Biometría aplicada a la Seguridad Pública

Pablo Niklas Facultad de Ingeniería
Universidad de Palermo
Ciudad Autónoma de Buenos Aires
Email: pablo.niklas@gmail.com

***Resumen*—Los avances tecnológicos permitieron automatizar y perfeccionar, métodos manuales ya existentes como la clasificación e identificación de patrones dactilares. A su vez, se crearon nuevas disciplinas biométricas como el reconocimiento del iris, del rostro, y la distribución capilar, entre otros. Este trabajo ilustra algunas de las implementaciones que posee el Estado Nacional y paralelamente presenta nuevas soluciones a los efectos de complementar las existentes. De esta manera, a través de un análisis integral, se intentarán vislumbrar nuevos resultados, mediante la utilización de recursos tecnológicos con desarrollos actuales de punta, que cumplan con la premisa de mejorar la performance de la seguridad pública.**

***Index Terms*—Biometria, Seguridad, Estado Nacional, Integral**

I. Introducción

La seguridad es cada vez una preocupación mayor en las sociedades actuales. [1] [2] Diferentes Países, especialmente los de mayor desarrollo, son blancos de ataques terroristas, o mismo de atentados perpetrados por su propio pueblo. De una manera u otra, la Seguridad Pública, dejo de ser un concepto, para convertirse en un tema candente, que preocupa a millones de ciudadanos y no reconoce limitaciones temporarias o geográficas. Pero, de lo que se habla precisamente cuando se refiere a la SEGURIDAD PUBLICA, se habla de: un servicio que debe brindar el Estado para garantizar la integridad de todos los ciudadanos y sus bienes; tal definición nos hace se plantee la siguiente pregunta, que desde su análisis intrínseco, resulta ser compleja ¿Cuenta el Estado con herramientas suficientes para resguardar la integridad de todos? Y antagónicamente la respuesta deviene sencilla: Si, cuenta con tecnología.

Sin ahondar, en las diferentes implicancias que causa el referirse a la efectividad con que la tecnología es aplicada a la Seguridad Pública, se puede precisar que su génesis se encuentra en el descubrimiento de la Biometría. Y, ¿Por qué la biometría?. Desde hace más de un siglo la biometría es utilizada para identificar seres humanos; el sabernos identificados contribuye a la equidad en la aplicación del derecho positivo[1]. Antiguamente, en sociedades pequeñas, todos eran conocidos, velar por la aplicación del conjunto de reglas y normas que establecían un marco adecuado para las relaciones entre personas e instituciones, autorizando, prohibiendo y permitiendo acciones específicas, era relativamente fácil; en nuestros días, al Estado, garantizar nuestra vida en sociedad le resulta una tarea bastante compleja. Para ello necesita diferentes herramientas: de prevención, de coacción y otras que le provean, no sólo la posibilidad de reconocer al autor de la falta, sino también que le den la certeza de identificarlo, y es ahí donde juega un papel importante la biometría.

Etimológicamente ”BIOMETRIA”deriva del griego *bios* que significa vida, y *metron* que significa medida y es conocida como el estudio de métodos que permiten identificar a seres humanos en base a características físicas o conductuales. Fue hallada su expresión primigenia en el 29.000 AC, en impresiones de las manos dejadas en las obras realizadas en las cavernas, como símbolo de autoría. Ya en el 500 AC en Babilonia se firmaban transacciones financieras, usando tablas de arcilla con impresiones digitales; la historia fue avanzando y con ella diferentes registros de biometría fueron marcando un devenir ineludible.

En el año 1882, Alphonse Bertillon, funcionario de la prefectura de la Policía de París, comienza a usar un sistema basado en la antropometría del cuerpo, que años después llevó se nombre; en el año 1889 la Policía Federal Argentina, en ese entonces, Policía de la Capital, lo incorpora a su investigación Forense. Finalmente en el año 1891 Juan Vucetich, oficial de la policía de la Provincia de Buenos Aires comienza su primer archivo de huellas dactilares, con un innovador método basado en los patrones de Galton. Sin embargo, fue recién en 1940 y casi llegando a los 50 que se empezó a utilizar la tecnología, para simplificar el control sobre la identidad del Ciudadano.

Con el correr del tiempo, la tecnología avanzó desarrollando algoritmos eficientes de procesamiento de imágenes. Con estos algoritmos se pudieron procesar e incorporar los distintos patrones biométricos. En un comienzo fueron las huellas dactilares, luego el rostro, el iris y la voz.

Existe una clasificación primaria entre los distintos patrones biométricos. En primer lugar los que dejan rastros, como las huelas digitales o el ADN y en segundo lugar los que no dejan rastros, abarcando al universo restante.

Sin embargo a pesar de sus ventajas, no queda exceptuada de problemas al momento de su utilización, como paso con las tecnologías innovadoras. [3]

También se puede citar otro de los grandes obstáculos que se debe atravesar al momento de incorporar la biometría a estándares de seguridad como ser: donde ubicar la barrera de la privacidad. [4]

El objetivo de este trabajo es describir distintas formas de utilización de la biometría para el fortalecimiento de la Seguridad Pública, soslayando obstáculos conceptuales y así lograr plasmar soluciones alcanzables.

[1]Es el conjunto de normas jurídicas escritas por una soberanía, esto es, toda la creación jurídica del órgano estatal que ejerza la función legislativa.

II. Modalidades Biométricas

Como se ha mencionado, las técnicas biométricas se clasifican en dos grupos diferenciados. El primero estudia las características fisiológicas del individuo y es comúnmente conocido como Biometría Estática, dentro de ella se puede agrupar a las huellas dactilares, la geometría de la mano, los termogramas de venas de rostro y mano, el reconocimiento facial, el ADN, la composición química del olor corporal y la caracterización ocular, encontrando esta última una nueva subdivisión: análisis de iris, análisis de retina y análisis de córnea. El otro grupo se basa en la medición de los patrones conductuales del individuo y es conocido como Biometría Dinámica, la misma agrupa a la voz, la firma y escritura manuscrita, la dinámica del tecleo y la cadencia del paso. A continuación se hará un breve análisis de las ventajas y desventajas de cada modalidad para luego desarrollar la incumbencia de aquellas que requieren un mayor énfasis.

- **Huellas:** Poseen muy alta universalidad (son posible de encontrar en casi todos), muy alta capacidad de recolección (son relativamente fácil de obtener), poseen una tasa muy alta de unicidad (la probabilidad de que dos personas tengan las mismas huellas es de 1 en 64.000.000 aproximadamente).
- **Geometría de la mano:** Tiene gran aceptabilidad y es de fácil implementación, sin embargo, requieren un alto grado de cooperación del individuo y poseen gran variabilidad con el tiempo.
- **Termogramas de las venas de rostro y mano:** Las venas son un patrón robusto, estable y oculto; se pueden leer fácilmente con sensores ópticos y técnicas de procesamiento digital, de imágenes pero el costo de los sensores es muy elevado.
- **Reconocimiento facial:** Es un rasgo biométrico por excelencia, permite su adquisición a distancia, aún sin la colaboración del sujeto, es altamente universal sin embargo posee una baja tasa de unicidad.
- **ADN:** Es la identificación con mejores tasas de error, ya que la misma es bajísima, sin embargo no es una medida de identificación biométrica directa, al no poder realizarse en tiempo real y los costos aún siguen siendo muy elevados.
- **Composición química del olor corporal:** Cada persona tiene un olor específico compuesto por 30 olores diferentes en distintas concentraciones. Si bien es un método que reconoce algunas aplicaciones, todavia no ha logrado implementarse a nivel de seguridad.
- **Reconocimiento por iris:** Tiene un alto grado de precisión, es de gran utilidad para la seguridad pero solo puede usarse en ambientes controlados, requiere un alto grado de colaboración por parte del individuo.
- **Reconocimiento por retina:** Posee gran confiabilidad, es seguro y compacto pero muy invasivo y tiene costos muy elevados.
- **Voz:** Es de fácil aceptación y adquisición pero sigue siendo un método muy complejo de implementar, imposible de trabajar en tiempo real.
- **Firma y escritura manuscrita:** Tiene muy buena aceptación por no ser para nada invasivo pero es muy vulnerable a las falsificaciones.
- **Dinámica del tecleo:** Al igual que el anterior es muy fácil de falsificar.
- **Cadencia del paso:** No es invasivo y no requiere la colaboración del sujeto, sin embargo todavía no se encuentran aplicaciones reales.

II-A. Huellas Dactilares

Definidas en sentido estricto, son las impresiones obtenidas por las crestas de los dedos humanos. En un sentido más amplio, pueden ser las impresiones de las crestas producidas por cualquier parte de la piel de un ser humano o de un primate. Al observar las palmas de las manos, se podrá ubicar en la tercer falange de los dedos, una especie de almohadilla; ésta se encuentra cubierta por crestas y surcos. Las mismos, adquieren diferentes formas, extendiéndose en múltiples direcciones, se disponen en forma totalmente al azar y conforman dibujos perfectamente diferenciables entre distintos individuos. [5]

Una cresta es una porción elevada de la epidermis de los dedos de manos y pies, la palma de la mano o la planta del pie. Se conocen como crestas epidérmicas, y conforman la interfaz entre las papilas de la dermis y la epidermis. Estas conformaciones papilares **se generan en el primer semestre de gestación de la persona**. Una de sus funciones, es la táctil; permitiendo la aprehensión de objetos a través de la humedad de la mano, producida por el sudor secretado por las glándulas sudoríparas que estas mismas conformaciones elevan.

Antes de que la revolución informática comenzara a proveer métodos de clasificación automáticos, sólo existían clasificaciones manuales. Estos sistemas clasificaban la información por presencia o ausencia de formaciones dactilares (por ej. patrones circulares en algunos dedos). [6]. De este modo se podían almacenar grandes volúmenes de información en un archivo de papel, y era fácil recuperar la información de manera relativamente eficiente. Con el fin de simplificar la explicación se puede manifestar con acierto que la clasificación dactilar es similar a encontrar páginas en *Google* por palabras clave. Las crestas papilares se agrupan de modo tal que conforman 4 dibujos o patrones, distinguidos entre sí, los cuales denominó Vucetich[2]: presilla (interna o externa), verticilo y arco. [7]

II-A1. Etapas del procesado de Huellas Dactilares: Al momento de procesar la imagen de una huella, hay que distinguir tres etapas: la captura propiamente dicha, el procesado y extracción de atributos y finalmente el almacenamiento para la generación de una base de datos o para comparar con datos ya existentes en la base.

