Ciencia, Docencia y Tecnología Suplemento
Vol. 4 | Nº 4 (2014) ISSN 2250-4559

PID 7035

Identificación de personas mediante Sistemas Biométricos. Estudio de factibilidad y su implementación en organismos estatales

Alvez, Carlos Eduardo; Benedetto, Marcelo Gabriel; Etchart, Graciela Raquel; Luna, Lucas Javier; Leal, Carlos Rafael; Fernández, Miguel Antonio; Berón, Gustavo Luis; Loggio, Sebastián René

AUTORES: Facultad de Ciencias de la Administración. Universidad Nacional de Entre Ríos (UNER), Argentina.
CONTACTO: caralv@fcad.uner.edu.ar

Resumen
En la actualidad, la biometría se encuentra presente en aplicaciones tales como acceso seguro a computadoras, redes, bases de datos, control horario y acceso físico a salas de acceso restringido, entre otros. Los organismos estatales disponen de información de diverso tipo, en volúmenes importantes y con distintos niveles de privacidad. El control de acceso a esta información, generalmente, se efectúa a través de mecanismos tradicionales como lo son las claves y tarjetas magnéticas. Se propone estudiar el funcionamiento de los sistemas biométricos y efectuar un estudio comparativo de los diversos sistemas. Además se prevé, un estudio de campo sobre un organismo estatal en áreas de la administración que requieren o deberían requerir procesos de identificación seguros. Se diagnosticarán las dificultades actuales en los procedimientos de dichas áreas para establecer sus necesidades. Se propondrán soluciones basados en sistemas biométricos, para los procedimientos que requieren de autentificación. Se desarrollarán e implementarán estos sistemas (software) en dispositivos genéricos (hardware). El desarrollo e implementación de estos controles en áreas críticas de organismos gubernamentales permitirá una mayor seguridad y control en el acceso a las mismas. Además, un desarrollo personalizado y ajustado a los estándares internacionales permitirá adecuar los controles a los requerimientos específicos de cada área.

Palabras clave: sistemas biométricos; identificación de personas; organismos estatales; seguridad y control.

I. Introducción

Muchos de los sistemas biométricos que se utilizan en la actualidad, se basan en ideas que fueron originalmente concebidas hace cientos e incluso miles de años. Uno de los más viejos y básicos ejemplos de una característica utilizada para el reconocimiento en los seres humanos es el rostro. Desde los principios de la civilización, los seres humanos han utilizado los rostros para identificar a los individuos conocidos (familiar) y desconocidos (no familiar).

El concepto de reconocimiento de humano a humano a partir de lo conductual, como lo es el paso y la voz es también analizado por la biometría. Los individuos utilizan estas características, en cierto modo de manera inconsciente, para reconocer a individuos sobre una base cotidiana. También se han

utilizado otras características a través de la historia de la civilización como medios más formales de reconocimiento [1].

Las investigaciones científicas acerca de la biometría, comienzan a principios del siglo pasado con el fin de buscar un sistema de identificación de personas con fines judiciales. Con el comienzo de estas investigaciones, se producen importantes avances y se comienza a utilizar los rasgos morfológicos únicos en cada persona para la identificación.

De esta manera, las características físicas del ser humano se han utilizado desde hace más de un siglo en el ámbito forense de evidencias biométricas: Juan Vucetich, en 1891, realizó las primeras fichas dactilares del mundo con las huellas de 23 procesados, luego en 1905 su sistema dactiloscópico fue incorporado por la Policía Federal de Argentina. En 1941, Murrary Hill de los laboratorios Bell, inició el estudio de la identificación por voz y sus trabajos fueron tomados y redefinidos por L. G. Kersta. En 1986, sir Alec Jeffreys utilizó por primera vez el ADN para identificar al autor de asesinatos en Inglaterra [2] [3].

Sin embargo, el uso del reconocimiento biométrico como medio automático de autenticación personal en áreas diferentes a las mencionadas previamente, es un área de investigación y desarrollo reciente, motivado por el avance en las tecnologías de información y de comunicaciones (TIC's).

Las nuevas tecnologías de identificación por medio de sistemas biométricos, se perfilan como la futura llave que permitirá abrir todas las puertas. La principal manera de identificarse en el siglo XXI será el propio cuerpo, las características físicas, únicas y distintivas de las de cualquier ser humano.

