para que, en caso de que sea insuficiente, se solicite la repetición de la captura.

Sobre esta base de datos se realizan dos operaciones básicas: **verificación de identidad** e **identificación**. Si bien en lenguaje coloquial "verificar la identidad" e "identificar" pueden resultar conceptos similares, en biometría tienen definiciones particulares que hace que sean diferentes, como se detalla a continuación.

>Verificación de identidad

En esta funcionalidad, el sistema intenta responder la siguiente pregunta: ¿es esta persona quien dice ser? En este escenario, la muestra biométrica del usuario se compara exclusivamente con la muestra almacenada en el sistema para determinar la identidad declarada.

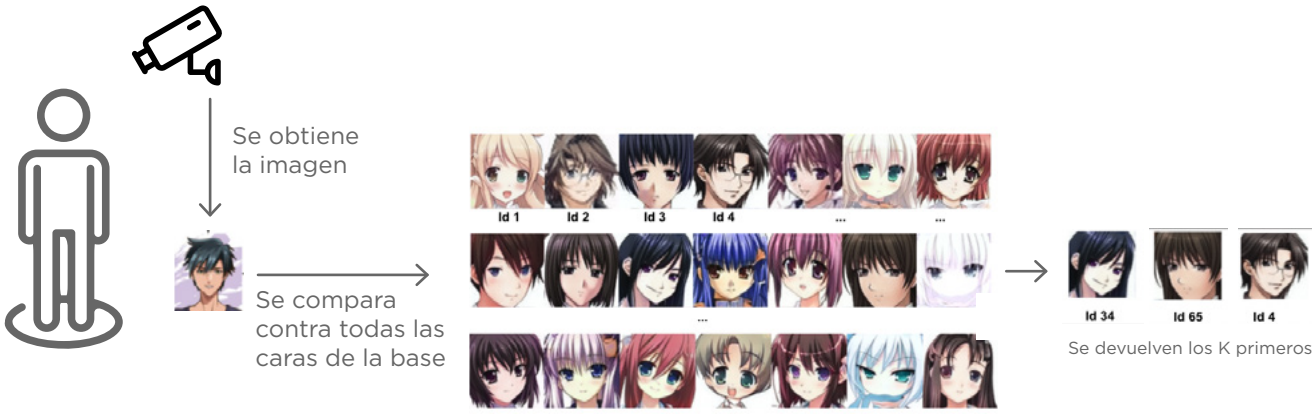


La verificación de identidad es también conocida como comparación uno a uno porque se comparan solo dos muestras biométricas[4].

>Identificación

La otra operación usual de un sistema biométrico es la identificación. En este caso, el sistema intenta responder a la siguiente pregunta: ¿quién es esta persona?

En otras palabras, la identificación es la funcionalidad que permite identificar a un individuo sin que este diga quién es. El resultado de un proceso de identificación es, en muchos casos, una lista de posibles candidatos ordenados según su grado de similitud o parecido y de acuerdo con el criterio definido por el sistema (véase más adelante).



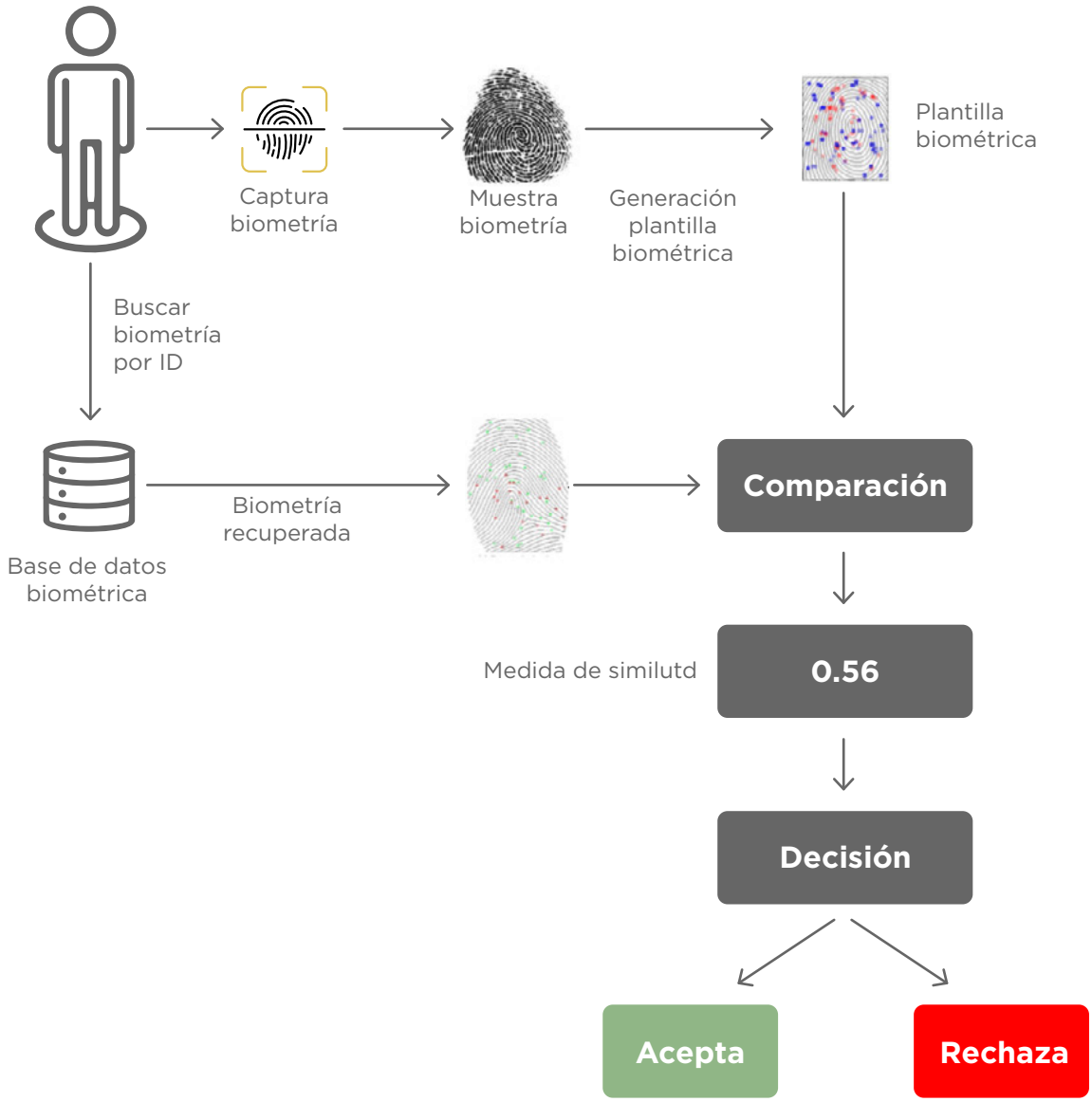
4 En rigor, es también verificación de identidad cuando se compara más de una muestra biométrica, aunque todas ellas asociadas con el mismo individuo (por ejemplo las huellas dactilares de dos dedos).

La identificación también se conoce como búsqueda uno a N, porque se compara una muestra contra las N muestras que componen la base de datos.

1.3 Procesos de un sistema biométrico

Para llevar a cabo cualquiera de las tres operaciones básicas descritas anteriormente, todo sistema biométrico debe realizar una serie de pasos que permitan capturar una muestra biométrica y compararla con otra previamente capturada. Los pasos a seguir son los siguientes:

1. Captura de la muestra biométrica
2. Generación de la plantilla biométrica
3. Comparación del vector de características biométricas
4. Decisión de aceptación o rechazo de la comparación



Paso 1 Captura de la muestra biométrica

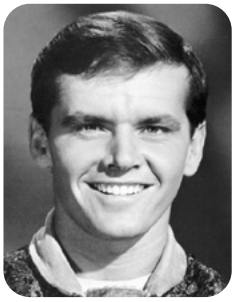
El primer paso en todo sistema biométrico es la captura de la característica biométrica con la que se quiere trabajar. Esta captura se realiza mediante un **sensor**[5] que, dependiendo de la característica biométrica, tendrá sus particularidades: una cámara fotográfica, un escáner de huellas dactilares, etc. En otras palabras, un sensor es algún tipo de dispositivo que permite la captura de la característica biométrica. La calidad y la facilidad de uso de este sensor pueden determinar la **efectividad** del rasgo capturado. Si bien la mayoría de los sensores capturan algún tipo de imagen bidimensional (imagen del rostro, huella dactilar, etc.), existen excepciones (firma autógrafa, ADN, voz, etc.). El objeto capturado durante esta etapa se llama **muestra biométrica**.

Definición: Una **muestra biométrica** es cualquier representación digital o analógica de una característica biométrica, previa a la extracción de características (ISO/IEC 2382)

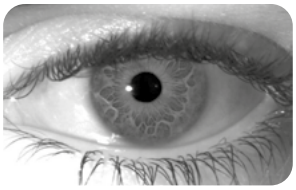
En la siguiente imagen se muestran tres características biométricas (huella dactilar, rostro e iris), junto con los sensores correspondientes y las muestras biométricas que capturan.

Huella Dactilar

Reconocimiento Facial



Iris



5 Es importante recordar que un sistema biométrico no implica necesariamente una solución informática. Los sistemas biométricos existen desde fines del siglo XIX en soporte de papel. En muchos países de América Latina, los sistemas de identificación nacional establecen la identidad con base en huellas dactilares obtenidas inicialmente en papel y comparadas mediante inspección visual por expertos dactiloscópicos.

Paso 2 Generación de la plantilla biométrica

Una vez capturada la muestra biométrica, se genera la plantilla biométrica correspondiente. Para esto, el sistema procesa la muestra biométrica capturada en la etapa anterior, extrae información y genera una representación más compacta que se conoce como **plantilla biométrica**[6].

> *Definición:* Una **plantilla biométrica** es un conjunto de características biométricas que pueden ser usadas para hacer una comparación directa (ISO/IEC 2382)

La razón principal para realizar esta operación es obtener una mejor representación de la muestra biométrica, dado que las plantillas almacenan aquellas características que hacen a la muestra única. Recuérdese que el objetivo principal de un sistema biométrico es poder reconocer a una persona, y que este reconocimiento se realiza mediante la comparación de muestras biométricas. Por lo general, estas muestras se han obtenido en distintos momentos a través de sensores variados y en condiciones ambientales disímiles. Esto hace que las muestras capturadas puedan ser muy distintas entre sí, incluso cuando se trata del mismo rasgo, lo cual hace que la comparación directa de las imágenes carezca de sentido.

Ni tan minucias

Desde fines del siglo XIX, existe un método de comparación de huellas dactilares basado en su estructura de crestas y valles. Si se mira una huella en detalle se notará que estas crestas y valles tienen comienzo (o fin) y bifurcaciones (donde se dividen en dos crestas). La distribución de estos puntos, conocidos como minucias, genera un patrón único. Por eso son muy útiles para comparar dos huellas dactilares. La ventaja que tiene contrastar estos puntos, en lugar de toda la imagen, es que esta distribución no cambia: es siempre la misma.

En el caso de las huellas dactilares, la plantilla de características biométricas es la lista de minucias con su respectiva posición, orientación y tipo.

Durante la fase de enrolamiento, lo que normalmente se almacena es la plantilla, aunque también es usual que se guarde la muestra biométrica como información adicional (por ejemplo, la imagen completa de la huella dactilar).

6 El término utilizado en inglés es *template*.

CONTENIDO AVANZADO

Preprocesamiento previo a la generación de la plantilla biométrica

Previamente a la generación de la plantilla biométrica, es usual realizar algún tipo de **preprocesamiento** con el objeto de mejorar la calidad del dato capturado de forma tal que la extracción de características sea óptima.

Existen tres tipos de preprocesamiento:

- **Análisis de la calidad:** Aquí se determina la calidad de la muestra capturada. Si es insuficiente, se desecha la muestra. En caso contrario, se acepta.
- **Segmentación de la imagen:** Esto consiste en separar la muestra biométrica (la huella, el rostro, p. ej.) del "fondo".
- **Mejora:** Como su nombre lo indica, este proceso incluye las mejoras que se aplican sobre la muestra capturada para optimizar los pasos siguientes de extracción y comparación. Un ejemplo típico de ello es la eliminación de ruido presente en todo sistema de obtención físico.

En muchos casos, estos procesos se realizan de forma simultánea, o por lo menos no se separan claramente entre sí. Cabe destacar también el hecho de que no tienen por qué ser parte del módulo de extracción de características; pueden considerarse como parte del módulo de captura o incluso como un módulo intermedio entre el de captura y el de extracción de características.

Paso 3 Comparación de características biométricas

El objetivo de este paso es comparar dos características biométricas para determinar qué tanto se parecen. Este paso se ejecuta tanto cuando se realiza una operación de verificación, como cuando se lleva a cabo una de identificación; la única diferencia es que en la identificación se realizan varias comparaciones.

La comparación de características biométricas se hace utilizando las plantillas biométricas extraídas en el paso anterior. Es importante resaltar que este proceso es independiente de dónde o cómo se encuentren almacenadas las plantillas. Lo usual es que los sistemas biométricos almacenen las plantillas en una base de datos y que la comparación se realice entre una nueva plantilla y la previamente guardada.

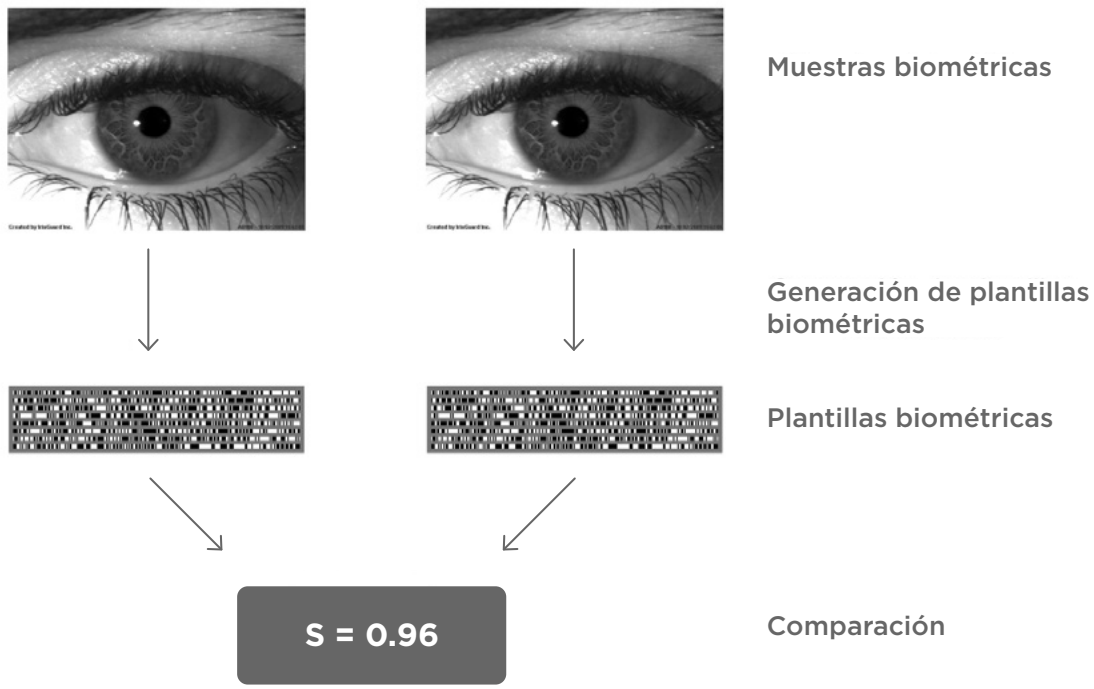
El resultado de este proceso de comparación es normalmente un **puntaje**[7] o una medida de **distancia** que indica cuán parecidas son ambas muestras. Si se trata de un puntaje, normalmente estará definido en un intervalo: cuanto mayor sea el puntaje, más parecidas serán las plantillas biométricas comparadas. Otra forma de ver el puntaje es pensarlo como una probabilidad: cuanto mayor sea el puntaje, mayor será la probabilidad de que las plantillas comparadas sean del mismo rasgo biométrico. Si se trata de una distancia, normalmente se define entre 0 y 1: cuanto más pequeña sea dicha distancia, más parecidas serán.

7 En la literatura relativa a los sistemas biométricos es usual encontrar el término en inglés, *score*, en lugar de puntaje.

Definición: El **puntaje** de comparación es un valor numérico que resulta de una comparación biométrica (ISO/IEC 2382).

Definición: La **distancia** es un resultado de la comparación que decrece con la similitud (ISO/IEC 2382).