1. **Captura:** Existen diferentes tipos de sensores usados en la captura de la imagen de las huellas digitales, los cuáles pueden ser clasificados en dos grandes categorías: Ópticos y Estado Sólido. A su vez, esta última categoría se divide en: capacitivos, térmicos, acústicos (ultrasonido) y de presión.

[2]Nacionalizado argentino con el nombre de Juan Vucetich Kovacevich, (Hvar, Croacia, 20 de julio de 1858 - Dolores, 25 de enero de 1925) fue un antropólogo, policía e inventor croata naturalizado argentino. Vucetich desarrolló y puso por primera vez en práctica un sistema eficaz de identificación de personas por sus huellas digitales.

Una de las características más importante a la hora de realizar la captura, es la resolución. Este parámetro indica la cantidad de puntos por pulgada. Una resolución de 500 dpi es la mínima usada por scanners del FBI. En el área forense se suele usar 1000 dpi. Periódicamente el FBI publica un listado con los dispositivos homologados que satisfacen esta característica. [8]

2. **Extracción de Características:** El proceso de transformar los datos originales que posee la imagen de la huella capturada, en datos que resulten más útiles para tomar una decisión, es lo que se denomina parametrización o extracción de características. Existen diferentes mecanismos para hacerlo, todo va a depender del sistema biométrico con el que se esté trabajando y de las características que tome el sistema como útiles para realizar la comparación. [6]
3. **Comparación:** Concluida la parametrización o extracción de características, generalmente se procede a la comparación de las huellas , la cuál consiste en asignar un puntaje a la similitud entre dos plantillas, donde el puntaje más alto indica que son iguales y el más bajo que son distintas. Existen diferentes métodos para comparar huellas, de los cuales se puede distinguir tres categorías: comparación basada en la correlación, basada en la minutiae, y basada en otros parámetros. Todo va a depender de la robustez del sistema con el que se este trabajando.

Para determinar la performance de un sistema biométrico de identificación de huellas dactilares suelen usarse bases de datos estandarizadas.

II-A2. Tecnología Biométrica en Argentina - AFIS: Hasta el año 2000, los expertos en la identificación dactiloscópica, utilizaban solo procedimientos manuales para la identificación de personas a través de las huellas dactilares; a mediados de Diciembre de 1999, se efectúo el primer equipamiento, mediante la utilización de un sistema de búsqueda biométrica automatizado. Esta tecnología recibe el nombre de AFIS.[3]

El AFIS ofrece todas las ventajas de la informática aplicada a la actividad papiloscópica. Aporta celeridad, seguridad y eficiencia en la práctica pericial de los especialistas y permite de este modo ampliar el ámbito de acción a través de la concentración de datos identificatorios imposible de vincular por medios manuales. Permite la selección, con gran precisión, de un número definido de candidatos, entre un voluminoso número de archivo dactilares. Este sistema informático, compuesto de hardware y software integrados, permite la captura, consulta y comparación automática de improntas dactilares (agrupadas por decadactilares, monodactilares, rastros o latentes[4]).

El 7 de Septiembre del año 2000, se crea oficialmente en el ámbito de la Policía Federal Argentina, la Sección AFIS, con una base de datos de 5.000.000 de registros. [6]

En el año 2011, se incorpora el Sistema AFIS MetaMorpho, con nuevas herramientas de búsqueda, mucho más flexibles y provee una solución completamente integrada para la captura, cotejo, almacenamiento y visualización de huellas, tanto dactilares como palmares.

La implementación de este nuevo Sistema AFIS, comprende la actualización y ampliación de la capacidad existente en el Sistema AFIS del año 1999. Se amplía la capacidad de almacenamiento a 15.000.000 de registros y 40.000 registros latentes. Se agrega la capacidad de procesamiento de palmares, con una capacidad de 200.000 registros y 10.000 registros de latentes palmares. También se agrega un sistema de reconocimiento facial de 100.000 registros. [9]

En el año 2015, se actualizó nuevamente llevándolo a una capacidad de 21.000.000 de registros. [10]

El sistema trabaja efectuando automáticamente la clasificación de huellas y extrayendo del mismo modo las minucias de las huellas -características íntimas de identificación-. Las propiedades así captadas resultan suficientes y autónomas para efectuar la comparación de las huellas y rastros latentes.

II-B. Voz

El análisis biométrico de la voz, tiene dos enfoques. El reconocimiento del locutor y el reconocimiento de la voz propiamente dicha. El reconocimiento de locutores es una

[3]Automated Fingerprint Identification System.

[4]Huella que se obtiene de la escena del crimen.

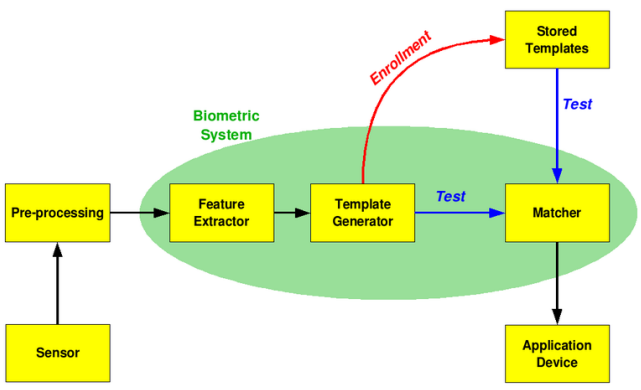

Figura 1. Esquema de un sistema biométrico

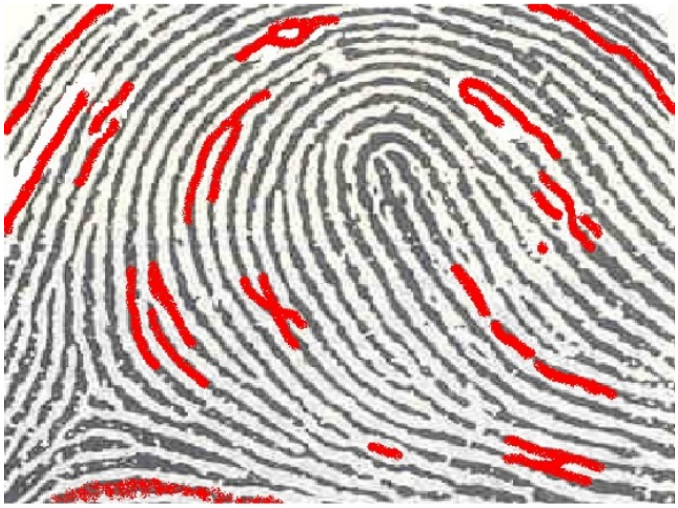

Figura 2. Crestas papilares

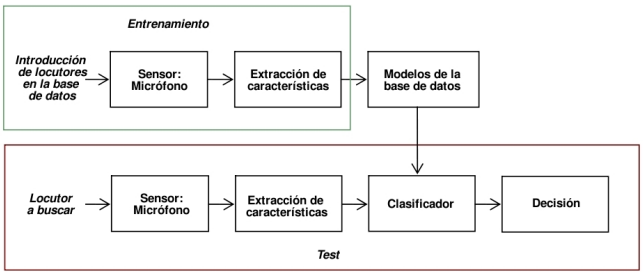

Figura 3. Esquema del sistema de reconocimiento de voz

modalidad biométrica que usa la voz con fines identificatorios, a diferencia del reconocimiento de la voz que solo intenta identificar las palabras articuladas, independientemente de quien sea el locutor.

II-B1. Reconocimiento de locutores: El reconocimiento de locutores pertenece a la rama de la inteligencia artificial y consiste en la identificación automática de una persona a través de su voz. El hecho de poder distinguir un locutor de otro está relacionado mayoritariamente con las características fisiológicas y los hábitos lingüísticos de cada uno de ellos. El reconocimiento conlleva un procesado de audio que permite extraer este conjunto de rasgos inherentes al locutor y la posterior búsqueda de posibles coincidencias mediante un proceso de reconocimiento de patrones. [11]. Esta modalidad biométrica, evoluciona conjuntamente con la evolución de las tecnologías de reconocimiento de voz, debido a que ambas modalidades poseen similares características. A diferencia de las huellas dactilares, recién en el año 1980 se hace un progreso significativo en el rubro, alcanzando mayor auge en el año 1996 cuando NIST (Instituto Nacional de Estándares y Tecnología de EEUU) comienza a desarrollar competencias anuales de reconocimiento de locutores para promover su avance. Los sistemas desarrollados en base a esta modalidad, pueden clasificarse en: Verificación de locutores, en tal sentido la conclusión arribada nos va a decir si el locutor es quien dice ser y como tal la decisión es (1:1), o Identificación de locutores propiamente dicha que identificara quien es el locutor, debiendo la decisión tomarse (1:N).

Arquitectura del sistema Un sistema de reconocimiento de locutores está formado por dos secciones: entrenamiento y test. A pesar de compartir una estructura similar en cuanto a los módulos que las conforman, ambas tienen una función bien diferenciada.

1. **La sección de entrenamiento** tiene la finalidad de registrar locutores mediante un micrófono para extraer sus características y guardarlas en la base de datos.
2. **La sección de test** se centra en registrar a un locutor y extraer las características para poder compararlas con las que se encuentran almacenadas en la base de datos. Finalmente, después de obtener posibles coincidencias, el sistema presenta al locutor susceptible de ser el buscado [11]. El esquema se puede apreciar en la figura 3.