Desde ya hace mucho tiempo, la mayoría de los países del mundo utilizan las huellas digitales como sistema práctico y seguro de identificación. Además, en las últimas décadas surgen nuevos instrumentos para la obtención y verificación de huellas digitales. También se comienzan a utilizar otros rasgos morfológicos como variantes de identificación, como por ejemplo el iris, el calor facial, el olor corporal, entre otros [4] [5].

Los sistemas biométricos, a partir de características físicas o conductuales, se encuentran clasificados en estáticos (basados en características fisiológicas) y dinámicos (basados en características conductuales). Dentro de los primeros se puede mencionar a: la huella dactilar [6], iris y retina, geometría y rayas de la mano [7], reconocimiento facial [8], entre otros; y dentro de los segundos incluyen la escritura manuscrita y reconocimiento de firma escrita, dinámica del teclado, reconocimiento de voz, entre otros [9].

II. Hipótesis o Justificación

Los organismos estatales cuentan con información de diversa índole, en volúmenes importantes y con distintos niveles de privacidad. Esta información, suele encontrarse clasificada en base a distintos criterios y alojada en diferentes dependencias, algunas de ellas con acceso restringido. Estos accesos generalmente se efectúan a través de los mecanismos tradicionales de control de acceso (claves, tarjetas magnéticas, etc.).

Si bien, en algunos casos ya se utilizan controles de acceso a través de sistemas y dispositivos biométricos provistos por empresas comerciales, estos dispositivos cuentan con código y base de datos propietarios que no pueden adaptarse a los requerimientos funcionales de las distintas áreas de estos organismos y que generalmente no soportan o tornan muy compleja la interoperabilidad e interconexión con otros sistemas.

El desarrollo e implementación de controles de acceso basados en sistemas biométricos en áreas críticas de organismos gubernamentales permitirá una mayor seguridad y control en el acceso a las mismas. Además, un desarrollo personalizado y ajustado a los estándares internacionales ya existentes de los distintos sistemas biométricos, permitirá adecuar los controles a los requerimientos específicos de cada área.

III. Objetivos

General:

El objetivo de este trabajo es analizar las dificultades en los procedimientos de autentificación de personas en organismos públicos e implementar posibles soluciones a través de la utilización de sistemas biométricos.

Específicos:

1. Delimitar el campo de la biometría digital, estudiar y clasificar los sistemas actuales de identificación basados en ella.
2. Relevar los métodos actuales utilizados por los sistemas de identificación, evaluar el rendimiento y establecer un análisis comparativo de dichos sistemas en base a diferentes parámetros.
3. Efectuar un estudio de campo en instituciones públicas que permita determinar las áreas claves que requieran procesos de identificación.
4. Establecer las necesidades de implementación de sistemas biométricos a partir de las dificultades de los procedimientos actuales en estas áreas.
5. Implementar soluciones basadas en los estándares de software y hardware asociados a la biometría informática que permitan una mayor interoperabilidad.

IV. Metodología

1. Delimitar el campo de la biometría digital

Para poder establecer el estado actual del conocimiento del tema en la identificación de personas a través de sistemas biométricos se llevó adelante un relevamiento bibliográfico que permitió conocer los antecedentes y trabajos relacionados, definir los conceptos y terminología básica y las ventajas que dichos sistemas introducen frente a los métodos tradicionales de autentificación. Se expuso el modelo general de funcionamiento de los sistemas biométricos, así como los parámetros existentes y a tener en cuenta para el reconocimiento y la clasificación de los sistemas.

2. Métodos actuales, rendimiento y comparación de los sistemas biométricos.

Se describieron y analizaron los sistemas biométricos de acuerdo a la siguiente clasificación: a) Estática: huella dactilar, iris y retina, geometría y rayas de la mano, reconocimiento facial y venas de muñecas y manos; y b) Dinámica: reconocimiento de la voz, escritura manuscrita y reconocimiento de firma escrita.

Se trabajó en la determinación y clasificación de los factores que afectan al rendimiento de los sistemas biométricos. Se presentó un estudio comparativo en función de las características de fiabilidad, facilidad de uso, prevención de ataques, aceptabilidad y permanencia que presentan los diferentes sistemas y que permitirá arribar a conclusiones respecto a los mismos.

3. Estudio de campo y diagnóstico en organismos estatales

Se realizó un estudio de campo en la Municipalidad de Concordia, con quien existe un acuerdo marco de colaboración y asistencia y un convenio específico para el presente proyecto. Este estudio permitió determinar las áreas claves que requieren o deberían requerir procesos de identificación. Se efectuó

un diagnóstico de las dificultades de los procedimientos usuales en estas áreas para establecer las necesidades de implementación de sistemas biométricos. En base a las necesidades detectadas en el diagnóstico, se propusieron para áreas estratégicas, soluciones en los procedimientos de autentificación basados en sistemas biométricos.