La siguiente figura ilustra este proceso, donde el puntaje de 0,96 da la idea de que son rasgos biométricos muy parecidos (es decir, corresponden a la misma persona):



En lo que sigue del documento se usará el concepto de **distancia** en lugar de puntaje para hacer referencia al resultado de la comparación.

Paso 4 Decisión

Dado que los procesos de captura y extracción de características para generar la plantilla biométrica no son perfectos, la comparación de dos muestras biométricas del mismo rasgo nunca dará una distancia 0. Es decir, la comparación de dos muestras biométricas obtenidas de la misma característica y persona (por ejemplo, dos muestras del pulgar derecho) nunca será perfecta, incluso en condiciones de captura ideal. Si la comparación produce una distancia, esto quiere decir que siempre será mayor que 0. Por lo tanto, a partir del resultado de la comparación de dos muestras biométricas, el último paso de un sistema biométrico será determinar si corresponden o no a la misma persona.

Esta etapa de decisión es muy importante en cualquier sistema biométrico, y por ende la selección del umbral —o de los umbrales— a utilizar es crucial para el funcionamiento final de todo el sistema. Por esta razón, en la siguiente sección se analizarán en detalle sus principales características.

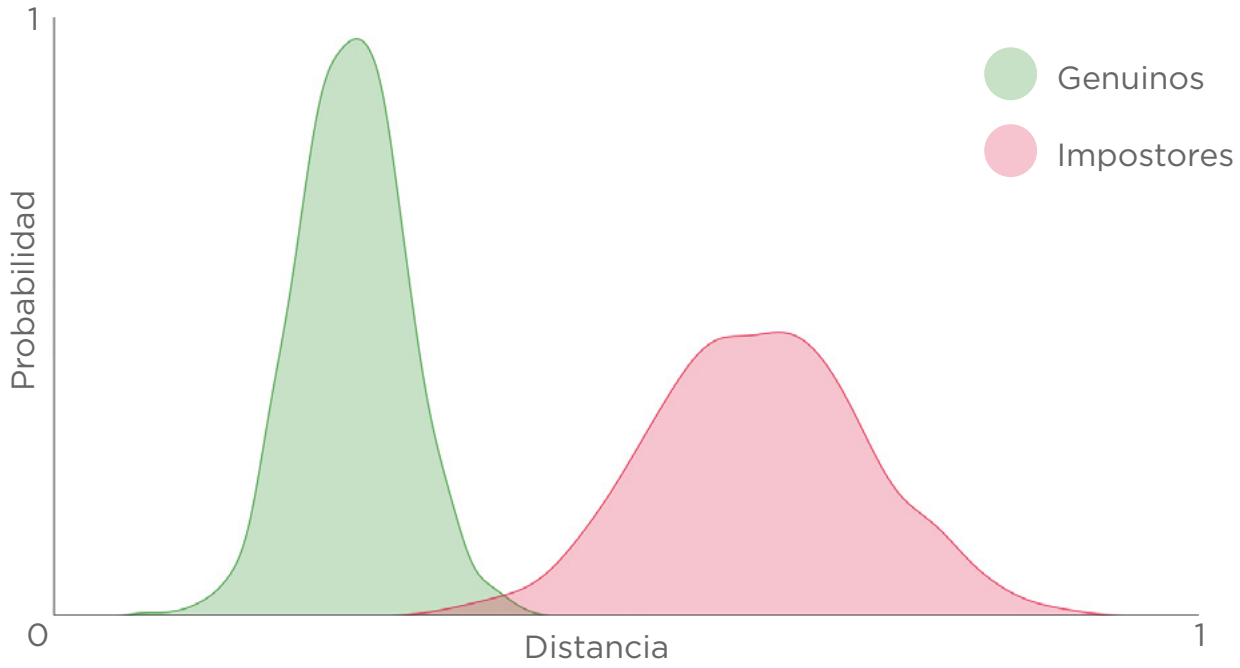
1.4 ¿Cómo se determina el desempeño de un sistema biométrico en la práctica?

Para comenzar, recuérdese que dos muestras de la misma característica biométrica nunca serán iguales, debido a los múltiples factores discutidos anteriormente. A modo de ejemplo, estas dos imágenes de huellas dactilares son del mismo dedo, pero claramente las imágenes son distintas[8]:

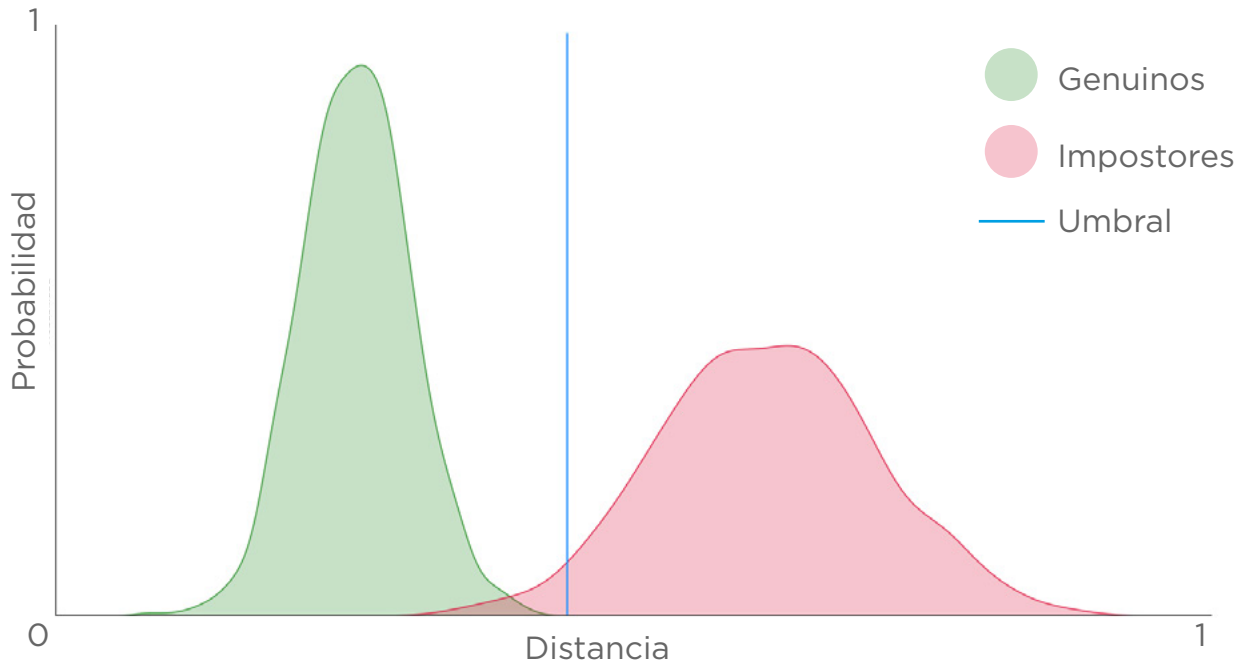
Por más que en las etapas de captura y generación de la plantilla biométrica se busque minimizar este problema, es muy poco probable que se obtenga exactamente la misma plantilla. Por lo tanto, al compararlas se obtendrá un valor de distancia a partir del cual se deberá decidir qué hacer: ¿se acepta que las dos tomas corresponden a la misma huella o no? Lo usual en estos casos es definir un **umbral de decisión**: si la distancia es menor al umbral, se dice que las dos muestras son del mismo dedo y si es mayor se dice que no. Ahora bien, ¿cómo se determina este umbral para un sistema biométrico dado?

La forma usual consiste en realizar un análisis estadístico con datos conocidos. Se toma un conjunto de pares de muestras que tienen el mismo origen (por ej., el mismo dedo), se los compara y se grafica su **distancia**. A este conjunto de pares del mismo origen se le conoce en la literatura como **"genuinos"**. Lo mismo se hace con un conjunto de comparaciones que se sabe de antemano que no tienen el mismo origen (por ej., dedos distintos) y también se grafica. A este conjunto se le denomina **"impostores"**. A continuación se muestran distancias en ambos conjuntos:

8 Imágenes tomadas de "NIST Special Database 301": https://www.nist.gov/itl/iad/image-group/nist-special-database-301

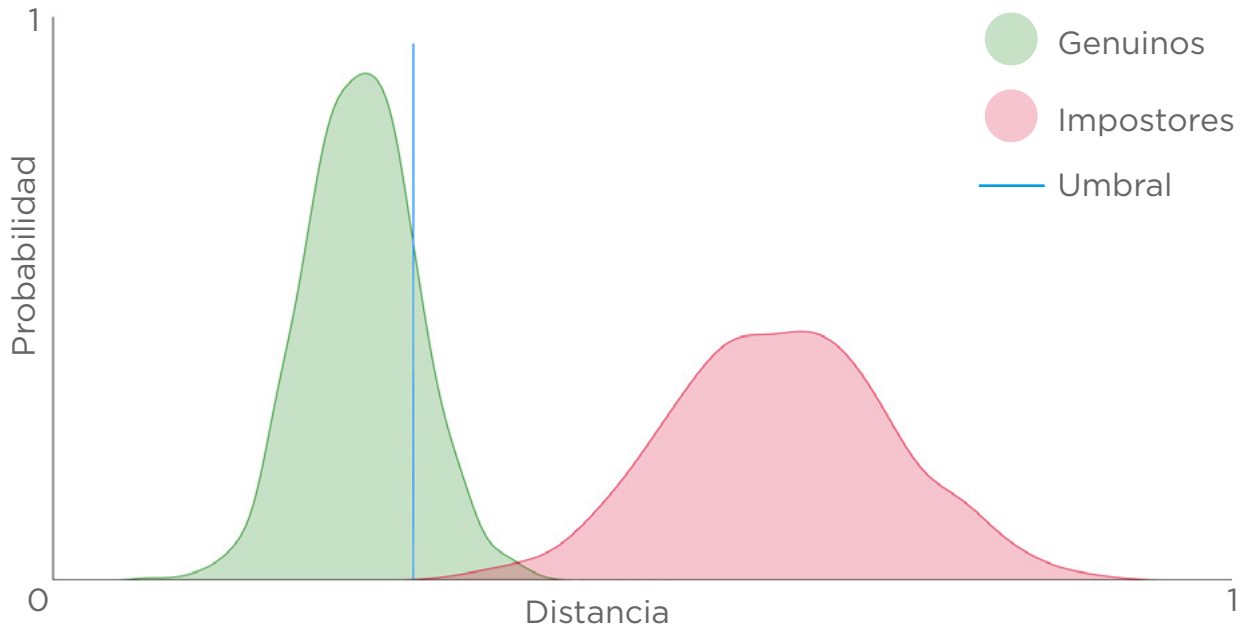


Nótese que en este gráfico, como era de esperar, la distancia entre la mayoría de los genuinos es menor que aquella entre la mayoría de los impostores. A partir de la distribución de distancias es posible definir un umbral: si la distancia obtenida es menor que el umbral, se considera que las muestras comparadas corresponden a la misma persona, mientras que si es menor que el umbral se considera que no:

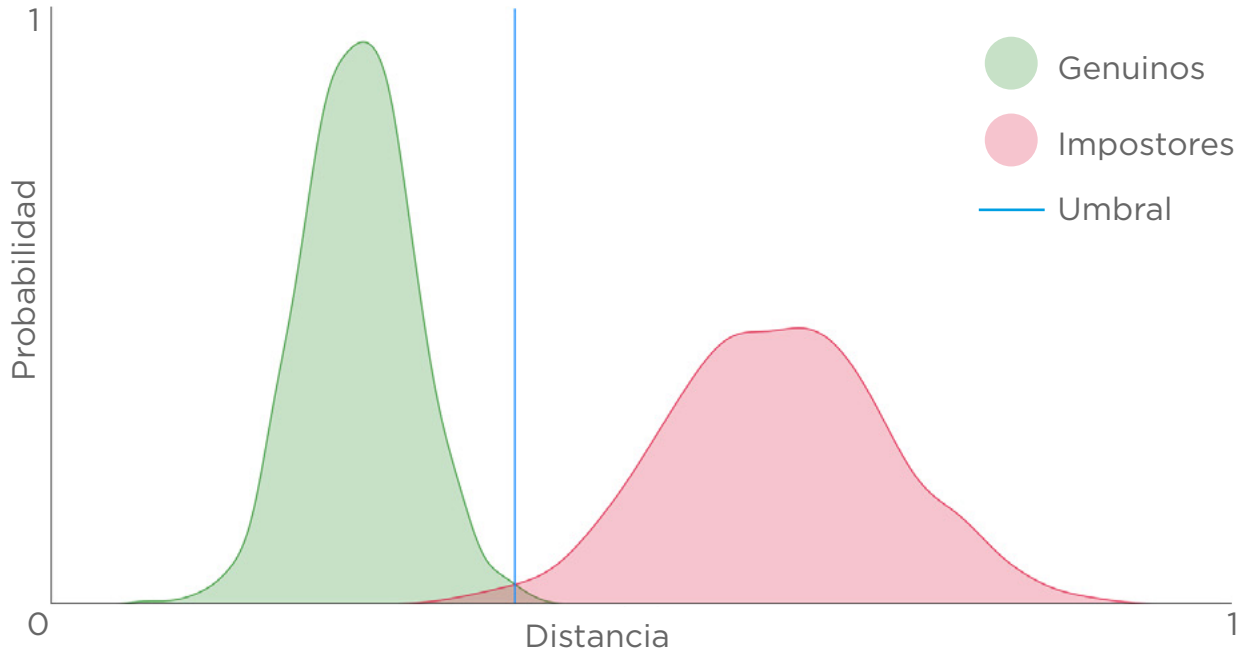


En este ejemplo, el umbral se definió de tal forma que no hubiera genuinos rechazados. Sin embargo, se puede observar que se registra un conjunto de impostores que será aceptado por el sistema por haber obtenido valores inferiores al umbral.

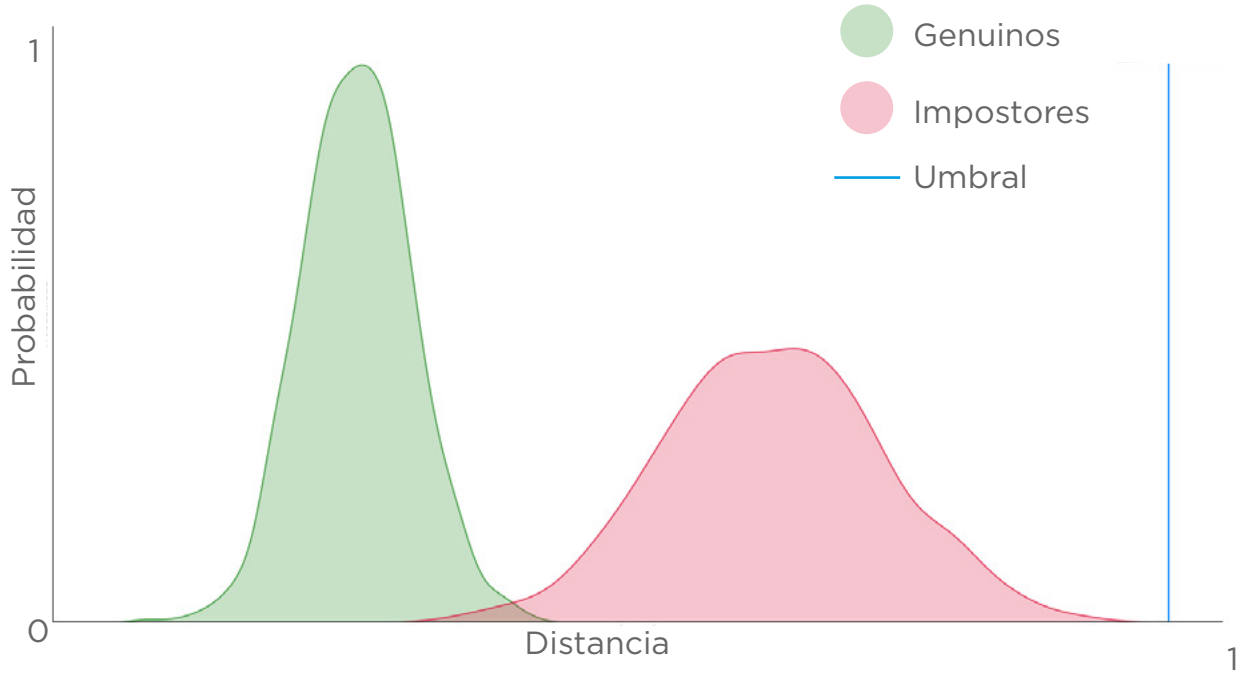
Ahora, si el umbral se fija de forma tal que se rechacen todos los impostores, también habrá genuinos que resulten rechazados debido a que su distancia es superior al umbral:



Dado que es muy probable que los conjuntos no puedan separarse completamente (como ocurre en este ejemplo), siempre existirá un **compromiso** en el momento de definir el umbral, ya que habrá una zona de intersección donde no será posible determinar si pertenecen a una clase o a la otra.