Los módulos son:

1. **Adquisición de datos** La adquisición de datos es esencial tanto para la sección de entrenamiento como para la de test. Para poder introducir locutores al sistema es necesario un transductor acústico-eléctrico, ya que la voz se propaga en forma de ondas y para poder extraer características es necesario transformar la presión sonora en un señal eléctrica y así poder proceder a su digitalización.
   El tipo de micrófono, la frecuencia de muestreo y la cuantización realizada en la captación del audio deberá adecuarse al ancho de banda de la voz y sus características. Hay factores externos al locutor como la elección de los parámetros anteriores, la relación señal ruido (SNR) de las muestras grabadas o la utilización de micrófonos con diferentes curvas de respuesta frecuencial que pueden influir negativamente en el resultado. [11]
2. **Extracción de características** Una vez digitalizado, el audio se procesa para extraer el listado de características elegidas, las cuales se llaman **descriptores de audio**. Estos descriptores **contienen las características acústicas de la señal que utilizará el clasificador para compararlos con el listado almacenado en la base de datos**. Las características a analizar pueden ser diversas pero se suelen utilizar los descriptores de audio de bajo nivel debido a la naturaleza de la fuente. Estos descriptores **tienen baja abstracción y se limitan a describir características espectrales, paramétricas y temporales de la señal de audio.**
   Para poder asociar las características de los descriptores a los archivos de audio correspondientes, se utilizan los metadatos (datos sobre datos). Uno de los estándares utilizados para esta tarea es el estándard MPEG-7[5], el cuál permite la gestión de estos metadatos, facilitando así el acceso a la información en el momento de la búsqueda.
3. **Clasificación** El módulo clasificador tiene acceso tanto a la parte de entrenamiento como a la de test. Este módulo hace de puente entre ambas partes encargándose de comparar los vectores de características a buscar con los vectores de los modelos de locutor que contiene la base de datos. Su tarea computacional consiste en encontrar coincidencias y como resultado extrae una serie de probabilidades de los locutores en la base de datos susceptibles de ser el buscado. La decisión puede ser diferente dependiendo de la configuración del sistema.
   a) **Cerrado:** Un sistema cerrado da por supuesto que el locutor que se quiere identificar se encuentra ya almacenado en la base de datos. El locutor con más probabilidades a la salida del clasificador, que comparte más características con el locutor a buscar, será la salida resultante del sistema.

[5]Es un estándar de la Organización Internacional para la Estandarización ISO/IEC y desarrollado por el grupo MPEG. El nombre formal para este estándar es Interfaz de Descripción del Contenido Multimedia (Multimedia Content Description Interface). La primera versión se aprobó en julio de 2001 (ISO/IEC 15938) y actualmente la última versión publicada y aprobada por la ISO data de octubre de 2004.

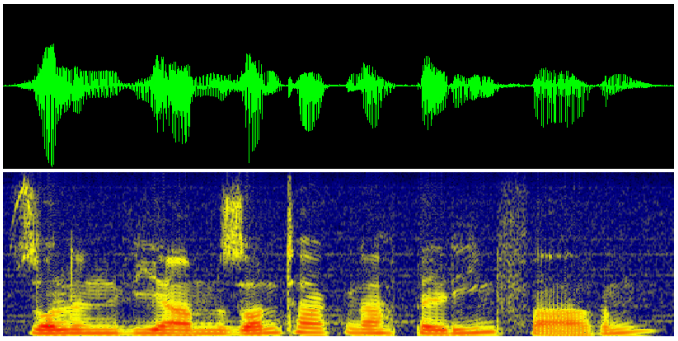

Figura 4. Frecuencias de la Voz

b) **Abierto:** Un sistema abierto es más complejo, ya que el locutor que se quiere identificar no está necesariamente en la base de datos. El clasificador debe tener en cuenta no sólo la más alta probabilidad, sino además, establecer si la semejanza es suficiente para dar un positivo. Si las probabilidades de un modelo de locutor se consideran suficientes como para suponer una coincidencia, se presenta al candidato como resultado de la búsqueda, en caso contrario la salida es "locutor desconocido".

II-B2. Reconocimiento de voz: El reconocimiento automático del habla (RAH) o reconocimiento automático de voz **es una disciplina de la inteligencia artificial que tiene como objetivo permitir la comunicación hablada entre seres humanos y computadoras**. El problema que se plantea en un sistema de este tipo es el de hacer cooperar un conjunto de informaciones que provienen de diversas fuentes de conocimiento (acústica, fonética, fonológica, léxica, sintáctica, semántica y pragmática), en presencia de ambigüedades, incertidumbres y errores inevitables para llegar a obtener una interpretación aceptable del mensaje acústico recibido.

Un sistema de reconocimiento de voz es una herramienta computacional capaz de procesar la señal de voz emitida por el ser humano y reconocer la información contenida en ésta, convirtiéndola en texto o emitiendo órdenes que actúan sobre un proceso. En su desarrollo intervienen diversas disciplinas, tales como: la fisiología, la acústica, el procesamiento de señales, la inteligencia artificial y la ciencia de la computación.

1. **Aprendizaje** Un aspecto crucial en el diseño de un sistema de RAH es la elección del tipo de aprendizaje que se utilice para construir las diversas fuentes de conocimiento. Básicamente, existen dos tipos:
   a) **Las técnicas de Aprendizaje Deductivo:** Se basan en la transferencia de los conocimientos de un experto humano a un sistema informático. Un ejemplo paradigmático de las metodologías que utilizan tales técnicas lo constituyen los Sistemas Basados en el Conocimiento y, en particular, los Sistemas Expertos.
   b) **Las técnicas de Aprendizaje Inductivo:** se basan en la adquisición automática de conocimientos. El sistema, consigue los conocimientos necesarios a partir de ejemplos reales, sobre la tarea que se desea modelizar. En este segundo tipo, los ejemplos los constituyen aquellas partes de los sistemas basados en los modelos ocultos de Márkov o en las redes neuronales artificiales que son configuradas automáticamente a partir de muestras de aprendizaje.
2. **Decodificador acústico-fonético** Las fuentes de información acústica, fonética, fonológica y posiblemente léxica, con los correspondientes procedimientos interpretativos, dan lugar a un módulo conocido como decodificador acústico-fonético (o en ocasiones a un decodificador léxico). La entrada al decodificador acústico-fonético es la señal vocal convenientemente representada; para ello, es necesario que ésta sufra un preproceso de parametrización. En esta etapa previa es necesario asumir algún modelo físico, contándose con modelos auditivos y modelos articulatorios.
3. **Clasificación** Los sistemas de reconocimiento de voz pueden clasificarse según los siguientes criterios:
   a) **Entrenabilidad:** determina si el sistema necesita un entrenamiento previo antes de empezar a usarse.
   b) **Dependencia del hablante:** determina si el sistema debe entrenarse para cada usuario o es independiente del hablante.
   c) **Continuidad:** determina si el sistema puede reconocer habla continua o el usuario debe hacer pausas entre palabra y palabra.
   d) **Robustez:** determina si el sistema está diseñado para usarse con señales poco ruidosas o, por el contrario, puede funcionar aceptablemente en condiciones ruidosas, ya sea ruido de fondo, ruido procedente del canal o la presencia de voces de otras personas.
   e) **Tamaño del dominio:** determina si el sistema está diseñado para reconocer lenguaje de un dominio reducido (unos cientos de palabras p. e. reservas de vuelos o peticiones de información meteorológica) o extenso (miles de palabras).

II-B3. En Argentina: Acústica Forense: La Sección Acústica Forense de la Policía Federal Argentina, realiza estudios analíticos mediante sistemas computarizados de identificación de voz, a efectos de determinar variantes inter e intra hablantes; también se dedica a determinar variaciones de la voz que dificultan la identificación, mediante sistemas de distorsión mecánicos y/o electrónicos, y a realizar estudios comparativos entre voces del mismo género y en algunos casos, edad; todos ellos, a fin de poder realizar estudios periciales tendientes a la identificación del hablante.
Su estudio, data de Mayo de 1985, fecha en la que se forma la primera comisión de estudio e investigación sobre el análisis de la técnica de identificación de la voz, mediante el dictado de un curso a cargo del Profesor Oscar Tossi, Director del *"Speech and Hearing Sciences Research Laboratory and Institute of Voice Identification"* (Laboratorio de Investigaciones Científicas del habla y la Audición e Instituto para la Identificación de la voz) de la Universidad de Michigan – USA.

En Agosto de 1987, se crea en el mencionado Organismo Estatal, una comisión para el estudio de voces en cintas grabadas y llamadas telefónicas, a partir de la cual se fijan las normas básicas de la especialidad en nuestro país. Diez años después, en Enero de 1997 comienza formalmente a funcionar el "Gabinete de Identificación de la Voz", conformado por fonoaudiológos, ingenieros en electrónica y personal técnico de apoyo, llevando a cabo los primeros estudios periciales.
Finalizando el año 2007, se renueva el equipamiento y se adquiere un Laboratorio de Voz Humana *netamente forense*, que cuenta con software específico para la identificación de la voz, que satisface las siguientes funcionalidades:

- laboratorio de Voz
- reconocimiento simultáneo de locutores
- realización de banco de voces
- software de filtrado de audio
- grabador de audio digital

Para el análisis forense de voces, se utiliza una metodología integral y jerarquizada, donde se consideran todos y cada uno de los aspectos de la voz y del habla en general, como son por ejemplo: las características tímbricas, melódicas, fonoarticulatorias, segmentales y suprasegmentales, prosódicas semánticas y sintáctico-gramaticales. Todos los rasgos del habla y la voz de la persona son considerados. Para la aplicación del método se utiliza una computadora equipada con programas de análisis espectral de la voz, procediéndose a:

- Procesos de filtrado, normalizado y nivelado del material verbal de interés, a fin de mejorar la inteligibilidad y la visualización del material espectrográfico del habla. Aquí se analiza también el tipo de ruido presente en las grabaciones y se realizan las comparaciones de contextos ambientales de habla entre las mismas.
- Análisis de la frecuencia fundamental, contornos de F_0 [6] y variaciones melódicas de la misma.
- Análisis de las formantes del habla que supone la comparación de los procesos articulatorios similares, donde la búsqueda de coincidencias y diferencias en los movimientos incontrolados de la producción de órganos fonoarticulatorios se refleja en un aumento de formantes y marcas dinámicas en el espectrograma, que son propias e individuales en cada persona, dado que éstas se corresponden directamente con los armónicos, el tamaño y estructura de los órganos del habla y con las propiedades mecánicas de los tejidos vivos. Este análisis es especialmente eficaz en situaciones de ruido de audio, diferentes idiomas y corta duración de las muestras de voz.
- Análisis Lingüístico (aural), que involucra el análisis fonético y prosódico del habla. En éste análisis se realiza un detalle acabado de todas las características del habla de la persona, desde el aspecto articulatorio, segmental y suprasegmental, prosódico, semántico y sintáctico-gramatical.