4. Implementación de soluciones basado en estándares

Se desarrolló específicamente la temática correspondiente a la biometría informática, considerando los estándares asociados a los sistemas biométricos, especialmente aquellos que refieren al intercambio de datos y conectividad entre dispositivos.

V. ACTIVIDADES REALIZADAS

V.I Delimitación del campo de la biometría digital

En el inicio de las actividades, se realizó un relevamiento bibliográfico que permitió definir los conceptos y la terminología básica, las ventajas que los sistemas biométricos introducen frente a los métodos tradicionales de autentificación. También se estudiaron los parámetros existentes y a tener en cuenta para el reconocimiento y la clasificación de los sistemas; así como los estándares asociados a estas tecnologías, especialmente aquellos que refieren al intercambio de datos y conectividad entre organismos y/o aplicaciones.

Conceptos básicos de biometría

El concepto de biometría o biométrica proviene de las palabras *bio* (vida) y *metría* (medida), por lo tanto con ello se infiere que todo sistema y dispositivo biométrico se encarga de medir e identificar alguna característica propia de los seres vivos [10] [11] [12] [13] [14] [15].

Los sistemas de reconocimiento que utilizan tecnologías biométricas reconocen a una persona en base a características físicas (huellas dactilares, rasgos de la mano o de la cara, patrones del iris) o características conductuales aprendidas o adquiridas (patrones de voz, patrones de firma ológrafa, patrones de tipeo). El uso de tecnologías biométricas para la identificación de personas se apoya en la utilización de dispositivos que contienen sus datos y de lectores de éstos.

Históricamente, siempre se comparó un rasgo con un dato, pero a medida que las aplicaciones fueron creciendo se hizo necesario contar con mecanismos no personales de reconocimiento. En Argentina, hasta no hace mucho tiempo, el Documento Nacional de Identidad era otorgado después de que un perito dactiloscópico cotejara la huella tomada al solicitante con la huella dactilar que obraba en la primera ficha. Este proceso llevaba su tiempo. Hoy, en el nuevo esquema de trabajo que puso en marcha el Ministerio del Interior, el cotejo está automatizado, acelerando el tiempo de entrega del nuevo DNI [16].

Verificación e identificación biométrica

A veces los términos biométricos como reconocimiento, verificación e identificación se usan de manera indistinta. Esto no solamente es confuso sino que incorrecto ya que cada término tiene un significado diferente.

- Reconocimiento es un término genérico y no necesariamente implica verificación o identificación. Todos los sistemas biométricos realizan un “reconocimiento” para “volver a conocer” a una persona que ya ha sido enrolada previamente [17].
- Verificación es una tarea donde el sistema biométrico intenta confirmar la identidad de alguien comparando una muestra presentada con otra u otras plantillas previamente enroladas.
- Identificación es una tarea donde el sistema biométrico intenta determinar la identidad de alguien. Se reúne una biometría y se la compara con todas las plantillas en una base de datos.

Los factores de verificación que se utilizan actualmente son tres y se basan en: 1) Algo que sé: la persona se autentica mediante algo que sabe: una clave, un número que la identifica - PIN, una frase o una respuesta a una pregunta de seguridad, etc.; 2) Algo que tengo: la persona se autentica utilizando algo que posee: un *token*, una *smartcard*, un certificado, etc. y 3) Algo que soy: el individuo se autentica en base a una característica que tiene su persona, esto es, un dato biométrico.

Los factores basados en conocimiento y en posesión requieren que la persona que se va a autenticar ante un sistema recuerde o lleve consigo el dispositivo. Además, estas cosas pueden extraviarse, olvidarse, ser sustraídas y/o duplicadas. En cambio, cuando se aplican tecnologías biométricas, el dato lo lleva consigo, y resulta casi imposible que se pierda, olvide o se falsee, de manera que sea utilizado por otra persona para suplantar su identidad [18]. Se dice que en los dos primeros factores, el vínculo entre el dato y su verificación es débil, lo cual facilita la usurpación de identidad, ya que el sistema no puede distinguir entre el legítimo poseedor del dispositivo y alguien que lo haya sustraído, lo mismo se aplica a la clave.