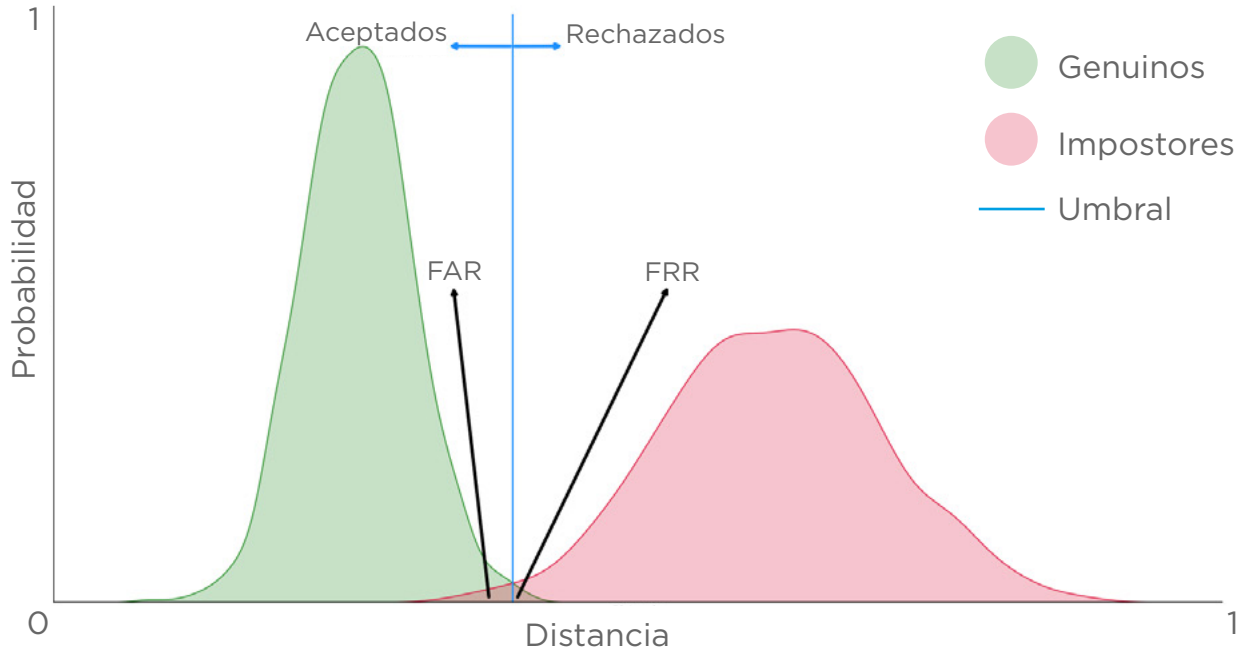


Ahora bien, ¿por qué carece de sentido hablar de que un sistema tiene un error de uno en un millón? Porque dependiendo donde se ubique el umbral, cualquier sistema puede tener esta tasa de error:



Un sistema así configurado tiene muy poco sentido ya que, si bien no aceptará falsos impostores, tampoco aceptará muchos genuinos. Por lo tanto, es necesario ver el escenario completo y evaluar siempre ambas tasas de error, a saber, no solo las falsas aceptaciones sino también los falsos rechazos:

- **Tasa de falsas aceptaciones** (FAR por la sigla en inglés de False Acceptance Rate): Del total de pares de comparaciones que corresponden a distintas personas, cuántas fueron aceptadas por el sistema.
- **Tasa de Falsos Rechazos** (FRR por la sigla en inglés de False Rejection Rate): Del total de pares de comparaciones que corresponden a la misma persona, cuántas fueron rechazadas por el sistema.



Definición: La **tasa de falsas aceptaciones** (FAR) es la proporción de comparaciones que corresponden a distintas muestras pero que fueron aceptadas por el sistema (ISO/IEC 2382).

Definición: La **tasa de falsos rechazos** (FRR) es la proporción de comparaciones que corresponden a la misma muestra pero que fueron rechazadas por el sistema (ISO/IEC 2382).

Además de estas dos medidas, se suele reportar también la tasa de verdaderos positivos (TAR por True Acceptance Rate o GAR por Genuine Acceptance Rate). Esta tasa se puede obtener directamente de la tasa de falsos rechazos, ya que TAR = 1 - FRR.

Definición: La **tasa de verdaderos positivos** (TAR) es la proporción de comparaciones que corresponden a la misma muestra y que fueron aceptadas por el sistema (verdadera aceptación)[9].

En la práctica se puede definir más de un umbral. De hecho, si bien un umbral marca una frontera de decisión, las reglas para manejar cada frontera pueden ajustarse para los distintos casos de uso. Por ejemplo, un sistema puede definir un umbral mínimo y un umbral máximo (el umbral mínimo será siempre menor que el umbral máximo). Si la distancia es menor que el umbral mínimo, se asume que las dos muestras son iguales; si la distancia es mayor que el umbral máximo, se asume que son diferentes. Si, por el contrario, la distancia cae en el medio, no se toma una decisión automática sino que se adopta un camino alternativo (por ejemplo, que la comparación sea revisada en forma manual por un operario).

En resumen, un sistema biométrico siempre debe analizarse en el contexto o bajo las condiciones en las que va a ser utilizado.

Como se indicó anteriormente, la definición del umbral es muy relevante cuando se diseña un sistema biométrico. Esto se conoce como el **punto de funcionamiento** del sistema y determina la tasa de falsas aceptaciones y de falsos rechazos que allí se registre.

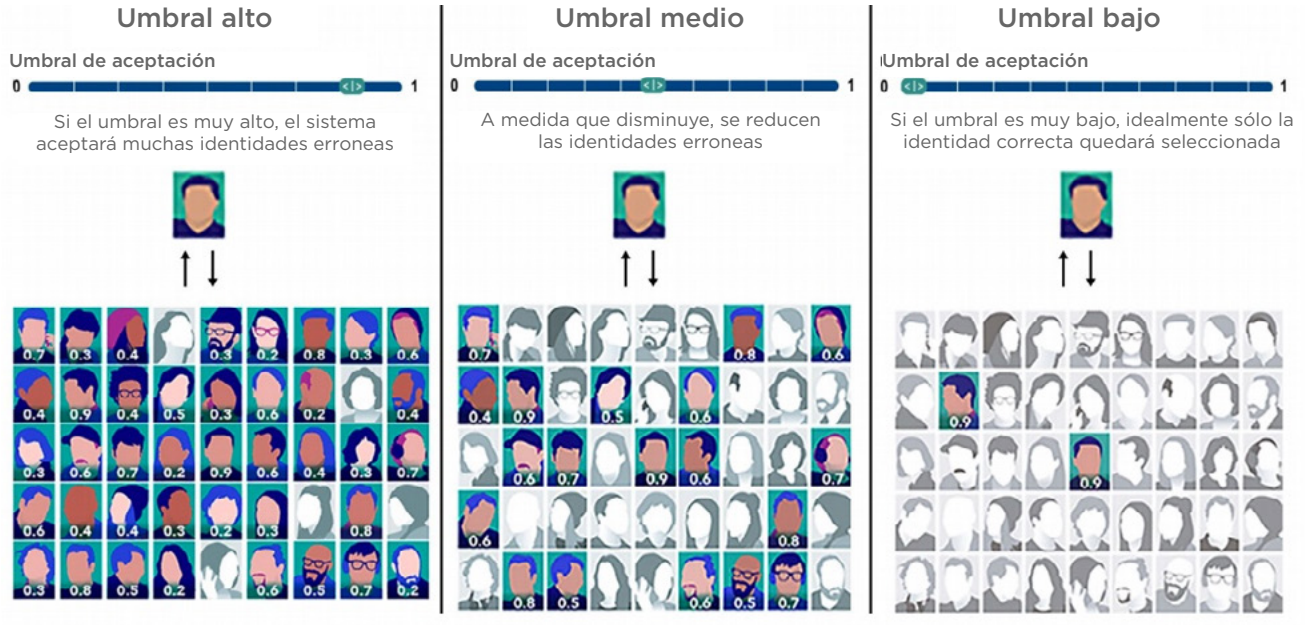
9 No existe definición de **tasa de verdaderos positivos** en el estándar ISO/IEC 2382. Se incluyó la que usualmente aparece en la literatura.

Sin embargo, diferentes escenarios pueden requerir **puntos de funcionamiento** completamente distintos, como se indica en los ejemplos a continuación:

- En el diseño de un sistema biométrico para registrar la entrada y salida de los empleados, tiene sentido que no haya una tasa muy baja de falsos rechazos; en caso contrario se produciría una gran frustración en los empleados, al no poder marcar su ingreso o egreso. En un sistema biométrico utilizado para que el usuario autentique su identidad en su celular también se buscará que la tasa de falsos rechazos sea baja, pues se trata de que su experiencia con esa tecnología sea satisfactoria (no lo sería si para un número importante de intentos el sistema no lo reconoce).

- En el momento de renovar el pasaporte se buscará que haya un alto grado de seguridad para garantizar que la persona que está haciendo el trámite sea la misma que está registrada. En este caso, lo ideal sería que la tasa de falsas aceptaciones sea muy baja, aunque haya más falsos rechazos (un falso rechazo puede ser atendido por otras vías).

Puede ocurrir también que existan distintos puntos de funcionamiento para operaciones diferentes dentro del mismo sistema. A modo de ejemplo, en un sistema de identificación ciudadana, lo deseable será que, durante el proceso de renovación del documento, el sistema biométrico tenga una tasa de falsas aceptaciones muy reducida, para lo cual se usará un umbral bajo. Sin embargo, en el proceso de registro por primera vez (enrolamiento), lo deseable será que la identificación (la búsqueda 1 a N en la base de datos para evitar duplicados) no deje pasar a nadie que sea "parecido". Esto implica tener una tasa baja de falsos rechazos, para lo cual será necesario fijar un umbral más alto.



Fuente: https://partnershiponai.org/paper/facial-recognition-systems/

CONTENIDO AVANZADO

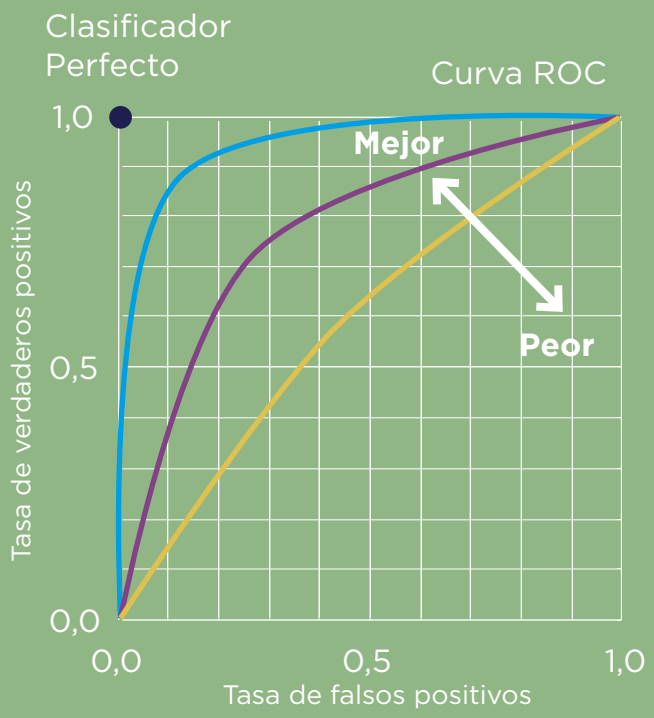
¿Cómo se determina el desempeño de un sistema biométrico en la práctica?

Un punto importante de la discusión anterior es que el desempeño de un sistema biométrico no depende solo del sistema mismo o de los algoritmos utilizados; los datos sobre los cuales se utiliza el sistema son también muy relevantes. ¿Cómo hacen entonces los proveedores de sistemas biométricos para reportar su desempeño? Lo analizan utilizando bases de datos biométricas previamente obtenidas. El método tradicional es el siguiente:

1. Se cuenta con una base de datos biométrica donde cada persona tiene al menos dos muestras biométricas almacenadas para la misma característica (por ejemplo, dos muestras del pulgar derecho o dos imágenes del rostro).
2. Para cada persona se toma una muestra y se la asigna a un conjunto (que en el lenguaje biométrico suele llamarse **galería**) y con la otra muestra se construye otro conjunto (llamado **de consulta**). Es decir, cada conjunto tiene una única muestra por persona.
3. Se toman todas las muestras de la base de consulta y se las compara contra todas las de la base galería. Como en el momento de realizar la prueba se conoce la base de datos, se puede saber qué comparaciones fueron con pares de la misma persona y cuáles no.

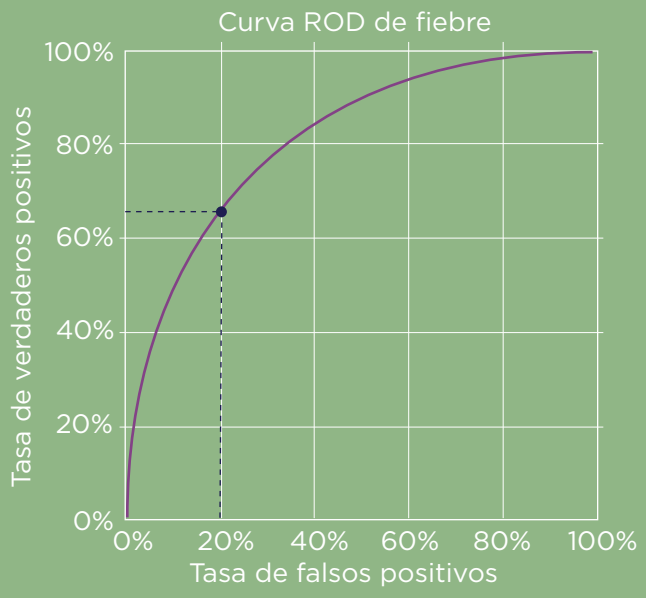
Al final del proceso se tienen pares de muestras (algunas correspondientes a la misma persona y otras no) con un puntaje asociado. Si se fija un umbral para este último a partir del cual todos los puntajes mayores se consideren como pertenecientes a la misma persona (y por ende, todos los menores a personas distintas), se puede entonces calcular el error que comete el sistema: del total de comparaciones hechas con pares de la misma persona, se determina cuántos superan el umbral y cuántos no.

Nótese que la cantidad de pares aceptados o rechazados dependerá del umbral utilizado. Para determinar la precisión de un sistema, se define un umbral que recorre en forma discreta todos los posibles valores del puntaje o de la distancia, y por cada valor se cuentan la cantidad de falsos positivos y de verdaderos positivos. Finalmente se construye una curva donde se muestra cómo varía la tasa de verdaderos positivos con respecto a la tasa de falsos positivos. Esta curva se conoce como ROC por la sigla en inglés de Receiver Operating Characteristic (Característica Operativa del Receptor en español):



En este ejemplo se tienen tres sistemas distintos (líneas naranja, morada y azul). Analizando la curva ROC se puede observar que uno de ellos —el azul— es siempre mejor que los otros dos.

Entonces, si se quiere que el sistema funcione con una tasa de falsas aceptaciones determinada, se puede establecer cuál será la tasa de verdaderos positivos asociada buscando simplemente el punto correspondiente. En el siguiente gráfico, para una tasa de falsas aceptaciones del 20% se puede observar que el sistema tendrá una tasa de verdaderos positivos cercana al 60%.



Caso de uso: India

Con más de 1.295 millones de personas registradas, el sistema de identidad de India —conocido como Aadhaar— es quizás el más grande del mundo (https://uidai.gov.in/aadhaar_dashboard). Este se encuentra sólidamente anclado en el uso de la biometría, no solo para asegurar la unicidad de la base de datos (durante el enrolamiento), sino también para el proceso de autenticación.

Durante el enrolamiento se toman las huellas dactilares y los dos iris de los individuos, de manera que se garantice la unicidad en la base de datos de casi 1.300 millones de personas (una sola biometría podría presentar problemas de unicidad debido a la gran cantidad de registros).