Este método integral muestra una alta fiabilidad y permite disminuir la posibilidad de errores en la apreciación y comparación de las voces, dado que al realizarse cada uno de los análisis paso a paso, y a su vez, buscar el consenso entre unas y otras etapas del mismo, las posibilidades de error son verdaderamente muy bajas, incluso menores a las que proporcionan los métodos de identificación automática; que si bien son de ayuda en la labor forense, pueden cometer errores graves a la hora de comparar la presencia de formantes en un contexto con gran componente de ruido. Una vez realizado todos los análisis posibles, se determinará el grado de certeza en relación a la coincidencia o no de cada una de las etapas; donde el mismo puede variar desde los resultados categóricos: "Las voces se corresponden" o "Las voces no se corresponden", a toda una gama de posibles aciertos o rechazos de la correspondencia como por ejemplo "Las voces podrían corresponderse", "Es altamente probable que las voces se correspondan", "No debería descartarse la correspondencia", "No debe atribuirse como tampoco descartarse la correspondencia", etc.

II-C. Facial

La cara es un patrón biométrico que usa la apariencia para identificar o verificar la identidad de una persona. La antropometría, que tiene su basamento en el Sistema Antropométrico de Alfonse Bertillón[7], fue uno de los primeros métodos de identificación basado en el estudio de las dimensiones y proporciones de las partes del cuerpo humano; esto se hacía con el propósito de comprender los cambios físicos del hombre y obtener una medida de las diferencias entre las distintas etnias. Con objetivos, no muy alejados de las modalidades implementadas en la actualidad para el reconocimiento de rostros; viene a convertirse esta técnica del milenio pasado, en un precedente de identificación de personas basado en mediciones corporales. La identificación facial reconoce múltiples ventajas: es un método utilizado, en forma natural y con frecuencia, por la mayoría de los seres humanos; nuestra cara es de información pública, mucho de los rostros se encuentran en documentos oficiales, la web y redes sociales; el método de reconocimiento es minimamente intrusivo, al no requerir contacto directo para la captura de la imagen. Uno de los problemas que se encuentran en este método de reconocimiento, es la detección del rostro. Para identificar o reconocer una persona, necesito imprescindiblemente poder detectar la cara entre una multiplicidad de objetos con características similares a lo que el sistema conoce como cara. Para ello es muy importante tener en cuenta la iluminación, la posición de la cara, la pose de la persona, la expresión facial, el maquillaje (el color ayuda a identificar la textura y en ella obtengo mucha información para el reconocimiento), la oclusión parcial (como anteojos, barba etc). Todas estas variaciones generan un alta grado de dependencia en el Sistema de Reconocimiento.

II-C1. Aplicación: Al igual que con las huellas y ampliando su ámbito de aplicación, el reconocimiento de caras es utilizado en:

[6]Frecuencia Fundamental.

[7]Alphonse Bertillon (París - Francia 1853, Münsterlingen - Suiza 1914), policía francés, hijo de Louis-Adolphe Bertillon (médico, antropólogo y estadístico al igual que el hermano de Alphonse, Jacques Bertillon, que también fue médico y estadístico); trabajó como preceptor en Escocia y, a su regreso a Francia, trabajó para la policía de París. Investigador e impulsor de métodos de individualización antropológica.

- Seguridad y control de acceso: me permite saber quien puede entrar o evita que salga quien no debe. También es utilizado en controles fronterizos.
- Etiquetado y agrupación de fotos: permite la agrupación de imágenes de videos de larga duración, también se utiliza en Facebook, Picasa, iPhoto, entre otras aplicaciones.
- Identificación.
- Vigilancia y seguimiento de individuos: Este método de detección, permite diferenciar al individuo y realizar un seguimiento para saber por que lugares transita. Es de uso frecuente en los aeropuertos y sirve para obtener una imagen y luego proceder a su reconocimiento.
- Mejora en cámaras inteligentes: es utilizado por cámaras fotográficas, para la detección del rostro y mejorar la focalización en la toma. Esta modalidad de detección permite obtener mejores imágenes para el reconocimiento.

Se entiende que un sistema de reconocimiento facial, es una aplicación informatizada para identificar o verificar la identidad de una persona desde una imagen digital o un fotograma de video. Una de las formas es comparando características faciales, contra una base de datos.

II-C2. Técnicas Tradicionales: Los métodos de reconocimiento facial tradicionales se pueden dividir en dos grandes grupos:

1. **Holísticos:** Reconocen toda la imagen facial. Son métodos basados en correlación. El esquema de clasificación más simple, donde se utilizan modelos de comparación para el reconocimiento, es el *template matching*. El problema del *template matching* es que ha de comparar muchas características (para él, un pixel es una característica), y si se tienen en cuenta que en la base de datos se encuentran *M* personas, con *N* imágenes por persona, se observa que este método no se puede implementar en tiempo real. Por lo tanto, se trabaja con otros métodos que decorrelacionan las características entre sí para conseguir reducir el *espacio facial* en un número menor de coeficientes, que tengan un alto poder discriminatorio entre las personas. Es lo que se denomina *subespacio facial*. Ejemplos de métodos que trabajan a partir de subespacios son el Análisis de Componentes Principales (*PCA - Principal Component Analysis*) a partir de *eigenfaces*[8], el Análisis Linear Discriminante (*LDA - Linear Discriminant Analysis*) o el Discriminante Linear de Fisher (*FLD - Fisher Linear Discriminant*) a partir de *fisherfaces*[9]. [12]

   PCA La técnica PCA se considera una de las que proporciona un mayor rendimiento. Funciona proyectando las imágenes faciales sobre un espacio de facciones que engloba las variaciones significativas entre las imágenes faciales conocidas. Las facciones significativas se llaman eigenfaces, ya que son los eigenvectors, o componentes principales, del conjunto de caras. La proyección caracteriza la imagen facial de un individuo como la suma de los diferentes pesos de todas las facciones y, de la misma manera, para reconocer una imagen facial determinada sólo hará falta comparar estos pesos con aquellos de los individuos conocidos previamente. No tiene en cuenta la información de qué imágenes pertenecen a un mismo individuo. Es muy sensible a cambios en las condiciones de iluminación en diferentes imágenes de una misma persona.

   LDA El método LDA permite utilizar la información entre miembros de la misma clase (imágenes de la misma persona) para desarrollar un conjunto de vectores de características donde las variaciones entre las diferentes caras se enfatizan mientras que los cambios debidos a la iluminación, expresión facial y orientación de la cara no. Es decir, maximiza la variancia de las muestras entre clases, y la minimiza entre muestras de la misma clase.

   FLD La técnica FLD es equivalente al LDA. Los resultados obtenidos con FLD son bastante mejores que los que se puede obtener con PCA, sobre todo cuando las condiciones lumínicas varían entre el conjunto de imágenes de entrenamiento y de test, y también con cambios de expresión facial, dando más peso a zonas como los ojos, la nariz o las mejillas que a la boca, porque son zonas más invariables en las diferentes expresiones que puede tener una persona.

   Otros métodos, en vez de utilizar subespacios faciales, siguen una clasificación por redes neuronales y plantillas deformables, como EGM - Elastic graph matching.
2. **Locales o geométricos:** Se comparan diferentes características geométricas de las caras. Existen dos divisiones, la basada en los vectores característicos extraídos del perfil, y la basada en los extraídos a partir de una vista frontal. Se utilizaban mucho anteriormente pero sus resultados no son óptimos.

[8]Eigenfaces es el nombre dado a un conjunto de autovectores cuando son utilizados para resolver el problema informatico del reconocimiento facial.

[9]El discriminante linear de Fisher es una técnica "clásica" en reconocimientod de patrones, desarrollado en primera instancia por Robert Fisher 1936 por clasificación taxonómica.

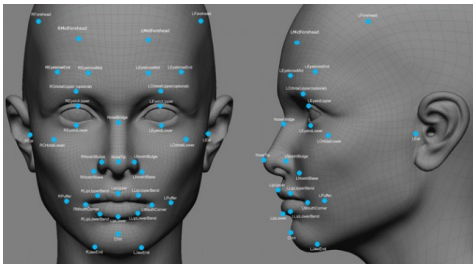

Figura 5. Biometría del Rostro

II-C3. Técnicas 3D: Últimamente se ha incrementado la tendencia del reconocimiento facial tridimensional, donde se utilizan imágenes 3D tanto en el entrenamiento como en el reconocimiento. Esta técnica, emplea sensores en tres dimensiones para captar información sobre la forma de la cara.

Esta información se utiliza posteriormente para identificar rasgos característicos del rostro como por ejemplo la barbilla, el contorno de los ojos, la nariz o los pómulos; reteniendo información espacial, a parte de la textura y la profundidad. Una ventaja del reconocimiento facial en 3D es que no se ve afectado por los cambios de iluminación, como pasa con otras técnicas. Además, otro punto a favor es que pueden reconocer una cara en diferentes ángulos, incluso de perfil. El problema es que es difícil obtener imágenes 3D fidedignas en la fase de reconocimiento, ya que los sensores 3D tienen que estar muy bien calibrados y sincronizados para adquirir la información correctamente [13]. Es por eso, que se utiliza el método de Análisis de Componentes Principales Parcial (P2CA - Partial Principal Component Analysis), derivado del PCA, donde se utilizan imágenes en 3D en la fase de entrenamiento y en la base de datos, permitiendo en la fase de test, utilizar tanto imágenes en 2D como en 3D. La técnica intenta reconstruir modelos faciales en 3D a partir de múltiples imágenes de la misma persona adquiridas mediante un sistema multicámara o a partir de aparatos 3D. Las imágenes 3D son imágenes de 180º en coordenadas cilíndricas. Otros ejemplos de técnicas 3D son 3-D Morphable Model i 3-D Face Recognition. [14]

II-C4. Técnicas de análisis de la textura de la piel: Esta técnica utiliza los detalles visuales de la piel. Analiza las líneas únicas, patrones y detalles evidentes como manchas y/o cicatrices del rostro del sujeto. Al utilizar este algoritmo se ahorra tener que recorrer toda la base de datos, ya que se puede descartar imágenes fácilmente. Hay estudios que demuestran que utilizando esta técnica, juntamente con el reconocimiento facial, el rendimiento puede aumentar hasta un 25 por ciento. [15]

Para el reconocimiento facial, independientemente del sistema que se utilice, siempre es necesario cumplimentar las siguientes etapas:

1. **Captura:** Comprende la primer etapa de todo el proceso y consiste en la captura de la imagen o el video.
2. **Detección de caras:** es necesario saber, dónde se encuentran caras en la imagen. Este proceso es el que requiere mayor cálculo y por ende es el más costoso de todo el sistema. las técnicas de detección se pueden clasificar en:
   a) Métodos basados en el conocimiento: usan las relaciones geométricas de la cara (las cuatro lineas principales).
   b) Métodos basados en características invariantes: buscan estructuras que no dependan de la iluminación, posición de la cara etc.
   c) Métodos basados en plantillas: describen una cara basándose en una serie de plantillas estándar.
   d) Métodos basados en apariencia: Mediante una base de datos anotada, se le enseña al sistema que debe detectar como cara.
3. **Extracción de parámetros:** Detectada una cara, se pueden los parámetros, ó sea aquellas características necesarias para luego realizar la comparación. Una vez obtenidos los parámetros, se genera un modelo y luego se procede a compararlos con otros perfiles biométricos que integran la base de datos. Los metodos de parametrización se pueden dividir en tres grupos:
   a) Parámetros Geométricos: Son los que miden las distancias relativas entre los puntos característicos de una cara.
   b) Parámetros de Apariencia: Este método consiste en comparar la textura de la cara o la intensidad de los pixeles que la representa. Existen dos formas de obtener parámetros de apariencia, el **Eigenfaces**, como se ha explicado es la implementación del análisis de los componentes principales (PCA) a las variaciones en la textura de la cara. Busca cuáles son las variaciones que más se presentan; y el **Fisherfaces** que se basa en el concepto de análisis de discriminación lineal (LDA) desarrollado por Fisher. Representa los componentes que permiten diferenciar las distintas clases.
   c) Método Combinado: Utiliza características de métodos basados en la geometría y características de métodos basados en la apariencia.
4. **Comparación y decisión:** La comparación puede hacerse 1:1 para saber si la persona es quien dice ser o 1:N, para saber quién es la persona porque se desconoce su identidad. Entre las distintas formas de modelar y comparar identidades, se pueden enumerar: Distancia euclideana, GMM[10], SVM[11] y las Redes Neuronales [16]. Este último si bien es muy efectivo, es de escasa implementación, por la capacidad computacional y el costo.

II-C5. Sistema de reconocimiento facial en nuestro país: MorphoFace: El MorphoFace es un sistema comercial de identificación de personas, a través del reconocimiento facial. Su objetivo principal es identificar un rostro mediante el cotejo con otros que se encuentran en la base de datos. Tiene una capacidad de almacenamiento de 100.000 registros, lo que limita su capacidad de búsqueda. Para mejorar la performance y soslayar la limitación, se trabaja previamente al cotejo del rostro, con diferentes softwares de mejoramiento de la imagen, contemplando las variaciones intra-clase significativas del sujeto, como pueden ser: los cambios propios de la edad y el crecimiento u oclusión del pelo. La captura debe realizarse ubicando a la persona de frente o ligeramente de perfil, ya que el sistema realiza una primer parametrización cuando detecta ambos ojos, obtiene la distancia existente entre ellos y la codifica. Asimismo, continúa parametrizando en base a otras características, siempre utilizando el método de parametrización geométrico. Una vez terminada la codificación, el sistema nos muestra resultados con distintos puntajes conforme la comparación realizada con los registros biométricos existentes en la base de datos; mientras más alto sea el puntaje, mayor es la posibilidad de que dos caras correspondan a la misma

[10]Gaussian Mixture Model. En probabilidades y estadística, un Modelo Generador es un modelo para generar valores aleatorios de un dato observable, típicamente dados algunos parámetros ocultos.

[11]Las máquinas de soporte vectorial, máquinas de vectores de soporte o máquinas de vector soporte (Support Vector Machines, SVMs) son un conjunto de algoritmos de aprendizaje supervisado desarrollados por Vladimir Vapnik y su equipo en los laboratorios AT&T.

persona.
La evaluación antropométrica facial, de la que se vale el sistema, está basada en la determinación de puntos característicos del rostro, definidos en términos de las características visibles o palpables del complejo facial. Distintos estudios han determinado que los ojos, la boca y la nariz se encuentran entre las partes más importantes para recordar rostros. Esto significa que presentan características distinguibles que no se pueden encontrar en otras partes como la frente o las mejillas.

II-D. Ventajas

Permite trabajar con videos, lo que ayuda a identificar rostros en situaciones cotidianas, por ejemplo si se presenta algún inconveniente en un aeropuerto o si se produce algún delito en la vía pública. Tanto en las fotos como en los videos, si la posición de la persona es frontal, las condiciones de luz apropiadas y la calidad del dispositivo de captura alta; mayor será la posibilidad de encontrar a quien se está buscando.
El MorphoFace es un sistema novedoso que puede ayudar a identificar rostros, en situaciones no colaborativas, permitiendo obtener resultados satisfactorios sin necesidad de contacto directo con la persona.

II-E. IRIS

El iris es una estructura delgada y circular que se encuentra en el ojo. Etimológicamente la palabra iris deriva del nombre de la diosa griega Iris, por la gran cantidad de colores que éste puede presentar (es el responsable de que los ojos presentes diferentes colores). **La textura fina del iris es altamente azarosa, como en las huellas dactilares y al igual que éstas, es determinada durante el proceso embrionario de gestación** [17]**.** Incluso individuos genéticamente idénticos tienen texturas del iris diferentes. El reconocimiento de iris es un método de identificación biométrica que usa técnicas de reconocimiento de patrones (en base a imágenes de irises) para identificar personas. **El patrón aleatorio del iris es único, y puede ser medido a distancia, basta la misma imagen obtenida para reconocimiento facial.**

II-E1. Enfoque: Antes de que ocurra el reconocimiento de iris, se localiza el mismo usando características del punto de referencia. Éstas, la forma distinta del iris, el aislamiento de las características, y la extracción, permiten la digitalización. La misma es apreciada en la figura 7. La localización del iris es un paso importante en su reconocimiento, porque, si está hecho incorrectamente, el ruido resultante (e.g., pestañas, reflexiones, pupilas, y párpados) en la imagen puede conducir al bajo rendimiento. [18]

II-F. Ventajas

El reconocimiento de iris tiene características muy interesantes: Es poco intrusivo respecto al reconocimiento por retina (sin embargo funciona mejor en condiciones colaborativas del individuo a identificar); es raramente obstaculizado por anteojos o lentes de contacto y es altamente universal (es una de las modalidades biométricas más universal de todas las conocidas). El órgano del ojo está bien protegido contra daños

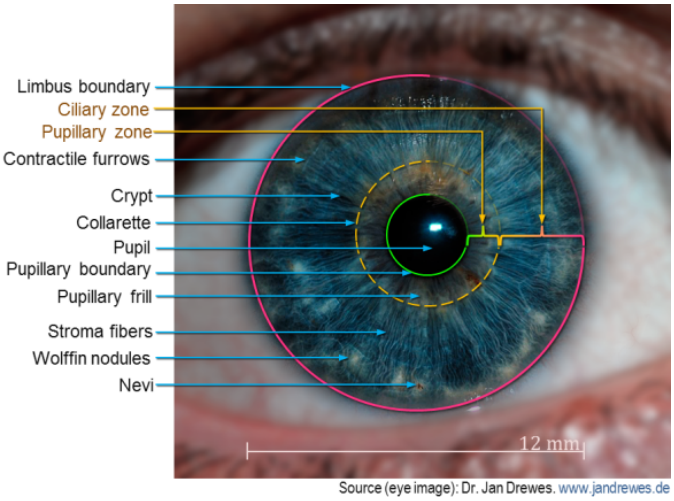

Figura 6. Esquema del Iris

y desgaste por la córnea. En otras modalidades esto no ocurre: en las huellas dactilares por ejemplo, es muy común encontrar desgaste de la epidermis por trabajos manuales, que pueden dificultar su obtención; en las caras, las cirugías con intervención osea, el maquillaje permanente, la edad y hasta accidentes con desfiguración de rostros, son factores que pueden influir a la hora del reconocimiento; y en menor medida, hasta la voz, por padecimiento de diferentes enfermedades asociadas al tracto vocal, puede verse afectada.
Los métodos de comparación son muy rápidos y esto hace, que junto a la bajísima tasa de error, sea apropiado para poblaciones grandes con bases de datos robustas [19]. Sin embargo, su implementación sigue siendo muy costosa y en consecuencia su incorporación a los sistemas biométricos utilizados en pos de la Seguridad Pública, todavía es una materia pendiente.
La captura de un iris es similar a la obtención de una fotografía. Se puede obtener a distancias de entre los 10 cm y varios metros, aunque en este último caso los dispositivos de captura deben ser más sofisticados. El reconocimiento de iris comienza en 1886 con Bertillon quien advierte que: ün dibujo detallado de la aureola del iris humano podría ser útil para identificar a seres humanos".

II-F1. Reconocimiento: En términos generales el reconocimiento de Iris consta de las siguientes etapas:

1. Adquisición de la imagen: Se realiza generalmente por medio de un sensor de captura de la imagen, siendo de suma importancia las condiciones lumínicas. En la mayoría de los sistemas comerciales se utilizan leds

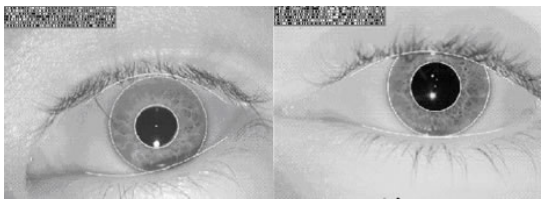

Figura 7. Iris Localizados con IrisCodes®

como fuente de iluminación, dado que tienen un ancho de banda relativamente pequeño.
2. Procesamiento (Localización / Segmentación): Cuando se captura la imagen del iris, se obtiene mucha información que no es iris, como por ejemplo párpados y pestañas que obstruyen la imagen y generan ruido; en principio se localiza el iris, descartando todo aquello que no es útil para el reconocimiento y se segmenta la porción con la que se va a trabajar. Una vez segmentada la imagen del iris, se está en condiciones de comprarlo con el iris registrado en una base de datos
3. Generación de plantillas: Lo que se busca en esta etapa es la representación del iris con independencia de los problemas de: iluminación, enfoque y dilatación de la pupila. Se genera la plantilla o iris code, con el que se va a realizar la comparación. Para ello, se trabaja con la textura del iris que se analiza por una serie de ondulas.
4. Comparación: Finalmente se procede a comparar el iris code obtenido con los obrantes en la base de datos. Para comparar los dos IrisCode, se utiliza una medida llamada Distancia de Hamming, que consiste en calcular la cantidad de bits diferentes, dividido la cantidad de bits comparados. Durante esta comparación es necesario tener en cuenta la máscara de zonas válidas del iris. Las regiones marcadas como inválidas, no son comparadas, disminuyendo la cantidad de bits totales a comparar.