Rasgos biométricos

Existen ciertas características de los sistemas de reconocimiento biométrico que deben tenerse muy presentes a la hora de elaborar un proyecto en el sector público [19]. Un proyecto debe considerar al seleccionar el patrón biométrico, que el mismo debe responder mínimamente a las siguientes características:

- *Universalidad*: Debe estar presente en todo individuo.
- *Distinción*: Debe ser único para cada individuo y distinto en su comparación con otra persona. Una persona sólo puede registrarse si posee el rasgo biométrico necesario.
- *Permanencia*: Debe ser suficientemente invariable a lo largo del tiempo. Significa que la característica biométrica no cambie con el tiempo.
- *Registración*: La característica biométrica debe poder ser medida, cuantificada y registrada. Esto significa, que se puedan extraer las características distinguibles (metadatos) para utilizarse como método de identificación.

Además, es deseable que un sistema biométrico contemple las siguientes propiedades [9] [10] [20] [21] [22]:

- *Unicidad*: Significa que no deben existir dos individuos que posean la misma característica. El genotipo está vinculado genéticamente, esto significa que dos gemelos monocigóticos, idénticos, poseen la misma biometría. El fenotipo no está vinculado genéticamente, esto significa diferencias de los gemelos incluso aunque sean iguales. El establecer la unicidad es difícil de probar analíticamente. La unicidad debe ser distinguible, aunque sea única.
- *Fiabilidad*: Se la suele denominar también como rendimiento (performance) o nivel de exactitud. La fiabilidad de un sistema es la probabilidad de que ese sistema funcione o desarrolle una cierta función, bajo condiciones fijadas y durante un período de tiempo determinado. Esta característica, hace referencia a la precisión del reconocimiento, los recursos requeridos y el entorno operativo.
- *Facilidad de uso*: Tiempo en el que los nuevos usuarios desarrollan una interacción efectiva con el sistema o producto. Está relacionada con la predictibilidad, la sintetización, la familiaridad, la generalización de los conocimientos previos y la consistencia.
- *Resistencia a ataques*: Se la suele denominar también como resistencia del sistema biométrico a ser burlado. El término se refiere a la preparación y disposición que se hace anticipadamente para evitar un riesgo ante posibles intentos de violación al sistema.

- *Aceptabilidad*: Significa el grado de aceptación de las personas en base a su cultura, al hecho de que no perjudique a las personas y que además sea higiénica.
- *Costo aceptable*: Los componentes del costo en cualquier sistema biométrico incluyen hardware y software asociado para capturar la biometría, investigación y testeo del sistema biométrico, instalación, incluyendo los sueldos del equipo encargado de la implementación, montaje, conexión e integración del sistema de usuarios, capacitación de los mismos, alternativas para usuarios que no pueden registrarse, procesos de excepción a usuarios que no pasan la prueba biométrica, mantenimiento del sistema, administración de bases de datos centralizadas de imágenes/plantillas biométricas y poder de procesamiento del programa de respaldo.
- *No intrusiva*: Un sistema biométrico es no intrusivo si el individuo no necesita contacto físico con un sensor o no tiene una connotación negativa, es decir, los datos pueden ser adquiridos, incluso, sin que el sujeto se percate de ello.
- *Tamaño del lector*: Los dispositivos de captura de los datos biométricos poseen particularidades que dependen del sistema o de los sistemas biométricos que implementen y que condicionan su diseño.

Clasificación de los sistemas biométricos

Existen múltiples características que permiten distinguir a una persona de cualquier otra. Sin embargo, los trabajos de investigación en biometría se han orientado, a lo largo de los años, a aquéllas que permiten una mayor fiabilidad desde el punto de vista del reconocimiento.

El cuerpo humano presenta una organización estructural y funcional, fruto de largos años de evolución biológica, y el estudio de sus características se pueden abordar desde diferentes niveles de complejidad organizativa que abarcan desde su composición química y biofísica, a la conductual. De todas las características biológicas presentes en los seres humanos con capacidad de ser medidas y por lo tanto, susceptibles de ser utilizadas por la biometría se pueden considerar dos grandes grupos: estáticas o dinámicas (Figura 1) [10] [15] [23 [24] [25] [26].

Dentro del primero, se ubican las características que se centran en aspectos estructurales y que por lo tanto se encuentran vinculadas a determinados órganos y sistemas, como por ejemplo el caso de la cara y mano, el iris, la piel, las venas, las huellas dactilares y el olor químico corporal. Dentro del segundo grupo, están las que se encuentran en características de tipo funcional, tales como el habla y la voz, la escritura manuscrita y el reconocimiento de la firma escrita, la dinámica del tecleo y los gestos y movimientos corporales.