Una característica particular del caso indio es que el sistema no emite ningún documento de identidad: la forma en que se identifican los individuos es mediante la verificación biométrica,[10] siendo la huella dactilar el mecanismo más utilizado. Y si bien esto ofrece grandes beneficios (la eliminación de los costos asociados con la entrega de cerca de 1.300 millones de tarjetas de identidad y de la exigencia de que los ciudadanos porten el documento consigo para todas las transacciones), también presenta grandes desafíos.

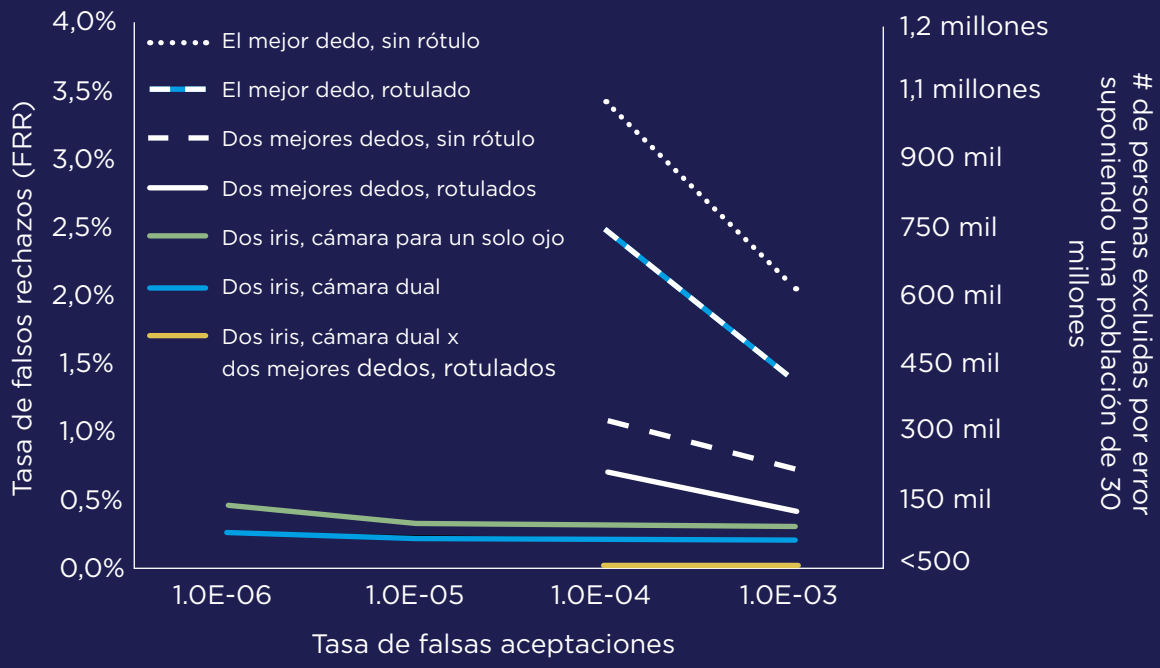
En un informe sobre los datos operativos del sistema publicado por la agencia de identidad india en 2012 (UIDAI, 2012) con base en 84 millones de personas, se mostró que la tasa de fallas de enrolamiento era de 0,14% y la de falsos positivos en la identificación del 0,057%. En términos prácticos, esto quiere decir que de cada 100.000 personas registradas por primera vez en el sistema, solo 57 casos tuvieron que ser revisados manualmente en busca de duplicados. Por otro lado, la tasa de verdaderos positivos (también en identificación) fue del 99,965%, lo cual indica que del total de registros duplicados, el 99,965% de estos fue detectado. En otras palabras, de cada 100.000 registros duplicados, el sistema solo dejo de detectar 35.

Los enormes beneficios que ha conllevado el uso de sistemas biométricos para el enrolamiento de una población tan numerosa son indudables. Ahora bien, India también es única en el sentido de que no emite ninguna tarjeta de identidad: solo un número. Aquí el gobierno indio se apoyó igualmente en la biometría para autenticar la identidad de los individuos.

El uso de la biometría para el proceso de autenticación presenta numerosos desafíos que lo diferencian del que se emplea para el enrolamiento. Por un lado, el ambiente donde se realiza el primero no es el mismo que aquel en que se lleva a cabo el segundo. En el enrolamiento se utilizan por lo general equipos de mejor calidad y más costosos, los cuales son manejados por personal capacitado para obtener buenas capturas biométricas en el tiempo necesario para garantizar su calidad. En cambio, en un proceso de autenticación donde el objetivo tanto del cliente como del operario es otro, todos estos elementos se degradan. Aquí los equipos son más económicos dado que se requieren en numerosos lugares, mientras que los operarios a cargo carecen de la experiencia requerida, de modo que ni ellos ni los clientes tienen el tiempo suficiente para hacerlo de forma adecuada. Todo lo anterior conduce a que el desempeño en autenticación se degrade de manera significativa, como se ilustra en la siguiente figura (Gelb y Clark 2013):

10 En los últimos años se agregó la posibilidad de verificar la identidad mediante un aplicativo en el móvil.

DET (Detection Error Tradeoff) = tasa de falsas aceptaciones (FAR) versus tasa de falsos rechazos (FRR) de iris y huellas dactilares



Dependiendo de la tasa de falsas aceptaciones, se puede observar que la tasa de falsos rechazos puede llegar a ser hasta de un 3,5%. Es más, estos errores tienden a ser sistemáticos ya que ocurren con mayor frecuencia en determinados sectores de la población: personas mayores, personas que realizan trabajos manuales, etc.

Son numerosos los artículos en los cuales se analizan las ventajas y desventajas del modelo indio. Sin embargo, aquí no se intenta hacer una reseña exhaustiva de la literatura, ni determinar si la tasa de falsos rechazos es de 3,5%, como se indicó anteriormente (Gelb y Clark, 2013), o del 10%, como se registra en otra fuente (Muralidharan, Niehaus, y Sukhtankar, 2020) De todas maneras, hay dos elementos en los que se puede estar de acuerdo: primero, que la única forma segura de garantizar la identidad correcta en un conjunto tan grande de personas es mediante el uso de información biométrica, y segundo, que el uso de la biometría en la autenticación para la entrega de beneficios sociales debe ser analizada con extremo cuidado, sopesando seriamente sus pros y sus contras.

1.5 Almacenamiento

Dado que un sistema biométrico no deja de ser un sistema de información, allí aplican todos los métodos y mecanismos tradicionales de almacenamiento de datos. En particular, es usual que los sistemas biométricos utilicen sistemas de bases de datos existentes.

Como se indicó anteriormente, los sistemas biométricos realizan sus operaciones principales de verificación e identificación utilizando las plantillas biométricas generadas. Esto quiere decir que un sistema biométrico podría funcionar sin almacenar la muestra biométrica original. Sin embargo, dado que por lo general no es posible recuperar la muestra biométrica original a partir de la plantilla, es usual que los sistemas biométricos almacenen tanto la muestra como la plantilla. Esto es útil, por ejemplo, para realizar una inspección visual de la muestra biométrica cuando existan dudas acerca del resultado de la comparación.

Los datos biométricos son en general considerados datos sensibles, ya que están ligados directamente a la persona. Es así como los sistemas biométricos buscan proteger estos datos de los diferentes ataques que un sistema informático pueda sufrir. Una descripción detallada de los tipos de ataques, y de las medidas preventivas que se pueden implementar para minimizarlos, se encuentra más adelante (numeral 1.8).

>Almacenamiento centralizado o distribuido

A la hora de almacenar datos biométricos, otro elemento de diseño importante es si aquellos se guardan en forma centralizada o distribuida. Un sistema de base de datos centralizada almacena la totalidad de sus datos en un solo lugar físico, mientras que en un sistema distribuido los datos se depositan en múltiples equipos. Dependiendo del tipo de sistema, y del tipo de operaciones a realizar, será más adecuada una modalidad u otra. En cualquier caso, un criterio básico de seguridad y privacidad (que se describe en detalle en el numeral 1.8) es el de la minimización de datos: cuanto menos dato haya en un sistema, menor será el impacto de una vulneración de seguridad. Así pues, independientemente de si el esquema es centralizado o distribuido, se recomienda minimizar no solo la información capturada sino, obviamente, las copias que existan más allá de los requerimientos básicos de copias de seguridad y redundancia[11].

El esquema distribuido es particularmente adecuado para operaciones de verificación de identidad. Este es el caso de los celulares que se autentican mediante reconocimiento facial, y de los documentos de identidad con aplicativos de tarjeta con circuito integrado o chip (Match-on-Card). En ambos casos, solo la información biométrica del titular se mantiene en el sistema —que además nunca sale del dispositivo—, con lo cual se minimizan los riesgos de acceso no autorizado a esos datos.

1.6 Interoperabilidad

Todos los pasos descritos anteriormente forman parte de un sistema biométrico básico. Ahora bien, estos pasos por lo general se implementan con módulos o componentes de software específico, distribuido por distintos proveedores, entre los cuales figuran fabricantes de sensores biométricos y desarrolladores de generadores de plantillas biométricas (o de

11 La redundancia hace referencia al sistema de almacenamiento que usa múltiples discos duros o SSD entre los que distribuyen o replican los datos.

comparación de las mismas). Incluso si todo el sistema fuese suministrado por un único proveedor, podría existir la necesidad de interactuar con otros sistemas biométricos externos.

Por qué es necesaria la interoperabilidad: ejemplos

Pasaporte electrónico: Los pasaportes electrónicos tienen un chip donde se almacenan datos relativos a su titular. En general, estos datos serán los mismos que los que se registran en la hoja de datos: nombres, apellidos, fecha de nacimiento, etc. Además, se incluye la versión digital de la fotografía de la persona. Muchos países han implementado los llamados eGates o cruces fronterizos automáticos. Estos sistemas cuentan con un mecanismo de puertas automáticas, acompañadas de un lector de pasaportes y de una cámara fotográfica. Cuando el usuario quiere pasar a través de estas puertas, coloca el pasaporte en el lector y el sistema lee la imagen almacenada en el chip. Luego toma una fotografía de la persona, que compara con la que está almacenada en el chip.

Dado que el fabricante de pasaportes no tiene por qué ser el mismo que el de los eGates —además de que un eGate deberá funcionar con pasaportes de variados países—, para poder realizar esta operación se necesita que tanto el pasaporte como los eGates sigan un conjunto de recomendaciones y estándares, sin los cuales aquella sería inviable. Esto se logra siguiendo las especificaciones del estándar de la Organización de Aviación Civil Internacional (OACI) en particular la serie 9303[b], que fue aprobada como estándar ISO 7501[c].

Match on Card (MoC): Otro ejemplo de interoperabilidad es Match on Card (comparación en la tarjeta). MoC es un aplicativo que se puede instalar en un documento electrónico y que permite comparar dos plantillas biométricas de huellas dactilares, con la particularidad de que dicha comparación se realiza en el propio chip —o circuito integrado— del documento electrónico. Esto no solo requiere que haya interoperabilidad para interactuar con el aplicativo del chip, sino que además exige definir el formato de la plantilla de huellas a enviar al aplicativo. En este caso también existe un estándar que define el formato de dicha plantilla: ISO/IEC 19794-2.

[a] ICAO por sus siglas en inglés.
[b] https://www.icao.int/publications/pages/publication.aspx?docnum=9303
[c] https://www.iso.org/standard/45562.html

La interoperabilidad entre diferentes sistemas requiere que exista un conjunto de estándares relacionados con la biometría que conviene tener en cuenta. Una lista completa de los más importantes se encuentra en el Anexo.

Un punto relacionado con la interoperabilidad que incide en el diseño de un sistema biométrico tiene que ver con el tipo de interacciones que ocurren entre los distintos componentes, en particular lo que atañe a la transferencia de datos biométricos. En el numeral 1.8 se encuentra un análisis detallado de los elementos de seguridad a considerar.

1.7 Tipos de errores de un sistema biométrico

Como se indicó anteriormente, un sistema biométrico realiza un conjunto de pasos para completar sus operaciones básicas. Independientemente de si se trata de una tarea de verificación o de identificación, el sistema debe primero capturar la muestra biométrica, generar luego la plantilla, comparar las plantillas y finalmente tomar una decisión. En cada uno de estos pasos pueden ocurrir errores que afectan el funcionamiento correcto de todo el sistema. A modo de ejemplo, una imagen de mala calidad generará una plantilla igualmente deficiente. Esto incide finalmente en la comparación de plantillas, arrojando medidas que no son confiables.

Sin embargo, en el momento de analizar los distintos tipos de errores de un sistema biométrico, es importante estudiar aquellos que están intrínsecamente relacionados con el objeto de medición, en este caso los rasgos biométricos.

>Errores propios del reconocimiento biométrico

De todas las características deseables en un sistema biométrico, existen dos que son de particular relevancia: el carácter único del rasgo biométrico y su **permanencia** en el tiempo (o por lo menos en el tiempo definido por el sistema como deseable). Estas dos premisas no son verdaderas en general; existen, por ejemplo, personas distintas que tienen rasgos faciales muy parecidos, y también personas que han cambiado mucho en unos pocos años.

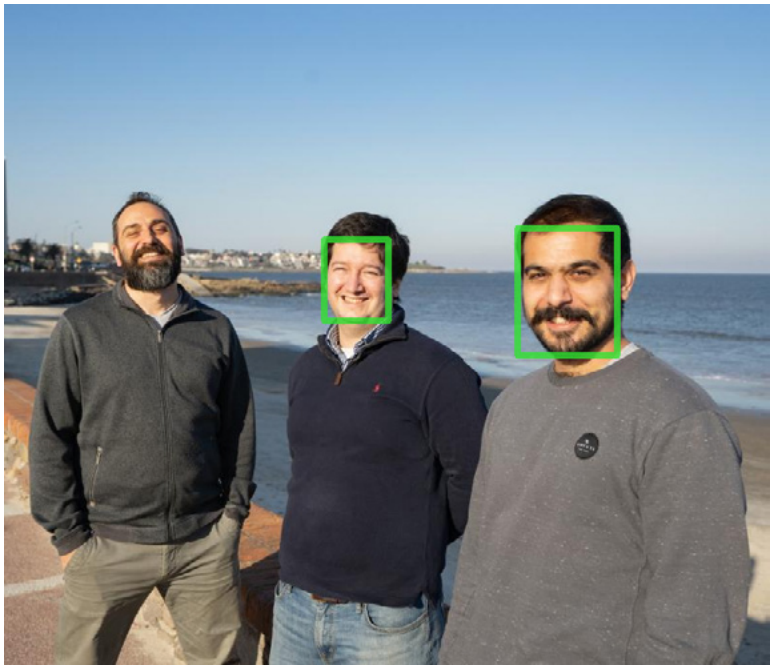
Por todas estas razones, no se puede esperar que dos rasgos biométricos tomados en dos instantes distintos sean iguales. De hecho, un resultado de comparación perfecto (por ejemplo, que la distancia entre las dos muestras sea 0) en realidad indicaría un posible intento de engañar al sistema. Esta es una diferencia fundamental entre un sistema basado en la biometría y otros mecanismos de identificación como son, por ejemplo, las contraseñas o los números de identificación personal o PIN (por su sigla en inglés).

>Error en la captura

Los errores relacionados con el módulo de captura se conocen como **errores de adquisición** o FTA (por las siglas en inglés de Failed to Acquire). Dentro de este tipo de error se incluye el error al detectar el rasgo biométrico o FTD (por las siglas en inglés de Failure to Detect). Este ocurre cuando el equipo de captura no reconoce que hay una muestra que se debe adquirir, mientras que el **error en la captura** o FTC (por las siglas en inglés de Failure to Capture) se presenta cuando el equipo de captura detecta que hay algo que se debe adquirir, pero no logra capturarlo.

A modo de ejemplo, un error de detección o FTD ocurre cuando un escáner de huellas dactilares no logra registrar que allí hay un dedo apoyado, en cuyo caso el aparato ni siquiera se activa. Por otro lado, un error de captura o FTC ocurre, por ejemplo, cuando el escáner detecta que hay un dedo, pero este puede presentar problemas de excesiva humedad o sequedad, entre otros, impidiendo así su captura.

En la siguiente imagen se puede observar un ejemplo, esta vez en un sistema de reconocimiento facial. El sistema logra detectar dos rostros, pero queda un tercero sin detectar, produciéndose un error en la adquisición.