El reconocimiento por Iris es mayormente utilizado como mecanismo de control de acceso ya que, en materia de seguridad e investigación forense, en el País, todavía es un sistema a implementar. [19]

El sensor de la figura 8, es para la captura del iris. La captura se realiza a una distancia entre 4.7 y 5.3 cm. Cuenta con certificaciones: Eye safety standard (IEC 62471:2006-07), RoHS, FCC-Class B*, IP54* [20]. Al igual que otros sensores, tiene conexión USB y puede alimentarse del puerto USB del teléfono móvil.

Figura 8. Iris Sensor MK 2120U

III. Sistema SIBIOS

La masificación de las actualizaciones tecnológicas coadyuvadas con la ampliación de las bases de datos, allanó el camino para interconectar todas las bases de datos de las fuerzas de seguridad del País, generando una Base de Datos Federalizada. El proyecto que se inició en el año 2010 y un año después encontró forma, buscó sanear la brecha que existía y afectaba considerablemente la Seguridad Pública, con búsquedas jurisdiccionales desconectadas entre sí, por poseer cada fuerza de seguridad (Nacional/Provincial) bases de datos propietarias e individuales. Así, si un delito era cometido en la Provincia de Chaco, por una persona natural de Rio Negro, aunque se poseía evidencia biométrica para identificarla, las posibilidades de lograr una identificación positiva eran casi nulas, ya que sus registros se encontraban en la Provincia de origen y la solicitud de búsqueda sólo se realizaba donde se había cometido el delito; y de extender la misma a todo el País, conllevaba una tarea de años. La tecnología permitía la conexión (mediante diferentes mecanismos) de las distintas Bases de Datos, y en consecuencia la posibilidad de disponer de sus registros en todo el País. De esta manera, a través de la creación del SISTEMA FEDERAL DE IDENTIFICACION BIOMETRICA PARA LA SEGURIDAD (SIBIOS), se lanzó una nueva ofensiva contra la criminalidad, que adquirió fuerza de ley a través del Decreto 1766/2011. [21].

III-A. SIBIOS: Importancia, antecedentes normativos

Por prerrogativa de la LEY Nº 17.671 DE IDENTIFICACION, REGISTRO Y CLASIFICACION DEL POTENCIAL HUMANO NACIONAL, promulgada en el año 1968, la Policía Federal Argentina tenía a su cargo, por facultad delegada del Registro Nacional de las Personas, el otorgamiento de pasaportes y la emisión de cedulas de identidad. Con ello, día a día alimentaba una base de datos de huellas dactilares y un sistema de registros patronímicos, asegurándose así la fidelidad de sus archivos civiles, por ser aportados directamente, con carácter de declaración jurada, por su propietario; sin embargo, la autenticidad de los datos sólo podía ser validada por el Registro Nacional de las Personas, a quién asiduamente se pedía colaboración. Durante décadas y décadas se ha conformado el archivo decadactilar más importante de Latinoamerica, conocido mundialmente por su capacidad de almacenamiento. A pesar de la unanimidad en la importancia del potencial resguardado por la fuerza de seguridad federal, dichos registros solo eran funcionales a su jurisdicción. En el año 2011, mediante el decreto 261 se deroga la facultad de emitir pasaportes a la Policía Federal Argentina y contemporáneamente se federaliza la utilización de las bases de datos de registros biométricos que existían bajo su órbita, materializándose la decisión a través de la promulgación del Decreto, que da nacimiento al SIBIOS, poniendo a disposición del país registros únicos de identificación humana y consecuentemente las ventajas de búsqueda con las que cuenta el Sistema AFIS. Como bien se enuncia en la letra del cuerpo normativo, el SIBIOS tiene por objeto prestar un servicio centralizado de información respecto de los registros patronímicos y biológicos individuales y reconoce como Unidad de Coordinación al MINISTERIO

DE SEGURIDAD. En uno de sus considerandos, la norma establece que *resulta imprescindible usufructuar al máximo las herramientas tecnológicas en dotación, teniendo en cuenta que la utilización de técnicas biométricas resulta un aporte fundamental a las funciones de seguridad pública en materia preventiva y respecto de competencias de investigación y policía científica, conforme las directivas de las autoridades judiciales.* Expresando, coincidentemente esta premisa, uno de los objetivos del presente trabajo. Siguiendo con el análisis del cuerpo normativo, se encuentra que en el mismo se establece que El REGISTRO NACIONAL DE LAS PERSONAS brindará la información biométrica necesaria para satisfacer los requerimientos de identificación que formulen los distintos usuarios. De esta manera, adquiere singular relevancia los datos que aporta, ya que ofrece una dualidad de destacables beneficios: por un lado abastece de forma continua e ininterrumpida las distintas bases de datos y por otro brinda la tan anhelada veracidad a los registros allí almacenados. Si bien solo el RENAPER puede autenticar la filiación de una persona, no es el único organismo, que en forma colaborativa aporta registros a las bases sino, todo usuario adherido al Sistema carga sus diferentes registros. En el mencionado Decreto se invita a las Provincias y a la Ciudad Autónoma de Buenos Aires a adherirse, contando en la actualidad con 24 Provincias adheridas. La consulta a la Base de Datos Nacional viabiliza la posibilidad de establecer la identidad de una persona, por sus características biométricas, de modo irrefutable, prescindiendo de cualquier otro dato.

IV. La Solución: Dinámica de una propuesta

Luego de analizar cada una de las técnicas biométricas de mayor auge en la actualidad, su ámbito de aplicación, su conformación y hasta ventajas y desventajas que representan; es momento de esbozar una idea de como se puede mejorar la utilización de los sistemas biométricos aludidos, en pos de la Seguridad Pública. Para ello es necesario destacar una serie de puntos, que serán de suma importancia para la solución propuesta.

IV-A. Concientización sobre la importancia de una Base Única de Datos a nivel Gubernamental

Una situación que es de común ocurrencia en el Estado Nacional, es la existencia de las múltiples bases de datos con la misma información, dentro y fuera de un mismo Organismo. Esto se debe, en primera instancia, a que en su génesis, no había mucha comunicación entre las distintas partes integrantes. Cada una de ellas, acorde a su estructura laboral, almacenaba registros de interés, que con el tiempo pasaron de ser pequeños archivos para convertirse en bases de datos con volúmenes importantes. La necesidad de implementar, con tiempos muy acotados, y esquivando la burocracia o intereses políticos contrarios, un sistema de registro y búsqueda más eficaz, hicieron que la duplicidad de datos vaya aumentando cada vez más.

Se ha descripto anteriormente, como el SIBIOS Federalizó las bases de datos biométricos-filiares, que poseían las Policías Provinciales de todo el País y las fuerzas federales como: Policía Federal, Gendarmería Nacional, Prefectura Naval y Policía Aeroportuaria; sin embargo, existe todavía un camino por zanjar, en idéntico sentido, y comprende a Organismos estatales bajo la órbita de otros Ministerios.

A continuación, se hará una enumeración no taxativa, pero sí significativa, de los Organismos que mantienen la duplicidad de datos, obteniendo diariamente, dentro de su jurisdicción operativa, distintos registros para abastecer archivos propios. Dichos registros, también se encuentran en otras bases de datos, y en cada oportunidad seguramente se almacenó junto a ellos diferente información, que de combinarse, indiscutiblemente sería de suma importancia para todas las partes.

IV-A1. ReNaPer: [12] En base a lo expuesto anteriormente, se concluye que el único organismo que genera y administra los datos patronímicos auténticos de las personas, es el ReNaPer, de donde se obtienen en forma fehaciente y unívoca registros de filiación y la biometría que corroborará la identidad de una persona. El ReNaPer como parte de su circuito para el trámite del DNI[13] realiza una toma fotográfica de frente, toma las huellas digitales y la firma.

IV-A2. Fuerzas Federales: Datos Patronímicos-Biométricos: Las fuerzas federales tienen su ámbito de respuesta sobre los delitos federales (secuestro extorsivo, tráfico de drogas, entre otros), en consecuencia, pueden alimentar sus bases de datos con independencia de cualquier otro Organismo.

IV-A3. DNR: [14] El Registro Nacional de Reincidencia es un organismo dependiente del Ministerio de Justicia y Derechos Humanos de la Nación. Su misión es centralizar la información referida a los procesos penales sustanciados en cualquier jurisdicción del país, conforme el régimen que regula la Ley 22.117.

IV-A4. AFIP: [15] Implementó hace ya un tiempo, el registro de datos biométricos para evitar documentos apócrifos y suplantación de identidad: *"... Esta información es registrada, para una identificación más segura con el objeto de evitar la utilización de documentación apócrifa y preservar la seguridad jurídica y patrimonial de las personas ajenas a la comisión de dichos fraudes."* [22].

IV-A5. ReNAr: [16] El ReNAr, toma las huellas dactilares de los aplicantes a los efectos de ser utilizados en sistemas biométricos: *"Se registrarán de cada individuo una imagen facial de toma frontal, sin obstrucciones de elementos en el rostro, y la totalidad de dedos de ambas manos en forma plana, ambos con la calidad y métodos técnicos que permitan su utilización en sistemas automatizados de reconocimiento e identificación biométrica acorde a estándares internacionales en la materia."* [23]

IV-A6. DNM: [17] La DNM registra los ingresos y egresos de personas al país; ejerce el poder de policía migratorio, y decide sobre la admisión de personas al territorio nacional. Para realizar esta tarea, se basa en la biometría, tanto sea decadactilar como facial. [24]. Registra la información en los

[12]Registros Nacional de las Personas.
[13]Documento Nacional de Identidad.
[14]Dirección Nacional de Reincidencia.
[15]Administración Federal de Ingresos Públicos.
[16]Registro Nacional de Armas.
[17]Dirección Nacional de Migraciones.

distintos puntos, sacando una foto y tomando la huella con sensores biométricos.