Si bien, en el trabajo se detallaron los sistemas biométricos estáticos que han alcanzado un grado de madurez importante, existen otros sistemas que se encuentran actualmente en distintas fases de desarrollo y evaluación, como lo son por ejemplo: el reconocimiento de la huella del pabellón auricular, el análisis de la huella de la oreja, el reconocimiento de uña, las crestas de las articulaciones de los nudillos, las arrugas del dedo y superficie tridimensional del dedo, entre otros [27] [28].

No existe una modalidad biométrica que mejor se adapte para todas las implementaciones. Se deben tener en cuenta muchos factores al momento de implementar un dispositivo biométrico que incluya la ubicación, riesgos de seguridad, tarea (de identificación o verificación), número posible de usuarios, circunstancias del usuario, datos existentes, entre otros. También es importante notar que las modalidades biométricas están en etapas de maduración fluctuantes [29] [30] [31]. La Figura 1 presenta la clasificación general de los sistemas biométricos citando los más representativos.

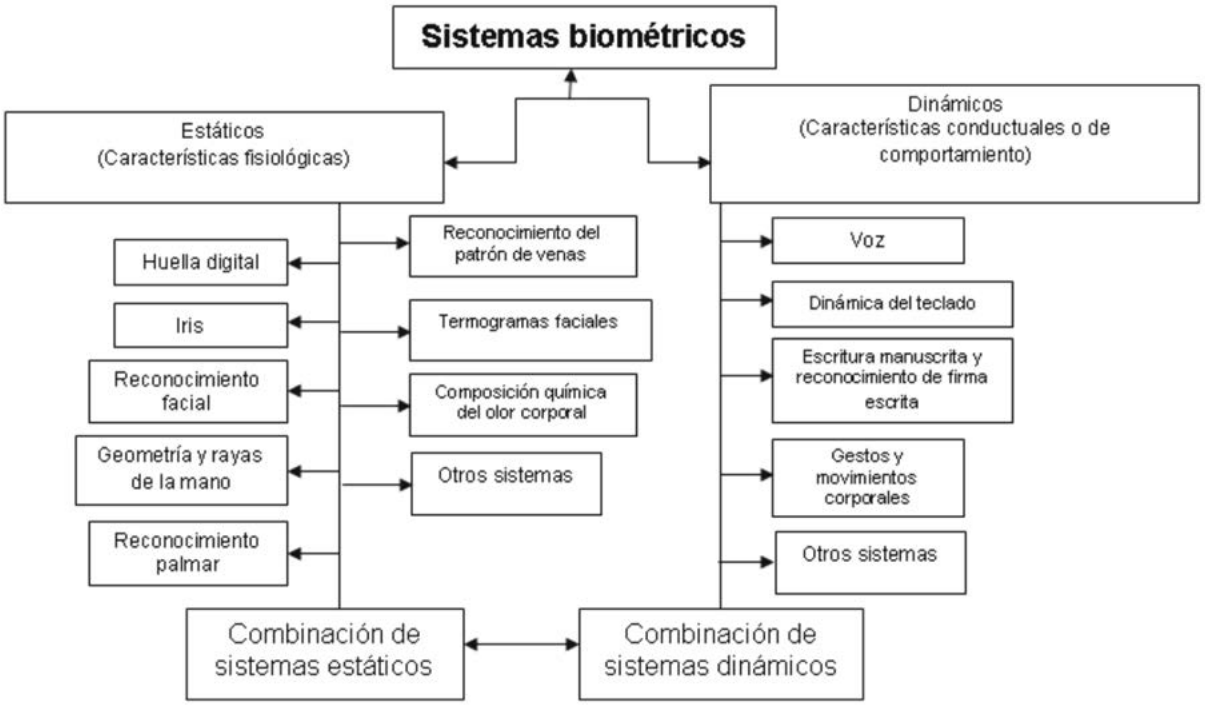

Figura 1: Clasificación de los Sistemas Biométricos.

Para mejorar las medidas biométricas y obtener una mayor fiabilidad, rendimiento y universalidad se puede pensar en utilizar sistemas muti-biométricos o sistemas biométricos multi-modales que combinan varias características de comportamiento y/o propiedades fisiológicas-biológicas de los individuos, realizando varios ciclos de análisis [9].