>Error en el enrolamiento

El **error en el enrolamiento** (FTE por las siglas en inglés de Failure to Enrol) ocurre cuando no se puede generar la plantilla biométrica correspondiente a la muestra biométrica capturada. Cabe notar, sin embargo, que esta denominación no es del todo correcta, dado que este error no ocurre solo en el momento de enrolar, sino siempre que se procesa una muestra biométrica. Esto por cuanto la generación de la plantilla biométrica es un paso previo a cualquier operación (identificación y verificación). En la siguiente imagen se observan tres muestras biométricas que, debido a su mala calidad, fallaron en su intento de crear la plantilla biométrica respectiva (huella muy seca, muy húmeda o con varias cicatrices).

Seco Húmedo Con cicatrices

>Error en la verificación

Como se indicó anteriormente, en el proceso de verificación se comparan dos muestras biométricas con el objetivo de determinar si tienen el mismo origen, de lo cual se obtiene un resultado binario: se acepta o se rechaza la comparación. Aquí los errores pueden ser dos: el falso rechazo biométrico, conocido también como FRR (por False Rejection Rate) o FNMR (por False Non-Match Rate), o la falsa aceptación biométrica, que también se conoce como FAR (por False Acceptance Rate) o FMR (por False Match Rate).

CONTENIDO AVANZADO

Sutilezas semánticas importantes

Aunque en la literatura por lo general se utilizan FAR y FMR de forma indistinta, en el estándar ISO/IEC 19795 se marca la diferencia entre uno y otro: FMR se utiliza a nivel del algoritmo biométrico utilizado, mientras que FAR se analiza a nivel de todo el sistema. Se trata de una sutileza semántica que vale la pena tener en cuenta.

>Error en la identificación

El proceso de identificación no consiste en verificar una identidad; lo que se busca es determinar si una persona está en la base de datos a partir de una muestra biométrica. Es usual que en este tipo de búsquedas se retorne más de un resultado (por ejemplo, los 10 más cercanos, es decir, los que se encuentran a menor distancia de la muestra biométrica de la búsqueda). En cualquier caso, el sistema retornará un conjunto de posibles candidatos (eventualmente con uno o ningún elemento).

Los errores que el sistema puede cometer son los siguientes:

- **Falsa identificación biométrica positiva.** Dada una muestra biométrica de una persona que NO está en la base de datos, el sistema la identifica erróneamente con una o varias de las allí registradas. Esto se conoce como FPIR por las siglas en ingles de False Positive Identification Rate.
- **Falsa identificación biométrica negativa:** En la lista de candidatos que arroja el sistema no se encuentra la persona acerca de la cual se consultó, aunque esta sí figura en la base de datos. Esto se conoce como FNIR (por las siglas en inglés de False Negative Identification Rate).

Caso de Uso: Seguridad Pública (Reino Unido)

Una de las aplicaciones de la biometría que genera más preocupación es el uso del reconocimiento facial en los sistemas de seguridad pública y de vigilancia por video. El Reino Unido ha sido pionero en esta última modalidad, llegando a tener en Londres cerca de un millón de cámaras (se estima que, en promedio, una persona es vista unas 300 veces al día).

Entre los años 2016 y 2019, la policía metropolitana realizó un conjunto de pruebas en su sistema de reconocimiento facial en vivo o LFR (por Live Facial Recognition). En total se completaron 10 pruebas durante procedimientos operativos reales. En las últimas seis pruebas se permitió la participación de un conjunto de investigadores independientes (Fussey y Murray, 2019). Durante las pruebas, el sistema emitió 42 alertas, de las cuales finalmente solo ocho resultaron correctas, siendo la tasa de verdaderos positivos solo del 19,05%. En otras palabras, cuatro de cada cinco alertas resultaron equivocadas.

En principio parece un muy mal resultado. Sin embargo, es importante entender la dificultad de identificar a una persona en una población de varios millones de individuos a partir de imágenes en situaciones no controladas (lo que en inglés se conoce como on the wild). Ahora bien, si se piensa desde otro punto de vista, lograr detener a ocho personas requeridas por la justicia en 42 intentos no es un resultado tan malo.

La utilización de la biometría en el campo de la seguridad pública genera otros cuestionamientos éticos que vale la pena mencionar, ya que hacen parte de un encendido debate que involucra, por un lado, la seguridad, y por otro, las libertades individuales. El riesgo de que un sistema de reconocimiento facial montado sobre un conjunto de cámaras desplegadas en toda una ciudad sea utilizado para seguir, monitorear y vigilar a una determinada persona es real. La forma de dar garantías a la población es a través de buenas políticas de manejo de sus datos personales, con claros protocolos de uso y con la transparencia suficiente. Por eso, a la hora de desplegar sistemas biométricos, el marco legal y su cumplimiento son sumamente importantes.

1.8 Seguridad en los sistemas biométricos

Dentro de las consideraciones más importantes en el momento de diseñar un sistema biométrico figuran todos los aspectos relacionados con la seguridad. Es usual que las regulaciones de protección de datos califiquen los datos biométricos como “sensibles”, es decir, como sujetos a un tratamiento especial.

En la medida en que son sistemas de información, los sistemas biométricos pueden sufrir todos los tipos de ataques que afectan a cualquier otro sistema de información. Sin embargo, existe un conjunto de amenazas que le es propio, en particular en el módulo de captura. La relevancia de este punto es tal que existe un estándar específico para analizar los tipos de riesgo y las medidas de protección en ese módulo (ISO/IEC 30107).

>Módulo de captura

Los ataques al módulo de captura son los más comunes, ya que este es el componente del sistema que está en directo contacto con la persona. Por eso se conocen por lo general como ataques de presentación. Los tipos de ataques de presentación más comunes son:

- **Asumir la identidad de otro (*impersonation*):** Este tipo de ataque ocurre sobre todo en biometrías de tipo conductual, donde el atacante se hace pasar por otra persona: firma y voz son los ejemplos más claros. En principio, el uso de biometrías físicas de índole no conductual puede ayudar a reducir estos ataques.
- **Ofuscación:** Este ataque incluye cualquier cambio en los rasgos biométricos del atacante para que no pueda ser detectado en el sistema. Es decir, el objetivo del ataque no es en este caso hacerse pasar por otro, sino no ser identificado por el sistema. Un ejemplo de ello es cuando una persona daña o altera sus huellas dactilares para no ser identificada.
- **Suplantación (*spoofing*):** Este es quizás el ataque más conocido y ocurre cuando el atacante presenta al sistema una muestra falsa de un rasgo biométrico. La suplantación incluye la presentación de rasgos biométricos artificiales (huellas dactilares de silicona, máscaras, lentes de contacto con la imagen de un iris), así como de rasgos no vivos (un dedo cortado).

>Mecanismo de protección

Suponer que el rasgo biométrico es secreto o solo accesible al dueño del mismo no ayuda cuando se trata de garantizar la seguridad del sistema. Una persona deja sus huellas dactilares en muchísimas superficies a lo largo de un día o la imagen de su rostro en muchas cámaras y páginas web. La forma de protegerse contra este ataque es incluir, en la etapa de captura, mecanismos para detectar la suplantación. El más utilizado es el de protección de suplantación de identidad o *anti-spoofing*. Este consiste en detectar que un rasgo biométrico corresponde a una persona viva y que es esa misma la que está interactuando con el sensor. El mecanismo más utilizado es el de medir signos vitales, lo que también se conoce como "prueba de vida" o *liveness*.

Obviamente, las técnicas de detección de suplantación dependen casi exclusivamente del tipo de biometría que se esté utilizando, así como del tipo de sensor. Por ejemplo, los iPhone tienen un mecanismo de reconocimiento facial para autenticar al usuario basado tanto en la cámara (2D), como en la construcción de una nube de puntos censados en la cámara infrarroja (3D).

Obviamente, el riesgo de suplantación (y por lo tanto las medidas para evitarlo) dependerá mucho del contexto de aplicación. Es obvio que aquellas aplicaciones donde la verificación biométrica se realice **sin** la intervención de un funcionario u operario del sistema requerirán más medidas que uno donde sí interviene una persona. Por ejemplo, en la renovación del pasaporte no es necesario realizar una prueba de vida al tomar la fotografía de la persona, aunque tal prueba sí será indispensable en un aplicativo móvil para realizar transacciones bancarias.

CONTENIDO AVANZADO

Mecanismos de detección de suplantación

Los mecanismos de detección de suplantación pueden agruparse en tres grandes categorías (Jain, Ross y Nandakumar, 2011):

1. **Medición de las características fisiológicas de la persona para determinar si está viva.** Ejemplos de este tipo son, por ejemplo, en el caso de un escáner de huellas dactilares, medir la presión o pulso sanguíneo, la transpiración o las características eléctricas de la piel.
2. **Medición de las características conductuales de una persona viva.** Los ejemplos de este tipo tienen que ver sobre todo con elementos del iris y con el reconocimiento facial: parpadeo, cambios en los gestos, movimientos espontáneos, cambios en la pupila, etc.
3. **Implementación de un mecanismo con requerimientos que deben ser cumplidos por la persona para verificar que está viva.** Ejemplos de este caso en materia de reconocimiento facial serían solicitar al usuario que realice un gesto particular (cerrar un ojo) o que siga la trayectoria de un marcador en pantalla.

Las opciones 1 y 2 no requieren que la persona realice nada especial, como tampoco que sea consciente de que está siendo analizada. Es por esto que tales métodos se conocen como "pasivos". Por el contrario, en la opción 3 sí se requiere la participación de la persona, y aquí los método se conocen como "activos".

Los métodos activos son muy buenos para realizar una prueba de vida satisfactoria, ya que el usuario tiene que realizar las acciones o requerimientos que le plantea el sistema. Sin embargo, pueden no resultar prácticos en todos los casos. Por ejemplo, resultaría muy molesto tener que realizar una serie de acciones cada vez que se quiere acceder al celular. Por eso, a menudo se combinan los métodos activos con los pasivos. Una configuración tradicional es utilizar métodos activos para aquellas acciones que no se realizan con frecuencia.

Por otro lado, las ventajas de los métodos pasivos consisten en que el usuario no sabe cuándo ni cómo se efectúa el control. En algunos sistemas donde la cámara se usa regularmente (por ejemplo en sistemas de conferencia), es posible realizar el control pasivo de prueba de vida a todo lo largo de la interacción del usuario con el sistema.

Por lo general, aquellos sensores y dispositivos que contengan medidas de detección de suplantación serán más costosos que los que carecen de ellos. Esto por cuanto, en muchos casos, es necesario incluir componentes adicionales con el objetivo específico de detectar la suplantación. También es importante resaltar que, al incorporar un nuevo módulo al sistema, se agregan nuevos posibles errores: o bien rechazar una adquisición porque no se pueden detectar los rasgos vitales o bien aceptar una adquisición cuando se trata de una suplantación.

>Almacenamiento

Una base de datos biométrica puede sufrir dos tipos de ataques: ser modificada por un atacante o ser leída por este. Obviamente, el que una base de datos pueda ser modificada por un atacante es extremadamente grave, pues esto básicamente altera la identidad de una persona. Sin embargo, este tipo de ataque no es por lo general el más común.

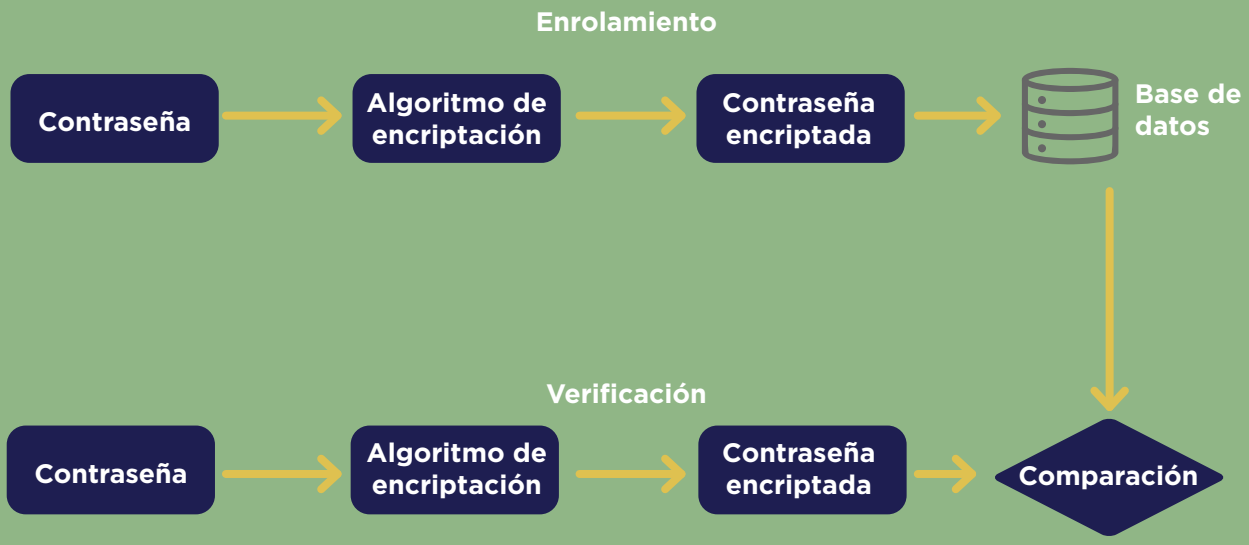
El otro tipo de ataque ocurre cuando el atacante obtiene una copia de los datos biométricos almacenados en la base de datos. Un error común es creer que, porque un individuo accede a los datos biométricos de otro, puede usar esa información para autenticarse como esta segunda persona. En realidad, esto solo funcionará si el sistema que realiza la autenticación no incluye mecanismos de detección de suplantación. De hecho, en el momento de diseñar las medidas de seguridad de un sistema biométrico lo recomendable es asumir que los datos biométricos pueden ser conocidos por personas distintas al titular, y por lo tanto deben incluirse tantas medidas de detección de suplantación como sean necesarias.

No sobra insistir en que los datos biométricos son considerados información sensible, y que por lo tanto la información almacenada en una base de datos biométrica debe ser protegida de ataques a toda costa. Existen mecanismos genéricos que se usan en otros sistemas de información, aunque también hay mecanismos específicos exclusivos para datos biométricos, los cuales se discutirán a continuación. Sin embargo, un criterio básico de seguridad y privacidad que ya se mencionó anteriormente es la minimización de la información capturada.

CONTENIDO AVANZADO

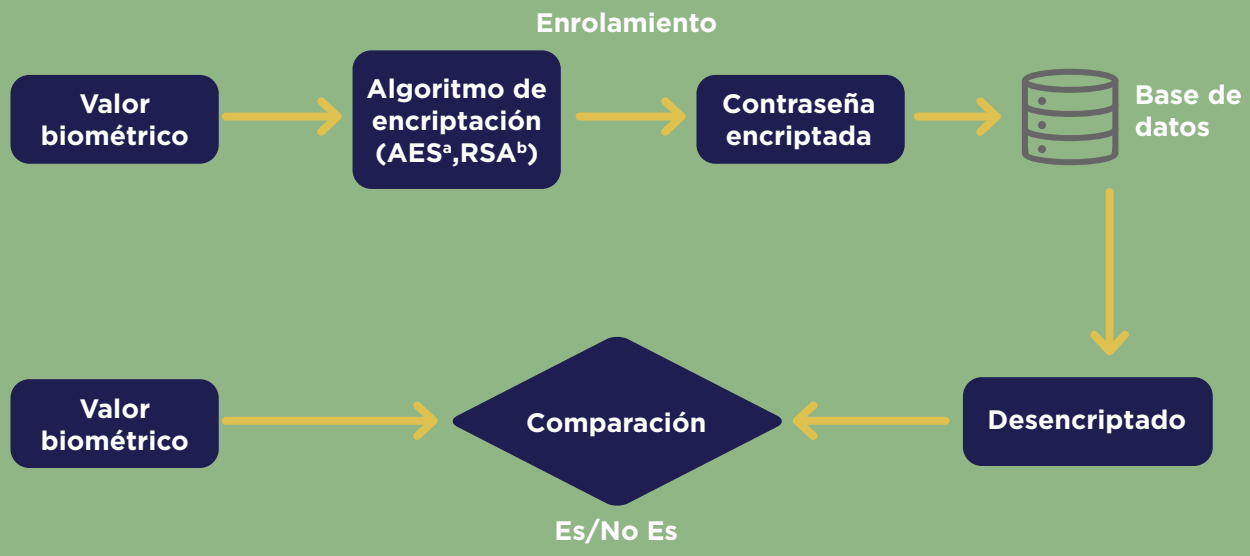
Uso de cifrado para proteger datos biométricos

Uno de los mecanismos más comunes para la protección de datos es la encriptación, que puede estar basada en llave pública o privada. Algunos métodos tradicionales son encriptación RSA[a] y AES[b]. Cuando se utiliza este esquema, solo se almacena el dato encriptado. Tómese como ejemplo el caso de las contraseñas para acceder a un sistema cualquiera. Estas se almacenan encriptadas, y cuando el usuario digita la contraseña para ingresar al sistema se aplica el mismo algoritmo de encriptación, lo cual resulta en un mensaje codificado que puede compararse directamente con el almacenado:



Ahora bien, una de las propiedades deseadas en un algoritmo de encriptación tradicional es que un pequeño cambio en el dato de entrada genere un cambio significativo en el dato encriptado, de forma tal que no se pueda obtener información a partir de intentos repetidos. Esto, sin embargo, presenta un inconveniente significativo para los sistemas biométricos, ya que los datos sujetos a comparación nunca son iguales. Por lo tanto, los datos generados a partir de un algoritmo de encriptación siempre serán distintos y la comparación entre ellos fallará.