IV-A7. ANSES: [18] El ANSES, con el propósito de mitigar los riesgos en la asignación de beneficios sociales y/o previsionales, implementó un esquema biométrico: "*Es un sistema que permite reconocer la identidad de las personas a través de la huella digital, para facilitar la realización de trámites en ANSES y entidades bancarias. Está destinado a los jubilados, pensionados y/o apoderados del SIPA*[19] *y a los titulares y/o apoderados de Pensiones no Contributivas que cobran sus haberes a través de la Cuenta Gratuita Previsional.*" [25]

IV-B. Sistema Automatizado de Informes

La presente solución consta de dos partes:

1. La creación de una base de datos biométrica-filial nacional, que integre a todos los Organismos del Estado, proveyendo la misma, datos auténticos con información entrecruzada, aportada directamente por cada entidad acorde a su competencia, la cuál se encargará de nutrir directamente a un sistema automatizado de informes, que comprenderá la segunda parte de la solución.
2. Una aplicación de arquitectura cliente-servidor, que pueda enlazar todos los Sistemas Biométricos que actualmente existen en el Organismo de contralor de la Seguridad Pública Nacional, a fin de incorporar una modalidad de búsqueda multibiométrica, que utilice la totalidad de los datos obtenidos de la persona, generando un sistema robusto con escasa tasa de vulnerabilidad.

Esta solución, totalmente alcanzable en el contexto actual, requiere por un lado, para la generación de la Base de Datos, tener en cuenta el formato de los archivos y el protocolo de transferencia de datos. Respecto al formato de archivo, se propone la unicidad del mismo para evitar problemas de compatibilidad, al respecto, el instituto NIST[20] junto al FBI, creo un estandard de formato de archivo para el intercambio de información entre las fuerzas de seguridad, denominado ANSI/NIST-ITL [26]. Este formato permite que un solo archivo pueda contener más de un registro con sus respectivos campos: datos alfabéticos de la persona, su fotografía y sus huellas dactilares. Si la resolución de dicha toma fue a 500 DPI, el formato de almacenamiento es WSQ[21] [27], si la resolución de la toma fue a 1000 DPI, el formato de almacenamiento es JPEG 2000. [28]. Actualmente es el formato utilizado para el intercambio de la información entre las fuerzas de seguridad de los distintos países e Interpol. Las revisiones mas nuevas de este estándard contemplan la voz. [29].

En lo referente a la transferencia de datos, se propone la utilización de vínculos exclusivos y de no poder utilizarlos por los costos, se puede utilizar Internet, implementado redes VPN[22] sobre la misma.

Figura 9. WebCam para toma fotográfica.

Por otro lado para la creación del Sistema automatizado de informes se propone la siguiente arquitectura:

1. **Cliente** Consistiría en una terminal de adquisición de muestras biométricas. Esto es, un CPU de características estándard (lo que lo hace económico), la cual estaría provista por distintos dispositivos de captura biométrica, a saber:
   - Una cámara de resolución HD o full HD (puede ser una webcam), se pide que tenga una sensibilidad por encima de 400 ISO, ya que es posible que las condiciones de luminosidad en el momento de la captura fotográfica, no sean las adecuadas. Figura 9.
   - Un scanner de huellas dactilares, certificado por FBI, con una resolución de escaneo no menor a 500 DPI. Con reconocimiento y análisis de la calidad de la toma. Figura 10.
   - Un pad de firma, a los efectos del registro de la firma hológrafa. Figura 11
   - Un micrófono, con un ancho de banda ente 20 y 20.000 Hz.

   El sistema utilizará un vinculo cifrado con el servidor (podría ser TLS[23]), sumado quizás a la arquitectura existente de vínculo de comunicaciones (VPN). Se requiere acceso de usuario y contraseña, o se puede sumar un token como un tercer factor de autenticación. Una vez que la información ha sido capturada, se enviará al servidor, empaquetada en un archivo con formato NIST.
2. **Servidor** Podría consistir en un software de workflow (por ejemplo de uno opensource[24]) que recibe la infor-

[18] Administración Nacional de la Seguridad Social.

[19] Sistema Integrado Previsional Argentino.

[20] National Institute of Standars and Technology.

[21] *Wavelet Scalar Quantization* - Cuantificación Escalar de Ondículas: Algoritmo de compresión utilizado en las imágenes de huellas dactilares en escala de grises. Este método de compresión es preferido sobre los algoritmos de compresión estándar, como JPEG, porque en las mismas proporciones de compresión, el WSQ no presenta los "artefactos de bloqueo" o pérdida de las características a escala fina.

[22] *Virtual Private Network* - Red Privada Virtual: Se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

[23] Protocolos criptográficos que proporcionan comunicaciones seguras por una red. Se usa criptografía asimétrica para autentificar a la contraparte con quien se están comunicando, y para intercambiar una llave simétrica. Esta sesión es luego usada para cifrar el flujo de datos entre las partes. Esto permite la confidencialidad del dato/mensaje, y códigos de autenticación de mensajes para integridad y como un producto lateral, autenticación del mensaje.

[24] ProcessMaker: www.processmaker.com

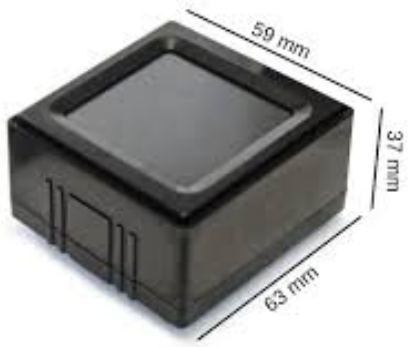

Figura 10. IB Watson Mini Dual Fingerprint Scanner

Figura 11. Pad de firmas.

mación enviada por la terminal de captura y la procesa para su transferencia a cada sistema biométrico, a fin de que puede ser procesado y almacenado.

El sensor de la figura 10, es un ejemplo de sensor biométrico, cuenta con certificaciones FCC[25], CE[26], ICES-003 Class A[27], IEC 61000-4-2[28], RoHS[29], IQS[30] [30]. Este sensor que también puede utilizarse en ambientes militares, es del tipo capacitivo, y de muy poco peso.

En el momento de la adquisición, se debe asegurar el orden de los dedos en la toma y consignar si falta algún dedo durante la misma. Durante el tiempo de la toma, el software de captura, realiza el cotejo del orden y de calidad de la toma. El tamaño y el poco peso de este sensor lo hace ideal para la integración con un teléfono celular.

Cada una de las etapas del workflow, que corresponderán a cada Sistema Biométrico, recibirá el patrón que corresponda y emitirá su dictamen y/o informe, con los resultados de su búsqueda y la información relacionada a ese patrón. Al finalizar el circuito, se unificarán en un documento en formato PDF, firmado digitalmente, las conclusiones de cada sistema y la totalidad de la información que se tenga de la persona. Esta forma de identificación, a través de un sistema multibiométrico, permite obtener con mayor certeza una respuesta identificatoria. Adicionalmente, para brindarle una mayor seguridad al documento papel (de imprimirse el informe en cuestión), se puede agregar un código QR con la información que figura en el documento digital.

[25]Federal Communications Commision. Comisión Federal de Comunicaciones

[26]Conformité Européene - Conformidad Europea.

[27]Interference-Causing Equipment Standard.

[28]Standard Testing for electrostatic discharge immunity.

[29]Restriction of Hazardous Substances Directive.

[30]Image Quality Specification. Certificacion otorgada por el FBI.

V. Trabajo Futuro

Para la implementación de la solución propuesta, se requiería de una terminal biométrica para la parte *cliente*, y del software opensource *processmaker* para la parte *servidor*.

V-A. Cliente

El cliente consistirá en una terminal con Windows 10™. El lenguaje de programación de la solución podría ser cualquiera que pueda proveer una solución monolítica (por sus características de seguridad y de fácil actualización remota). Ejemplos: C# o JAVA. El software cliente deberá permitir trabajar en modalidad *offline*, para complementar aquellas situaciones en las cuales el vínculo se encuentre inoperativo temporalmente. Por esta misma causa, debería contemplarse un subsistema de colas para el manejo de los archivos NIST al servidor. Adicionalmente, para el momento de la obtención del patrón biométrico, el software deberá permitir realizar controles de calidad de la muestra biométrica obtenida (huella, foto, o voz).

V-B. Servidor

A los efectos de balancear factores de disponibilidad y costos, se implementaría un esquema de *cluster* HA[31], y dos *storage* implementados con FreeNAS [31]. Para ambos servidores se prepará el cliente de iSCSI. Dicho cliente, conjuntamente con los procesos de montado de *filesystems* y asignado de IP dinámica de servicio, se configurarían en cada nodo del *cluster* HA. Asimismo deberá ser obligatorio, la utilización de *fencing*[32] para evitar acceso simultáneo al *storage* provocando así corrupción de datos.

V-B1. Aplicación: Consistirá en dos servidores en HA con el software de servidor web *Apache* con soporte para *PHP* [32]. Se recomienda que los *filesystems* que alojen la aplicación sean formateados con XFS[33]. Como software de

[31]Alta Disponibilidad.

[32]Método utilizado para llevar al *cluster* a un estado conocido.

[33]XFS es un sistema de archivos de 64 bits con *journaling* de alto rendimiento creado por SGI (antiguamente Silicon Graphics Inc.) para su implementación de UNIX llamada IRIX. En mayo de 2000, SGI liberó XFS bajo una licencia de código abierto.

workflow se sugiere el denominado *Processmaker*, ya que es *opensource*, de arquitectura abierta, que permite interactuar con la interfaz web nativa, o por medio de Webservices[34] o REST[35], lo que a su vez permite la comuicación con interfaces customizadas o con otros sistemas.

V-B2. Base de Datos: Consistirá en dos servidores en HA con el RDBMS MySQL instalado. Se recomienda que los *filesystems* que alojen las tablas, también sean formateados con XFS.

V-B3. Almacenamiento: El almacenamiento se implementará con dos servidores, uno para base de datos y otro para aplicación. El mismo debe contemplar la mayor cantidad de discos posibles. Cada uno de los servidores iniciarán su arranque con un *pen drive* con FreeNAS formateado. FreeNAS provee una administración remota WEB para la caja de discos. Otra ventaja de esta solución, es que los discos formen parte de una estructura controlada por ZFS[36], configurando así un RAID 6[37]. El acceso será por medio de iSCSI [38] proveyendo así, una comunicación estándar y compatible.

V-B4. PKI: [39] Para darle una mayor seguridad a los informes emitidos, se utilizará la infraestructura PKI. El esquema de PKI se puede implementar por medio de *firma digital* o *firma electrónica*. La diferencia entre ambos mecanismos consiste en quien ejerce la potestad de CA[40].

- **Firma Digital:** La CA son organismos del Estado Nacional. [33]. El organismo debe poseer una AR[41] certificada. La AR del organismo es responsable de la generación de los certificados de los usuarios y de firmarlos.
- **Firma Electrónica:** La función de CA es ejercida por una dependencia interna de la estructura organizativa de una empresa u organismo. A su vez exige un esquema de dos capas, un servidor para la CA y un servidor para la AR. AR crea su certificado que es firmado por la CA, luego el servidor de la CA se apaga y se retiran los discos para su almacenamiento en una caja fuerte. La AR se utiliza para la generación de los certificados de los usuarios (y su firmado por la AR).

V-C. Programación

Se deberá tener en cuenta:

- El workflow del circuito en la aplicación.
- Los procesos *Batch*[42].
- La programación de automatismos dentro del mismo workflow (triggers). [34]
- La interfaz ABM[43] para el manejo de los certificados de los usuarios.
- Si bien Processmaker provee de una interfaz web, es preferible una interfaz customizada (por WebServices o REST) para cada una de las etapas del circuito.

VI. Conclusión

El sistema multibiométrico abastecido por una base de datos con unicidad de registros, ha sido una solución estudiada detalladamente y la experiencia en el campo me permitió corroborar la factibilidad de su implementación, en sentido técnico. Sin embargo, no puedo desconocer que su desarrollo conlleva una decisión política, que muchas veces es mas difícil de obtener que la siempre cuestionada proyección económica. Lograr que los Organismos compartan su información para alimentar una base única, y que a su vez, la utilicen, más allá de la potestad de administración que cada uno posea sobre la misma, parece una tarea difícil de alcanzar, aunque no imposible. Luego de infructuosos intentos, ha quedado demostrado que el Estado Nacional, está dando sus primeros pasos hacia el objetivo de mejorar la seguridad pública en tal sentido. Esta solución acompaña y mejora esa decisión, siempre en pos de una mejor Nación.

Agradecimientos

A los docentes, que fueron una fuente de inspiración y consulta inagotables. A mi esposa, por su apoyo incondicional.

Referencias

[1] D. Gallo. La inseguridad es la mayor preocupación. [Online]. Available: http://www.lanacion.com.ar/1496430-la-inseguridad-es-la-mayor-preocupacion

[2] La seguridad es nuestra mayor preocupación. [Online]. Available: http://www.infobae.com/2014/04/25/1559832-la-seguridad-es-nuestra-mayor-preocupacion/

[3] Human Dignity. [Online]. Available: https://en.wikipedia.org/wiki/Biometrics#Human_Dignity

[34] Un servicio web (en inglés, *web service* o seb services) es una tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. Distintas aplicaciones de software desarrolladas en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma, pueden utilizar los servicios web para intercambiar datos en redes de ordenadores como Internet.

[35] La Transferencia de Estado Representacional (en inglés *Representational State Transfer*) o REST es un estilo de arquitectura software para sistemas hipermedia distribuidos como la World Wide Web. El término se originó en el año 2000, en una tesis doctoral sobre la web escrita por *Roy Fielding*, uno de los principales autores de la especificación del protocolo HTTP y ha pasado a ser ampliamente utilizado por la comunidad de desarrollo.

[36] ZFS es un sistema de archivos y volúmenes desarrollado por Sun Microsystems para su sistema operativo Solaris. El significado original era *Zettabyte File System*, pero ahora es un acrónimo recursivo. De 128 bits, ZFS destaca por su gran capacidad, integración de los conceptos anteriormente separados de sistema de ficheros y administrador de volúmenes en un solo producto, nueva estructura sobre el disco, sistemas de archivos ligeros y una administración de espacios de almacenamiento sencilla.

[37] En informática, el acrónimo RAID (del inglés *Redundant Array of Inexpensive Disks* o, más común a día de hoy, *Redundant Array of Independent Disks*), traducido como çonjunto redundante de discos Independientes", hace referencia a un sistema de almacenamiento de datos en tiempo real que utiliza múltiples unidades de almacenamiento de datos (discos duros o SSD) entre los que se distribuyen o replican los datos. Dependiendo de su configuración (a la que suele llamarse "nivel"), los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor throughput (rendimiento) y mayor capacidad.

[38] iSCSI (Abreviatura de Internet SCSI) es un estándar que permite el uso del protocolo SCSI sobre redes TCP/IP.

[39] En criptografía, una infraestructura de clave pública (o, en inglés, PKI, *Public Key Infrastructure*) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

[40] Autoridad de Certificación.

[41] Autoridad de registro.

[42] Se conoce como sistema por lotes (en inglés *batch processing*), o modo batch, a la ejecución de un programa sin el control o supervisión directa del usuario (que se denomina procesamiento interactivo). Este tipo de programas se caracterizan porque su ejecución no precisa ningún tipo de interacción con el usuario.

[43] Acrónimo para las opciones de Alta, Baja y Modificaciones.

[4] J. Crettaz. DNI: la privacidad, en riesgo por la identificación biométrica. [Online]. Available: http://www.lanacion.com.ar/1647826-dni-la-privacidad-en-riesgo-por-la-identificacion-biometrica

[5] P. A. L. Ricardo Rosset, *El ABC del Dactilóscopo*. Editorial Policial, 2008, cap. VI, Pag 59-61.

[6] ——, *El ABC del Dactilóscopo*. Editorial Policial, 2008, cap. VI, Pag 59-61.

[7] Facial Recognition System. [Online]. Available: http://en.wikipedia.org/wiki/Facial_recognition_system

[8] What device categories are certified? [Online]. Available: https://www.fbibiospecs.cjis.gov/Certifications/FAQ

[9] Superintendencia de Policia Cientifica. [Online]. Available: https://prezi.com/kilst0xbzgem/superintendecia-de-policia-cientifica/

[10] "El sistema AFIS de Policia Federal Argentina." [Online]. Available: http://www.lacapital.com.ar/jornadas-actualizacion-ciencias-criminalisticas-n968368.html

[11] Reconocimiento de Locutores. [Online]. Available: https://es.wikipedia.org/wiki/Reconocimiento_de_locutores

[12] J. H. Peter N. Belhumeur and D. J. Kriegman. Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection. [Online]. Available: ftp://ftp.idiap.ch/pub/courses/EE-700/material/17-10-2012/fisherface-pami97.pdf

[13] Sistema de reconocimiento facial - Técnicas 3D. [Online]. Available: https://es.wikipedia.org/wiki/Sistema_de_reconocimiento_facial#T.C3.A9cnicas_3D

[14] Delac, K., Grgic, M., Liatsis, P., Ed., *Appearance-based Statistical Methods for Face Recognition*.

[15] M. W. Pontin. Better Face-Recognition Software. [Online]. Available: https://www.technologyreview.com/s/407976/better-face-recognition-software/

[16] W. M. Campbell, D.E.Sturim,D.A.Reynolds,A.Solomonoff. SVM BASED SPEAKER VERIFICATION USING A GMM SUPER VECTOR KERNEL AND NAP VARIABILITY COMPENSATION. [Online]. Available: https://www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/060514_CampbellW.pdf

[17] Iris recognition - Advantages. [Online]. Available: https://en.wikipedia.org/wiki/Iris_recognition#Advantages

[18] Reconocimiento del Iris. [Online]. Available: http://www.biometria.gov.ar/metodos-biometricos/iris.aspx

[19] Departamento de Computación - Facultad de Ciencias Exactas - Universidad de Buenos Aires. Identificación de Personas por Reconocimiento de Iris. [Online]. Available: http://www.biometria.gov.ar/media/46163/uba_reconocimiento_iris.pdf

[20] Grado de proteccion IP. [Online]. Available: https://es.wikipedia.org/wiki/Grado_de_protecci%C3%B3n_IP

[21] Sistema Federal de Identificación para la Seguridad. [Online]. Available: https://es.wikipedia.org/wiki/Sistema_Federal_de_Identificaci%C3%B3n_Biom%C3\%A9trica_para_la_Seguridad_(SIBIOS)

[22] ABC - Consultas y Respuestas Frecuentes sobre Normativa, Aplicativos y Sistemas. - Datos Biométricos. [Online]. Available: http://www.afip.gob.ar/genericos/guiavirtual/directorio_subcategoria.aspx?id_nivel1=557&id_nivel2=1684

[23] Requisito para acceder a la Condición de Legítimo Usuario de Armas de Fuego de Uso Civil o de Uso Civil Condicional. [Online]. Available: http://www.renar.gov.ar/index_seccion.php?seccion=legislacion_visualizar&m=3&ley=32&disp=si

[24] "Acerca de la DNM." [Online]. Available: http://www.migraciones.gov.ar/accesible/indexP.php?acerca

[25] Mi Huella. [Online]. Available: http://www.anses.gob.ar/prestacion/mi-huella-201

[26] Especificación del estandard ANSI-NIST/ITL. [Online]. Available: https://www.nist.gov/programs-projects/ansinist-itl-standard

[27] Especificación del estandard WSQ. [Online]. Available: https://www.fbibiospecs.cjis.gov/Document/Get?fileName=WSQ_Gray-scale_Specification_Version_3_1_Final.pdf

[28] Estandard JPEG 2000. [Online]. Available: https://es.wikipedia.org/wiki/JPEG_2000

[29] Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information - ANSI/NIST-ITL 1-2011 Update:2015. [Online]. Available: http://biometrics.nist.gov/cs_links/standard/ansi_2015/ANSI_NIST_ITL_1.pdf

[30] Certificacion IQS. [Online]. Available: http://www.integratedbiometrics.com/wp-content/uploads/2016/01/Watson-Mini-Certifications.pdf

[31] Almacenamiento con FreeNAS. [Online]. Available: http://www.freenas.org/

[32] Requerimientos de instalación para Processmaker. [Online]. Available: http://wiki.processmaker.com/3.0/ProcessMaker_Installation_Requirements

[33] Ley de Firma Digital. [Online]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

[34] Triggers. [Online]. Available: http://wiki.processmaker.com/3.0/Triggers

ÍNDICE DE FIGURAS

Pablo Niklas Estudiante avanzado de la Licenciatura de Tecnología de la Información correspondiente a la Facultad de Ingeniería de la Universidad de Palermo. Se desempeña hace mas de 15 años en la Superintendencia de Policía Científica de la Policía Federal Argentina. Desde hace cuatro años, se desempeña en una sección específica de biometría investigando nuevas tecnologías biométricas. Asistió a los Congresos Internacionales de Biometría de la República Argentina $CIBRA$ entre los años 2006 al 2011, también asistió a la conferencia mundial de Morpho Sagem año 2013 en París, Francia. Tiene como hobby coleccionar computadoras de los 80's y la fotografía[44].

[44] www.pabloniklas.com