Obviamente, la solución a este problema es desencriptar el dato previo a comparar, tal como se ilustra en la siguiente figura:



Los mecanismos de protección tradicionales son ampliamente utilizados en los sistemas biométricos, dado que son muy sencillos de implementar y no afectan el desempeño general de aquellos. Sin embargo, como se requiere desencriptar el dato para compararlo durante las etapas de verificación, esto genera una vulnerabilidad y un punto de ataque en el sistema. Es por ello que se han propuesto otros mecanismos de encriptación específicos para sistemas biométricos, los cuales se describirán a continuación.

Transformación del espacio de las características biométricas

Este tipo de protección se basa en aplicar una transformación a la plantilla biométrica (por lo general con la ayuda de una clave privada) y almacenar solo su resultado. Cuando se la quiere comparar con una nueva muestra biométrica, se aplica la misma transformación y se comparan los resultados. Este mecanismo es exactamente el mismo que el que se emplea para proteger contraseñas. Ahora bien, como se observó en el punto anterior, los métodos de encriptación tradicionales no pueden usarse porque hay datos de entrada similares que generan salidas muy distintas. Lo ideal es que la salida de entradas parecidas sea también parecida. Uno de los métodos para lograrlo es que la transformación genere el mismo tipo de datos que la entrada, es decir que, por ejemplo, una transformación de minucias de huellas dactilares genera otro conjunto de minucias de huellas dactilares.

Encriptación homomórfica y privacidad biométrica

Los métodos de encriptación tradicionales son "no homomórficos". Esto quiere decir que dos muestras biométricas que son muy parecidas antes de encriptar serán muy distintas luego de que se las encripte (es decir, si se compara el dato encriptado). Por esta razón, cuando se utilizan métodos de encriptación tradicionales, es necesario desencriptar los datos para su comparación, generando la vulnerabilidad arriba mencionada.

La encriptación homomórfica es una modalidad que hace que la encriptación de dos muestras muy similares también lo sea, permitiendo que se compare el dato encriptado **sin necesidad de desencriptar**. Este mecanismo de encriptación produce el nivel más alto de privacidad del dato puesto que, una vez encriptado, nunca vuelve a exponerse.

Un ejemplo práctico de encriptación homomórfica es el uso de redes neuronales convolucionales (CNN por sus siglas en inglés) para el reconocimiento facial. Los métodos de reconocimiento facial basados en CNN reciben una imagen y generan una plantilla biométrica. Las redes son entrenadas para que generen estas plantillas de forma tal que concentren las características que hacen a cada rostro único. Así pues, una vez generado el vector, la comparación se realiza en este nuevo espacio.

a https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
b https://en.wikipedia.org/wiki/RSA_(cryptosystem)

>Módulo de comparación

Un punto clave en todo el proceso de verificación biométrica es la comparación de las plantillas para determinar si pertenecen o no a la misma característica. Por lo tanto, el módulo de comparación debe recibir las dos plantillas a comparar. Esto genera posibles puntos de ataque: un atacante puede tratar de sustituir una plantilla por otra.

Otra posible vulnerabilidad es que, como para comparar se deben tener ambas plantillas biométricas, puede ocurrir que un atacante acceda a la original, lo cual es un problema en términos de la privacidad de datos. Una forma de evitarlo es que el módulo de comparación tenga almacenada internamente la plantilla biométrica original y que solo reciba la plantilla a comparar. Obviamente esto restringe el uso del módulo para la operación específica de verificación de identidad fija. Sin embargo, la verificación de identidad es la operación más común en los sistemas biométricos.

Este tipo de verificación, conocido como **verificación en el dispositivo**, es por lo general lo que se implementa con un Match-on-Card incorporado en el chip —o circuito integrado— del documento electrónico o en la verificación de identidad en un celular. En ambos casos, la identidad del titular es conocida y es la única contra la cual se puede comparar la muestra nueva. Las ventajas de este método es que en ningún caso la biometría original se expone fuera del dispositivo (el documento electrónico, el celular, etc.).

Parte II.
Cómo planificar un sistema biométrico

Parte II. Cómo planificar un sistema biométrico

En la parte I se definieron los conceptos más importantes relacionados con un sistema biométrico. En esta segunda parte se abordará una serie de consideraciones prácticas para tener en cuenta en el momento de planificar un sistema biométrico.

2.1 Entender el contexto

>Entender el universo de aplicación del sistema que se va a implementar

Para entender el universo de aplicación, el primer paso consiste en determinar cuál es el público objetivo del sistema biométrico. Algunos rasgos biométricos tienen un mejor desempeño para determinado grupo de personas que otros. En general, será necesario tener en cuenta los siguientes aspectos del universo seleccionado:

Edad: El rango de edad en el que debe operar un sistema biométrico puede incidir en el rasgo biométrico a seleccionar. Por ejemplo, los sistemas de reconocimiento facial adolecen de dificultades a la hora comparar rostros de niños y adolescentes.

Tiempo transcurrido: Otro factor que tiene un impacto significativo en los sistemas biométricos es el paso del tiempo entre la muestra almacenada en la base de datos y la que se está comparando. Una forma de minimizar este problema es actualizar el rasgo biométrico ante cada nueva presentación. Sin embargo, esto no siempre es posible y dependerá del caso de uso concreto. Así las cosas, se recomienda capturar los rasgos más estables en el tiempo (huellas dactilares, iris).

Lugar de aplicación: El lugar donde se utilice el sistema biométrico es sumamente importante. En determinados ambientes, algunos rasgos biométricos son más sencillos de obtener que otros. Por ejemplo, el uso del sistema biométrico como mecanismo para registrar el ingreso de operarios de una cantera o construcción es poco recomendable debido a la mala calidad de la huella obtenida (por la suciedad y desgaste de la misma). En estos casos, un sistema basado en reconocimiento facial podría ser más adecuado.

Tipo de operación: Puede ocurrir que no sea necesario implementar todas las operaciones que realiza un sistema biométrico. Por ejemplo, un sistema para dar acceso a un determinado servicio podría requerir solo la verificación de identidad contra un mecanismo ya existente (servicio web de identificación civil o Match-on-Card en el documento de identidad). En este caso, el sistema no necesitará realizar el enrolamiento y/o contar con una base biométrica; solo requerirá la captura de la muestra biométrica durante la verificación de la identidad.

Verificación desatendida: Otro punto para tener en cuenta es si el proceso de verificación se realizará de forma desatendida o no. Por **desatendida** se entiende que para esta verificación no habrá un funcionario u operario que supervise el proceso. En estos casos será más fácil intentar engañar al sistema mediante suplantación, ya que no hay nadie observando al atacante potencial. En estas instancias, los sistemas basados en reconocimiento facial son por lo general más robustos, ya que permiten hacer una “prueba de vida” de forma mucho más eficiente.

Consideraciones culturales: Un aspecto fundamental es que la biometría seleccionada sea aceptada por el público objetivo. Por ejemplo, en algunos países la toma de huellas dactilares está muy mal vista ya que se asocia con criminales. En otros, el uso de huellas dactilares es habitual en el día a día. Por ejemplo, en Uruguay, cuando se implementó el sistema de venta de marihuana recreativa en las farmacias se realizaron varios grupos seleccionados (*focus groups*). Durante el ejercicio los integrantes prefirieron la huella dactilar a cualquier otra forma de verificación de identidad (necesaria para llevar un registro de la cantidad de marihuana adquirida, ya que está limitada).

>Definir el alcance del uso de la biometría

Como se indicó anteriormente, la utilización de sistemas biométricos busca resolver el problema de identificar a una persona en una determinada aplicación o transacción. Esta identificación puede ocurrir en distintas operaciones, por lo cual es importante entender cuándo se requerirá su utilización, ya que no siempre es necesario valerse de la biometría para cumplir con los objetivos de tener un sistema seguro. Nótese, por ejemplo, cómo la mayoría de los bancos permiten realizar una enorme cantidad de transacciones en línea que por lo general no utilizan biometría y se consideran igualmente seguras. Solo para operaciones muy concretas (apertura de cuentas, retiro o giros superiores a un cierto monto) se solicita una verificación biométrica.

En el momento de definir el posible uso de un sistema biométrico, es conveniente hacerse las siguientes preguntas:

1. ¿Es el uso de un sistema biométrico realmente necesario? ¿Existen alternativas? ¿Cuáles son las ventajas y desventajas del sistema biométrico frente a otros mecanismos de identificación?
2. ¿El uso de biometría resolverá el problema a abordar?
3. ¿Cuáles son las características más apropiadas? ¿Qué rasgo biométrico se va a utilizar? ¿Qué tipo de servicios de almacenamiento se van a emplear?
4. Finalmente, ¿de qué forma se va a garantizar la privacidad y protección de los datos biométricos?

Todas estas preguntas deben ser planteadas y respondidas en el momento de analizar el proyecto.

>Cuándo usar un sistema biométrico

En términos generales, la incorporación o no de una solución biométrica debe analizarse con cuidado. Para esto, el ejercicio de pensar las respuestas a las preguntas planteadas en la sección anterior es primordial. Con un propósito meramente ilustrativo, en esta sección se incluirá una breve descripción de los tipos de proyectos en que esta podría ser relevante.

Cuando existan motivaciones para no identificarse. En algunos casos, no reportarse o no quedar registrado puede ser un incentivo para falsificar otros mecanismos de identificación. Por ejemplo, cuando se brinda un beneficio económico, puede haber motivaciones para intentar obtener este beneficio varias veces con distintas identidades. En este caso, el uso de la biometría puede ayudar, aunque se debe tener especial cuidado en no negar el servicio por errores intrínsecos a los sistemas biométricos (analizados en detalle en la Parte I).

Cuando sea necesario llevar un registro a lo largo del tiempo. En algunos proyectos, como por ejemplo los programas de vacunación, es sumamente importante llevar un registro temporal de las dosis aplicadas a cada persona. En general, las personas querrán ser identificadas, pero puede ocurrir que no existan los mecanismos para ello (por ejemplo, que no exista un sistema de identidad nacional). En estos casos, el uso de la biometría permite realizar el seguimiento del programa.

Cuando no haya otras alternativas. En muchos casos no existe un mecanismo formal de identificación. Por ejemplo, para el caso de los refugiados de países en conflicto (UNHCR, 2015), es probable que estos no cuenten con documentos de identidad y que no existan mecanismos sencillos para obtenerlos. Aquí la identificación biométrica es la única forma de generar una identidad que pueda ser utilizada luego, no solo para brindar servicios sino como mecanismo de seguridad (por ejemplo, al trasladarse hacia otros países).

Cabe insistir en que, como se indicó más arriba, un sistema biométrico tiene un alcance muy acotado en cuanto a las operaciones que realiza y por lo tanto no resolverá otros problemas: interoperabilidad, manejo de datos, sistematización, etc. En este sentido, la biometría es un componente de un sistema más amplio en el que se deberá proteger otro conjunto de elementos: humanos, de infraestructura, de gobernanza y operativos, entre otros.

2.2 Seleccionar la característica biométrica a utilizar

Todo sistema biométrico se basa en la captura, procesamiento, almacenamiento y comparación de muestras biométricas. Por lo tanto, a la hora de diseñar un sistema biométrico es importante decidir cuál es la característica o rasgo biométrico (o, si es del caso, más de uno) que se va a emplear (Jain, Ross y Nandakumar, 2011):

Debe ser universal: Toda la población objetivo debe tener el rasgo seleccionado. Esto es importante porque el concepto de universal está restringido al público objetivo.

Debe ser único: El rasgo biométrico debe ser distinto para personas diferentes dentro del público objetivo, pero además la muestra biométrica obtenida también debe ser distinta al compararla con la de otros individuos. Esta aclaración es importante: si bien no hay dos rostros iguales, sí los hay muy parecidos, y en ocasiones lo suficiente como para que un sistema biométrico los considere iguales. Es por ello que a veces se incluye más de un rasgo biométrico para aumentar la probabilidad de que sea único. Tal es el caso del sistema Aadhaar de India, para el cual se toman las 10 huellas dactilares y los dos iris.

Debe ser permanente: El rasgo biométrico elegido debe ser estable en el tiempo, al menos durante el lapso para el cual se ha diseñado el sistema. Existen estrategias para mitigar los problemas que ocasiona la no permanencia del rasgo. Por ejemplo, en un sistema de reconocimiento facial puede ser oportuno actualizar la imagen allí registrada cada cierto tiempo.

Debe ser medible: El rasgo biométrico tiene que ser fácilmente obtenible, procesable y comparable. Esto obviamente dependerá del objetivo del sistema biométrico. En este punto entran en consideración también la disponibilidad de los equipos y sistemas para procesar el rasgo biométrico seleccionado. Por ejemplo, hasta hace pocos años, los sistemas de reconocimiento de iris eran considerablemente más cotosos que aquellos que capturan huellas dactilares.

Desempeño: Es deseable que el sistema biométrico se procese en un tiempo razonable para el uso determinado. Por ejemplo, la comparación basada en ADN puede ser muy segura pero demora mucho tiempo en procesarse.

Debe ser aceptado: Un punto crítico que en ningún caso se debe pasar por alto es si la adquisición del rasgo biométrico es aceptada por el público objetivo. Por ejemplo, en muchos países de América Latina es común usar huellas dactilares como mecanismo usual para probar la identidad. Sin embargo, ya se ha visto cómo en otros esta modalidad no es aceptada por el público, dado que se la vincula a sistemas de identificación de criminales.

El sistema debe ser seguro: Finalmente, es muy importante que el sistema biométrico sea seguro y difícil de vulnerar.

Ninguna característica o rasgo biométrico cumple con todos los criterios listados anteriormente. A continuación, se resumen las biometrías más comunes y se indica hasta qué punto cumplen con los distintos requerimientos (*Scientific American*, 2008):

Características biométricas	**Huella dactilar**	**Rostro**	**Iris**	**Voz**
Grado de peculiaridad	**Alto**	Bajo	**Alto**	Bajo
Grado de permanencia	**Alto**	Mediano	**Alto**	Bajo
Grado de sensibilidad a la captura	Mediano	**Alto**	Mediano	Mediano
Velocidad y costo-eficiencia del sistema	**Alto**	Bajo	**Alto**	Bajo
Grado de aceptación entre el público objetivo	Mediano	**Alto**	Bajo	**Alto**
Grado de dificultad de suplantación	**Alto**	Bajo	**Alto**	Bajo
Tasa de falsos rechazos*	0,4%	1,2-2,5%	1,1-1,4%	5- 10%
Tasa de falsas aceptaciones*	0,1%	0,1%	0,1%	2-5%

*Las tasas de error dependerán del entorno de la prueba, de los sensores utilizados y de la composición de los usuarios en la población

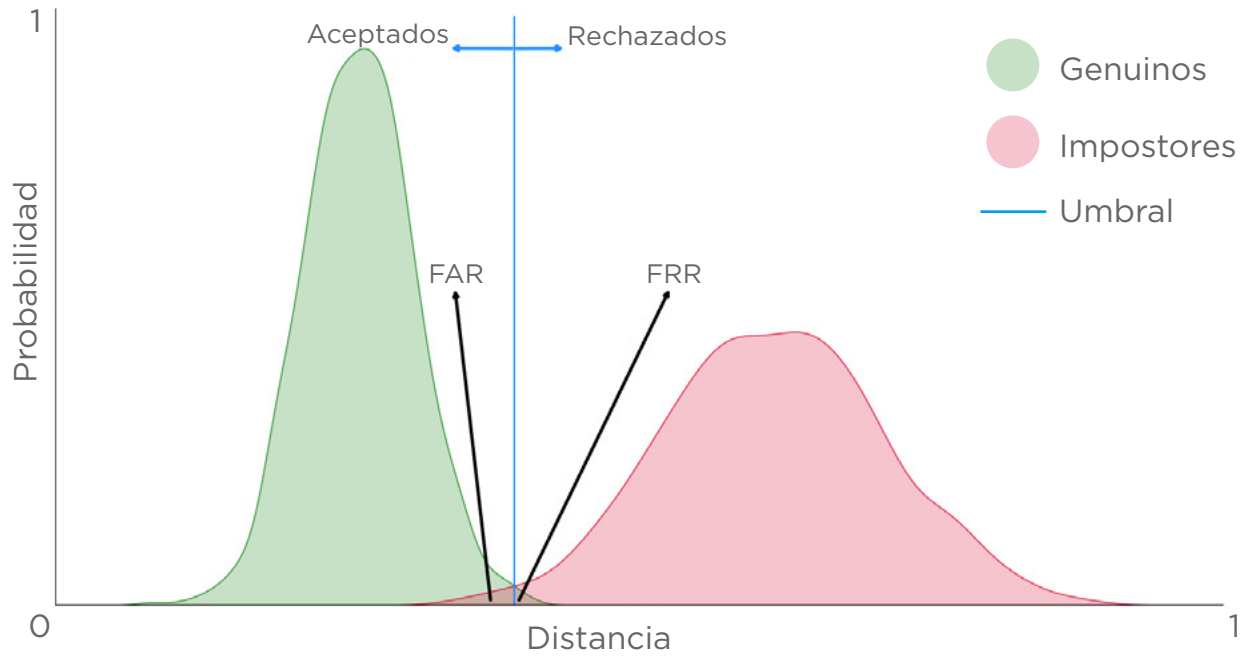
>Multibiometría

Como bien se señaló en la sección anterior, es posible que un rasgo biométrico sea adecuado para las necesidades del sistema en una de sus características, pero no en otras. Puede ocurrir que el rasgo seleccionado sea "casi" universal pero que exista una pequeña porción de la población que no lo tenga o lo pueda adquirir. También puede ocurrir que con un único rasgo biométrico no se logre la precisión deseada. En estos y otros casos posibles, es usual agregar un nuevo rasgo biométrico al sistema: huella dactilar y reconocimiento facial, huella dactilar e iris, etc.

Para obtener el mayor potencial del uso de múltiples biometrías, estas deberán ser utilizadas en forma conjunta. Por ejemplo, en el momento de verificar la identidad se compara tanto la huella dactilar como el rostro de la persona. Para esto se requiere combinar los resultados obtenidos de cada comparación por separado, lo cual se conoce como **fusión biométrica** o **multibiometría**. Es importante aclarar que la fusión biométrica también se realiza cuando, en lugar de agregar un tipo de biometría nueva, se agrega una nueva muestra del mismo tipo de biometría (las huellas dactilares del índice y del pulgar o los iris de ambos ojos). En estos casos, el sistema también aumenta su precisión. Es así como muchos sistemas nacionales de identidad ciudadana y de migración (que tienen que identificar correctamente a una persona entre millones de registros) utilizan las 10 huellas dactilares, dado que la seguridad de una operación de identificación aumenta al agregar huellas en la búsqueda.

2.3 Definir el punto de funcionamiento

En la sección 1.3 se indicó que la comparación entre plantillas biométricas arroja una medida de distancia. Es necesario entonces definir el umbral a partir del cual se decidirá si una comparación es aceptada como perteneciente a la misma muestra biométrica o no:



Una vez definido el umbral, pueden ocurrir dos tipos de error:

- **Falsas aceptaciones:** Cuando dos muestras distintas son aceptadas por el sistema como la misma.
- **Falsos rechazos:** Cuando dos muestras iguales son rechazadas por el sistema como distintas.

En el gráfico anterior se observa que, al mover el umbral en una dirección u otra para disminuir uno de los tipos de error, automáticamente aumenta el otro. Por lo tanto, en el momento de configurar un sistema biométrico resulta crítico entender cuál de estos es el error más relevante. A modo de ejemplo, en un punto de control fronterizo se buscará que la tasa de falsas aceptaciones sea mínima, suponiendo que el aumento en los falsos rechazos puede ser manejado de otra forma. Por otro lado, en un aplicativo de Match-on-Card incluido en un documento de identidad electrónico, será más importante que la tasa de falsos rechazos sea mínima para no frustrar al usuario durante su uso, además de que la seguridad de la transacción aumenta al requerir dos factores de autenticación: poseer el documento de identidad electrónico y verificar la huella dactilar incorporada en el chip.

>Análisis de un sistema biométrico previo a su compra

Ya se señaló en secciones anteriores cómo un sistema biométrico no solo depende de los componentes de software, sino también, y de manera fundamental, de los datos biométricos a utilizar: tanto los almacenados en el sistema como los que se capturarán para comparar. Siendo así, ¿cómo se pueden contrastar sistemas biométricos entre sí? ¿Cómo seleccionar el que mejor se adecue a las necesidades establecidas? Existen al menos dos opciones: analizar los informes de desempeño existentes, y planificar y ejecutar una prueba de desempeño propia.

Analizar informes de desempeño existentes

Es probable que las empresas cuenten con sus propios informes de desempeño. Lo usual es que estos incluyan curvas ROC de donde se puede derivar las tasas de falsas aceptaciones y de falsos rechazos. También es usual que se incluyan cuadros con los valores más usuales. En estos casos, es sumamente importante determinar cómo se realizó la prueba: cuál fue la base de datos y cómo se armó el experimento.

Una segunda fuente de información —mucho más confiable que la anterior— son los informes de desempeño que publican algunas agencias de gobierno o universidades, en los cuales se analizan varios sistemas biométricos. Estos informes tienen la ventaja de ser imparciales y comparables, ya que se ejecuta el mismo protocolo con los mismos datos para todos los sistemas. Uno de los más usados es el de la agencia de normas técnicas de Estados Unidos, el National Institute of Standards and Technology (NIST). Desde hace más de 15 años, este instituto lleva a cabo pruebas de sistemas biométricos: huella dactilar, reconocimiento facial, iris, etc. En la página web del instituto se pueden consultar los resultados de cada una de estas pruebas, junto con toda la documentación técnica para analizarlas: https://www.nist.gov/biometrics. En particular, para reconocimiento facial las pruebas se realizan en forma permanente, dado que para ello se cuenta con un mecanismo en línea: https://pages.nist.gov/frvt/html/frvt11.html.

Cuando se utiliza información existente, es muy importante entender bien cómo se realizaron estas pruebas, pues las hay para analizar cosas distintas. En tal sentido se debe buscar la que mejor se adecue al sistema que se está diseñando (por ejemplo, si el sistema considerado va a adquirir las huellas dactilares de dos dedos, es mejor analizar las pruebas que se han hecho usando dos dedos y no solo uno).

Planificar y ejecutar una prueba de desempeño propia

En esta segunda opción se planifica un conjunto de pruebas utilizando una base de datos existente. Esta base de datos puede ser pública (como las que tiene el NIST[12]), pero más interesante aún es hacerlo sobre uno de los subconjuntos de datos en que el sistema deberá operar. Obviamente, esto no siempre es posible. Si el proceso biométrico es nuevo, muy seguramente no existirán datos sobre los cuales se puedan hacer pruebas. Sin embargo, es posible utilizar esta estrategia si lo que se está haciendo es reemplazar un sistema biométrico existente. En este caso sí se contará con una base de datos biométrica que se pueda utilizar para organizar las pruebas.

>Análisis de un sistema biométrico operativo

Como se explicó anteriormente, el desempeño de un sistema biométrico depende tanto del software como de los datos biométricos utilizados. Dado que estos últimos van cambiando con el tiempo, es muy importante realizar chequeos periódicos del desempeño del sistema biométrico, para verificar que el punto de funcionamiento seleccionado está realmente generando la tasa de falsas aceptaciones y de falsos rechazos esperada. Aquí también, la forma de hacer este análisis consiste en tomar un subconjunto representativo de los datos y realizar las pruebas de verificación e identificación correspondientes.

2.4 Gestión ética de los datos biométricos

La correcta gestión de los datos personales por parte de gobiernos y empresas es fundamental en cualquier sistema de información. Esto abarca obviamente los sistemas biométricos, puesto que sus datos son información personal.

>Consideraciones legales y éticas

Existe un conjunto de estándares y normativas que se deben tener en cuenta a la hora de pensar una solución de biometría, incluso si estos estándares o reglas no aplican en el país o región en la cual se está desarrollando el proyecto. Quizás el más importante de estos marcos sea el Reglamento General de Protección de Datos o RGPD de la Unión Europea (Parlamento y Consejo Europeo, 2016).

RGPD

Este Reglamento General de Protección de Datos (Parlamento y Consejo Europeo, 2016) fue aprobado por la Unión Europea (UE) en abril del 2016 y entró en vigor en mayo de 2018. Con este se busca reforzar y unificar la protección de datos para todos los individuos dentro de la Unión Europea. El RGPD busca dotar a ciudadanos y residentes de control sobre sus datos personales y simplificar el entorno regulador de los negocios internacionales unificando la regulación dentro de la UE.

12 https://www.nist.gov/itl/iad/image-group/resources/biometric-special-databases-and-software

El RGPD define seis principios básicos para la protección de datos personales (Artículo 5: Principios relativos al tratamiento):

1. Deben ser tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»).

2. Deben ser obtenidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines («limitación de la finalidad»).

3. Deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»).

4. Deben ser exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»).

5. Deben mantenerse de forma tal que sea posible identificar a los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales («limitación del plazo de conservación»).

6. Deben ser tratados de manera tal que se garantice su seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)[13].

Obviamente, estos seis principios básicos tienen relación con la información biométrica, ya que esta es parte de los datos personales manejados por los organismos.

Por otro lado, existe en la reglamentación una consideración especial para los datos biométricos, ya que solo autoriza su tratamiento bajo condiciones muy específicas, las cuales se detallan en el Artículo 9 (Consentimiento explícito por parte del dueño de la información e interés público, entre otros).

BIPA

El Biometric Information Privacy Act (BIPA) es un estatuto del estado de Illinois sobre la privacidad de la información biométrica (Illinois General Assembly, 2013). Es importante tenerlo presente porque se trata de una de las regulaciones más estrictas al respecto en los Estados Unidos. Entre otras obligaciones, requiere que se indique por escrito al usuario que su información biométrica está siendo recolectada y almacenada, con qué fines y por cuánto tiempo. También limita (prohíbe) que las empresas obtengan beneficios comerciales del uso de la información biométrica almacenada, así como su distribución y transferencia sin el consentimiento de la persona involucrada.

HIPAA

El Health Insurance Portability and Accountability Act (HIPPAA) de 1996 es un estatuto que rige la portabilidad y rendición de cuentas relativas a la información sobre la salud de las personas en los Estados Unidos. Allí se define la forma en que tales datos deben ser

13 Traducción y resumen del autor.

administrados por los distintos operadores. En este contexto se ha publicado un conjunto de reglas para dar cumplimiento a dicha regulación: reglas de seguridad HIPAA y reglas de privacidad HIPAA.

Dentro de las reglas de privacidad HIPAA se define el concepto de "información de salud protegida" (protected health information), que incluye cualquiera que permita identificar al individuo. En este sentido, los datos biométricos están comprendidos en esta regulación, aunque no aplica fuera del ámbito de la salud.

>Privacidad por diseño

La privacidad por diseño es un marco para el desarrollo de sistemas y procesos en el cual la protección y privacidad de los datos se incorpora desde la concepción misma del sistema. El concepto de "privacidad por diseño" fue desarrollado por la Dra. Anne Cavoukian (Cavoukian, 2009) y luego estandarizado en el ISO 29100 (Privacy Framework Principles) (ISO/IEC, 2011), mediante la descripción de 11 principios básicos. A continuación, se verá cómo estos principios están íntimamente relacionados con la protección de datos personales en general, y con los principios incluidos en el RGPD de la UE descritos anteriormente:

1. **Consentimiento y decisión**
   A menos que esté claramente permitido por la ley, toda recolección, almacenamiento y divulgación de datos debe ser aprobada por la persona. De ser posible, el individuo debe ser informado de:
   - qué tipo de rasgo biométrico será adquirido y cuándo,
   - quién está autorizado a hacerlo y por qué,
   - quién más está autorizado a acceder a sus datos biométricos y con qué propósito,
   - quién va a proteger, almacenar, transmitir acceder o relacionar sus datos biométricos, y
   - por cuánto tiempo serán almacenados los datos.

2. **Especificación y legitimidad del propósito**
   Las razones por las cuales la información biométrica es solicitada, registrada y eventualmente transmitida deben ser explicadas claramente al individuo. Es de suma importancia que esto sea claro, no solo para los responsables y técnicos del sistema biométrico, sino para todos los involucrados (operadores, funcionarios en general y obviamente el propio individuo). Es usual que la información del propósito se publique en el sitio web del organismo.

3. **Limitación del registro biométrico**
   El registro de información biométrica debe estar ajustado a derecho y sujeto a límites, de modo que responda estrictamente a las necesidades para las cuales se solicita. Cuando se analiza un sistema biométrico deben considerarse los riesgos eventuales para la privacidad del individuo, y asegurar que dichos riesgos sean proporcionales a los beneficios que el sistema biométrico le reportará. A modo de ejemplo, si se está considerando un sistema basado en huellas dactilares, ¿cuántas huellas se van a solicitar? ¿Cuáles son los beneficios y riesgos de solicitar más o menos huellas?

4 Minimización de datos recolectados
Los datos almacenados en los sistemas deben ser los mínimos necesarios. Siempre que sea posible, las transacciones que se generen en los distintos sistemas deberían no poder relacionarse entre sí.

5 Minimización en el uso, retención y divulgación de datos biométricos
Como se indicó en la sección "Ciclo de vida de un sistema de identidad", los sistemas biométricos pueden utilizarse en distintas etapas del ciclo de vida de sistemas de identidad. Es muy importante definir en qué etapas se va a usar, de qué forma y con qué fines. Dicho uso debe ser el mínimo necesario para el objetivo fijado.

6 Precisión y calidad de los datos
Los datos deben estar correctos, completos y actualizados. En particular, mantener los datos biométricos al día es de vital importancia, sobre todo los que tienen que ver con aquellos rasgos que cambian significativamente con el paso del tiempo.

7 Transparencia, apertura y notificación
Todos los involucrados deben ser adecuadamente informados de las políticas y prácticas de manejo de datos personales.

8 Participación y acceso
Las personas deben tener acceso a sus datos personales, y conocer sus usos e instancias de divulgación. Esto permite a su vez que, en caso de que se requiera, los usuarios indiquen al organismo que los datos no son correctos para que se hagan las enmiendas del caso.

9 Responsabilidad
Se requiere documentar y poner en conocimiento de todos aquellos con los cuales se interactúe las políticas y procedimientos definidos para manejar correctamente la privacidad. Lo ideal es que las entidades definan una función específica en lo que tiene que ver con la protección de los datos personales.

10 Seguridad de la información
Las entidades deben ser responsables por la seguridad de los datos biométricos almacenados, para lo cual deben cumplir con estándares reconocidos y emplear las mejores prácticas en materia de seguridad.

11 Adherir a estándares de seguridad
Las personas deben tener un mecanismo claro para presentar quejas, incluyendo información sobre cómo llevarlas a niveles superiores.

>Discriminación algorítmica y sesgo en sistemas biométricos

Por lo general, e independientemente de si se usan técnicas de aprendizaje automático o no, la información técnica sobre el desempeño de los sistemas biométricos es específica a una base de datos. En el caso de aquellos sistemas biométricos donde se haya utilizado un proceso de aprendizaje automático (caso de todos los sistemas recientes de reconocimiento facial), se debe tener en cuenta el desempeño diferencial de los mismos (González, Ortiz y Sánchez, 2020). Sin embargo, incluso en aquellos sistemas donde no sea común el uso de técnicas de aprendizaje (como son la mayoría de los que capturan huellas dactilares

o iris), también pueden existir sesgos. En particular, el sesgo puede producirse cuando, al reportar medidas de desempeño, se utiliza una base de datos con determinadas características. Aunque en algunos casos se puede saber a qué base de datos se hace referencia (por ejemplo, el resultado de las pruebas del NIST), es importante que se la analice y se la compare con la estadística de la población donde se instalará el sistema biométrico.

Los sesgos más comunes se relacionan con el sexo, la edad y la raza de la persona. Estos dependen también del tipo de biometría considerada. En el caso de las huellas dactilares, el sesgo más importante ocurre con la edad: es habitual que las huellas de los menores presenten una pérdida de precisión importante en comparación con los resultados que producen las de los adultos. También ocurre algo similar en los adultos mayores, aunque la pérdida de precisión en este caso es mucho menor que en el de niños y niñas. Recientemente se comenzó a analizar el sesgo en los sistemas de reconocimiento facial. Dado que estos utilizan datos para entrenar, dependiendo del tipo pueden registrar sesgos. Se ha reportado que existen sesgos evidentes por sexo y raza. El sesgo en sistemas de reconocimiento facial por edad —especialmente en lo que tiene que ver con los menores— es también un hecho conocido.[14]

>Capacidades

A la hora de pensar en el uso de información biométrica, es muy importante considerar las capacidades –tanto técnicas como institucionales-- con que cuenta la entidad a cargo.

Desde el punto de vista técnico, la entidad deberá contar al menos con personal capacitado en el uso de dicha biometría. Es fundamental contar con especialistas, particularmente en lo que tiene que ver con el diseño de la solución a implementar, así como con el procedimiento de adquisición de dicho sistema (trátese de un proceso de compra o de desarrollo interno). Es altamente recomendable que el sistema sea revisado con regularidad para detectar cualquier desvío de funcionamiento normal (baja en el desempeño, sesgos frente a determinada población, etc.).

Con respecto a las cuestiones operativas, es importante que los usuarios del sistema biométrico cuenten con formación específica en su uso. Esto no siempre es posible; si un sistema biométrico es desatendido, será difícil capacitar a los usuarios sobre su uso. Pero incluso en estos casos, pueden generarse infografías simples que permitan al usuario realizar acciones mínimas que garanticen una mejor toma de la muestra biométrica (por ejemplo, solicitarle que mire de frente a la cámara). En otros casos, como cuando haya funcionarios que ayuden al usuario en el momento de presentar la muestra biométrica, es recomendable incluir una capacitación sobre la mejor forma de operar los distintos dispositivos.

Desde el punto de vista institucional, es sumamente importante que la entidad siga las recomendaciones y regulaciones en el manejo de datos personales, y que incluya en este contexto el manejo de los de índole biométrica.

>Cuestiones comerciales

Por lo general, los sistemas biométricos se licencian de tres formas distintas: (1) según la cantidad de individuos registrados en la base de datos, (2) según la cantidad de muestras de rasgos biométricos almacenados, y (3) según la cantidad de transacciones realizadas.

14 Para un análisis detallado de discriminación algorítmica en biometría, véase Drozdowski et al. (2020).

El licenciamiento se relaciona de manera fundamental con el componente principal del sistema biométrico, a saber, la base de datos y las operaciones de verificación e identificación.

Además de este componente principal, es posible adquirir en forma independiente tanto los dispositivos de captura biométrica (escáneres de huellas dactilares e iris, cámaras fotográficas, etc.), como el módulo de generación de las plantillas biométricas. En ambos casos, existen licenciamientos de uso que deben estudiarse. Algunos proveedores requieren activar una licencia por cada módulo de captura, mientras que otros permiten su libre instalación.

Cabe señalar que no es usual que el proveedor del módulo de captura incluya el módulo de generación de la plantilla como parte del paquete. Por ejemplo, tratándose de escáneres de huella dactilar, no es común que estos contengan el aplicativo para generar la plantilla. Por lo tanto, en el momento de adquirir un componente biométrico, la institución deberá asegurarse de que este tenga todo lo necesario para interoperar con el resto del sistema.

Otro elemento crítico a la hora de obtener el licenciamiento es determinar si el sistema operará en las instalaciones y equipos del cliente ("*on premise*") o si por el contrario se contratará como servicio (SaaS por *Software* as a *Service*).

Cuando el sistema se instala en los equipos del cliente, a menudo el tipo de licenciamiento se realiza al dimensionar la base de datos: ya sea por la cantidad de individuos o por la cantidad de muestras biométricas registradas. El licenciamiento por transacciones realizadas (operaciones de verificación e identificación) requiere que el proveedor pueda contabilizarlas, lo que por lo general se realiza cuando el sistema se licencia como SaaS.

A la hora de decidir si se contrata una solución SaaS, es imperativo que se consideren todas las implicaciones relativas al manejo de datos en términos de la privacidad y seguridad de la información. Dado que las soluciones SaaS operarán por fuera de la institución, es muy importante revisar en detalle todo lo relacionado a la protección de datos. Nótese que, en algunas entidades, incluso puede ser ilegal utilizar servicios SaaS, ya que esto puede requerir que los datos salgan del país.

Otra opción de licenciamiento es la compra de licencias de desarrollo específicas. Por ejemplo, se podría adquirir un paquete de desarrollo de software (SDK por las siglas en inglés de Software Development Kit) para la extracción de características o para la comparación de dos conjuntos de características. A menudo, estos SDK no tienen limitaciones en lo que tiene que ver con el desarrollo del software; sin embargo, sí podrían requerir licencias adicionales para su ejecución, lo cual entrañaría costos adicionales a los estimados inicialmente.

>Qué incluir en un pliego

Durante un proceso de adquisiciones, será necesario especificar los requerimientos técnicos del sistema biométrico que se busque, tal y como se detalla a continuación.

Requerimientos funcionales. Estos deben ser compatibles con los requerimientos de uso del futuro sistema:

1. El sistema debe tener un mecanismo para la verificación e identificación basado en servicios web.
2. El sistema debe proveer una interfaz gráfica donde se visualicen los resultados de las búsquedas.
3. El sistema debe incluir un aplicativo móvil que interactúe con el sistema central, permitiendo recuperar datos y realizar tanto verificación como identificación.

Requerimientos no funcionales. Aquí se especifican los criterios no funcionales que el sistema debe cumplir, dentro de los cuales figuran los siguientes:

1. El uso de estándares que permitan la interoperabilidad y portabilidad de los datos en el futuro, lo cual incluye almacenamiento de los datos en formatos estándar. Ejemplos:
   - Todas las comunicaciones entre el sistema central y los periféricos deben hacerse usando el estándar ANSI/NIST-ITL-1 2011 - Update 2015: Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information.
   - Las huellas dactilares deben almacenarse como WSQ, con un factor de compresión entre 1:5 y 1:15 (https://www.fbibiospecs.cjis.gov/Document/Get?fileName=_WSQ_Gray-scale_Specification_Version_3_1_Final.pdf)
2. La definición de métricas de desempeño que aseguren que el sistema satisface las necesidades para las que se diseñó. Ejemplos:
   - Una vez instalado y con la base datos completa,15 el sistema deberá tener un desempeño en verificación de al menos 0,01 FNMR para un FMR de 0,001.
   - Una vez instalado y con la base de datos completa, el sistema deberá tener un desempeño en identificación de al menos 0,01 FNIR para un FPIR de 0,001.
3. La definición de tiempos de respuesta, ya que algunas de las funcionalidades requieren respuestas en tiempo real. Ejemplos:
   - Una vez instalado, y con la base de datos completa, el sistema deberá poder procesar al menos 50 consultas de verificación simultáneas.
   - La consulta de verificación no podrá demorar más de dos segundos.
   - La consulta de identificación no podrá demorar más de 10 segundos, con la base de datos completa.

15 Se debe incluir la información acerca del tamaño de la base de datos.

Criterios de evaluación objetiva. Dado que la instalación de estos sistemas es a menudo costosa, se recomienda minimizar los riesgos exigiendo un conjunto de criterios de evaluación objetiva. Esta evaluación estará comúnmente asociada con las medidas de desempeño del sistema. Para poder comparar varios sistemas entre sí, es necesario que el conjunto de datos y el protocolo de pruebas sea el mismo para todos. Existen por lo menos dos formas de proceder:

1. Planificar, como parte del proceso de evaluación, la realización de pruebas.
2. Solicitar que los distintos oferentes hayan participado en pruebas públicas que puedan referenciarse.

El primer caso tiene un mayor grado de flexibilidad, ya que la prueba puede adaptarse a las necesidades específicas de la compra. Sin embargo, el diseño de una prueba requiere que se tenga un conocimiento importante de biometría, ya que un mal diseño de las pruebas puede conducir a un análisis deficiente de los sistemas. Es, además, mucho más difícil pues exige seleccionar los datos, revisarlos, realizar pruebas y definir su protocolo, todo lo cual consume tiempo y esfuerzo.

En el segundo caso, lo que se incluye en el pliego es una referencia específica a alguna de las pruebas usadas como referencia, la más conocida de las cuales es la que organiza el NIST para diversos tipos de biometría (reconocimiento facial, huellas dactilares, etc.). En este caso también es necesario conocer bien estas pruebas, dado que son numerosas y has sido diseñadas para analizar distintos problemas.

>Licenciamiento

Finalmente, y como ya se señaló anteriormente cuando se abordaron los aspectos comerciales de los sistemas biométricos, es muy importante solicitar toda la información relativa a la forma de licenciamiento. Se indicó entonces cómo una solución biométrica comprende numerosos componentes: equipos de captura (escáneres de huellas dactilares e iris, cámaras fotográficas), extractor de características, comparador de huellas dactilares, etc. Si no se tiene especial cuidado, alguno de estos componentes podría tener una forma de licenciamiento no apta para las necesidades del sistema.

Referencias

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada, 5, 12.

Drozdowski, P., Rathgeb, C., Dantcheva, A., Damer, N. y Busch, C. (2020). Demographic bias in biometrics: A survey on an emerging challenge. IEEE Transactions on Technology and Society, 1(2), 89-103.

Fussey, P. y Murray, D. (2019). Independent report on the London Metropolitan Police Service's trial of live facial recognition technology.

Disponible en: https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

Gelb y Clark, J. (2013). Performance lessons from India's universal identification program. CGD Policy Paper, 20.

González, F, Ortiz, T. y Sánchez, R. (2020). IA Responsable. Manual Técnico – Ciclo de vida de la inteligencia artificial. Disponible en: https://el-bid.github.io/Manual-IA-Responsable/

Illinois General Assembly (2013). Biometric Information Privacy Act (BIPA). 2013 Illinois Compiled Statutes Chapter 740 - CIVIL LIABILITIES 740 ILCS 14/ - Biometric Information Privacy Act.

ISO/IEC (2011). 29100:2011 - Information technology — Security techniques — Privacy framework. Disponible en: https://www.iso.org/standard/45123.html

Jain, A. K., Ross, A. A. y Nandakumar, K. (2011). Introduction to biometrics. Springer Science & Business Media.

Muralidharan, K., Niehaus, P. y Sukhtankar, S. (2020). Identity verification standards in welfare programs: Experimental evidence from India (No. w26744). National Bureau of Economic Research. Disponible en: https://econweb.ucsd.edu/~kamurali/papers/Working%20Papers/ABBA%20(NBER%20WP%2026744).pdf

NIST. S.f. Special Data Base 301. Disponible en: https://www.nist.gov/itl/iad/image-group/nist-special-database-301

Parlamento y Consejo Europeo (2016). REGLAMENTO (UE) 2016/679

Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Scientific American. (2008). The Future of Privacy. New York: Munn & Co., septiembre. Disponible en: https://www.scientificamerican.com/magazine/sa/2008/09-01/

UDIAI. (2012). Role of biometric technology in Aadhaar enrollment. Disponible en: http://www.dematerialisedid.com/PDFs/role_of_biometric_technology_in_aadhaar_jan21_2012.pdf

UNHRC (2015). Joint Inspection of the Biometrics Identification System for Food Distribution in Kenya. Disponible en: https://documents.wfp.org/stellent/groups/public/documents/reports/wfp277842.pdf

Anexo: Estándares

La industria ha desarrollado numerosos estándares relacionados con los sistemas biométricos: desde estándares de interoperabilidad, hasta estándares de adquisición y almacenamiento.

Estándares generales

- ISO/IEC 2382-37 (https://www.iso.org/standard/66693.html). Define el vocabulario utilizado en biometría. Disponible solo en inglés.

Estándares relacionados con el intercambio de información biométrica

- ISO/IEC 19794 (https://www.iso.org/standard/50862.html). Formato de intercambio de datos biométricos. Es una familia de estándares (del 1 al 11) que definen los formatos y mecanismos de intercambio para distintos datos biométricos. A modo de ejemplo, el 19794-2 define cómo se almacenan e intercambian datos de minucias de huellas dactilares, mientras que el 19794-5 aplica a los datos de imágenes del rostro y el 19794-6 a datos de iris. Es un estándar muy importante para mantener la interoperabilidad entre sistemas.
- ISO/IEC 19785:2020 (https://www.iso.org/standard/77892.html). Este estándar define los mecanismos de comunicación entre sistemas biométricos.
- ISO/IEC 397974 (https://www.iso.org/news/ref2478.html). Este estándar especifica el formato de intercambio de datos biométricos y está previsto que reemplace al ISO/IEC 19794.

Estándares relacionados con la evaluación de sistemas biométricos

- ISO/IEC 19795: En este documento se establecen principios generales para probar el rendimiento de los sistemas biométricos en términos de tasas de error y tasas de rendimiento, con los siguientes fines, entre otros: medición del rendimiento, predicción del rendimiento, comparación del rendimiento y verificación de la conformidad con los requisitos de rendimiento especificados.

- ISO/IEC 29109: En este documento se especifican los elementos de la metodología de prueba de conformidad, las pruebas de consistencia, y los procedimientos de prueba aplicables a las imágenes faciales bidimensionales definidas en el estándar de formato de intercambio de datos biométricos ISO/IEC 19794-5: 2005 para datos de imágenes faciales.

Estándares relacionados con la seguridad y la privacidad

- ISO/IEC 24745: Contiene orientaciones para la protección de la información biométrica en virtud de diversos requisitos de confidencialidad, integridad y renovabilidad/ revocabilidad durante el almacenamiento y la transferencia. Asimismo especifica requisitos y pautas para la gestión y el procesamiento seguro y compatible con la privacidad de la información biométrica.

- ISO/IEC 29100: Proporciona un marco de privacidad que especifica una terminología de privacidad común; define a los actores y sus roles en el procesamiento de información de identificación personal (PII por sus siglas en inglés); describe las consideraciones de protección de la privacidad e incluye un conjunto de referencias a los principios de privacidad usados para la tecnología de la información.

- ISO/IEC 19989: En este documento se presenta el marco general para la evaluación de la seguridad de los sistemas biométricos, incluidos los componentes funcionales de seguridad.

- ISO/IEC 30107: El propósito de este documento es proporcionar una base para la detección de ataques de presentación (PAD por sus siglas en inglés). Esto a través de la definición de términos y el establecimiento de un marco a través del cual puedan especificarse y detectarse tales eventos, así como clasificarse, detallarse y comunicarse para la toma de decisiones posteriores y las actividades de evaluación de rendimiento.

Estándares relacionados con la calidad

- ISO/IEC 29794 (https://www.iso.org/standard/62782.html) : Es una familia de estándares que especifica criterios de calidad para obtener muestras biométricas. A modo de ejemplo, el estándar 29794-5 especifica criterios para la imagen del rostro y el 29794-6 para el iris.

Estándares relacionados con la autenticación

- ISO/IEC 24761: En este documento se definen la estructura y los elementos de datos del Contexto de Autenticación para Biometría (ACBio por su acrónimo en inglés), el cual se utiliza para verificar la validez del resultado de un proceso de registro y verificación biométrica ejecutado en un sitio remoto. Este documento permite que cualquier instancia de ACBio acompañe cualquier proceso biométrico relacionado con la inscripción y verificación. La especificación de ACBio es aplicable no solo a la inscripción y verificación biométrica monomodal, sino también a la fusión multimodal.

Varios

- ISO/IEC 19784 ANSI-INCITS 358-2002, BioAPI Specification – (ISO/IEC 19784-1). Define la interfaz de programación de aplicaciones (API por sus siglas en inglés) y la interfaz de proveedor de servicios (SPI por sus siglas en inglés) para interfaces estándar dentro de un sistema biométrico que admite componentes de varios proveedores. Permite interoperabilidad entre dichos componentes a través de la adhesión a esta y otras normas internacionales.

- ISO/IEC 24787:2010: En este documento se establecen los requisitos para realizar comparaciones de muestras biométricas y decisiones de devolución en una tarjeta con circuito integrado (Match On Card), así como medidas de seguridad para la comparación biométrica en tarjeta.

- FBI - ELECTRONIC BIOMETRIC TRANSMISSION SPECIFICATION (EBTS), en particular el APPENDIX F – FBI/CJIS IMAGE QUALITY SPECIFICATIONS: Es el estándar para escáneres de huellas dactilares. : http://www.fbibiospecs.cjis.gov/Document/Get?fileName=Master_EBTS_v10_-_FINAL_20130702_new_figures.pdf


BID
Mejorando vidas