Los sistemas multi-biométricos pueden ser subdivididos en cuatro categorías distintas: a) multimodal: utiliza múltiples modalidades biométricas diferentes (ej. huella digital + huella palmar), b) multiinstancia: aplica múltiples instancias biométricas con una modalidad biométrica (ej. iris izquierdo + iris derecho), c) multisensorial: emplea múltiples sensores para medir la misma instancia biométrica (ej. para la huella digital: sensores ópticos, electrostáticos y sensores infrarrojos) y d) multialgorítmico: aprovecha múltiples algoritmos para procesar el mismo ejemplo biométrico. El objetivo de estos sistemas es mejorar uno o más de los parámetros biométricos [32], de los cuales se habla más adelante en este texto.

Estándares en biometría

Un aspecto relevante para las aplicaciones biométricas es la fijación de estándares tecnológicos universalmente aceptados, a fin de permitir el uso de esta tecnología en distintos lugares. Los estándares reducen las diferencias entre los productos y generan un ambiente de estabilidad, madurez y calidad. Esto asegura además, la disponibilidad de múltiples fuentes de productos comparables y con precios competitivos en el mercado.

Las aplicaciones deben ajustarse a estos estándares para facilitar el proceso de reconocimiento de las personas. Los estándares tecnológicos biométricos se refieren a distintos aspectos involucrados, tales como los dispositivos de almacenamiento, las bases de datos, los patrones biométricos a utilizar, los datos que se levantan y almacenan, los dispositivos de lectura, entre otros.

Los primeros estándares surgieron a mediados de los años 80 para el intercambio de información forense sobre huellas dactilares. Actualmente, están elaborando dichas normas varios organismos nacionales e internacionales entre los que puede citarse la Organización Internacional de Normalización

(ISO) [33], la Comisión Electrotécnica Internacional (IEC: *International Electrotechnical Commission*) [34] y el Sector de Normalización de las Telecomunicaciones (UIT-T) de la UIT (Unión Internacional de Telecomunicaciones). Los consorcios industriales también crean normas que soportan los objetivos de sus miembros, mientras que los organismos especializados de las Naciones Unidas, tales como la Organización de la Aviación Civil Internacional (OACI) y la Organización Internacional del Trabajo (OIT), redactan normas en el marco de sus dominios específicos que posiblemente no hayan sido abordados por otras organizaciones.

A finales de los años '90 se empieza a ver la necesidad de crear interfaces comunes, así como formatos de datos conocidos [35]. De ahí surgen iniciativas de carácter privado y sectorial, que impulsan determinadas tentativas de estándares de facto. Sin embargo, a consecuencia de los eventos del 11 de septiembre de 2001, se empuja esa necesidad, y sobre todo, el hecho de que los acuerdos sean de índole mundial. Esto motiva que en agosto de 2002, se cree un Subcomité dedicado a la Identificación Biométrica, dentro del Comité Conjunto ISO/IEC sobre Tecnologías de la Información (JTC1).

El hecho de que hayan aparecido un número importante de estándares referidos al uso de tecnología biométrica, denota el creciente interés de autoridades públicas y del sector privado por este ámbito tecnológico.

Los sistemas biométricos pueden necesitar confiar en otros estándares que fueron desarrollados para un amplio espectro de aplicaciones, tales como el *Federal Information Processing Standard* 180*, Secure Hash Standard* [36]. Existe publicada una lista de los estándares biométricos y sus áreas de aplicación para el Gobierno de Estados Unidos. El "*Registry of USG Recommended Biometric Standards*" [37] tiene las siguientes categorías: colección de datos biométricos, almacenamiento y registros de intercambio; perfiles de transmisión de datos biométricos; perfiles biométricos de credenciales de identidad; normas técnicas de interfaz; métodos de prueba para la prueba de conformidad con los estándares biométricos; y estándares para la metodología de prueba de rendimiento de sistemas biométricos.

Por otra parte, los estándares biométricos pueden dividirse en cuatro grupos: interfaces técnicas, formato de intercambio de datos biométricos, perfiles de aplicación y pruebas de rendimiento. Las principales normas que se utilizan son las siguientes:

- ANSI/NIST-ITL *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information* [38].
- Perfiles de Aplicación desarrollados para usos específicos tales como: FBI/agencias de policía de EE.UU, EE.UU. *Department of Defense, Royal Canadian Mounted Police, Terrorist Watchlist Person Data Exchange, US-VISIT, INTERPOL, United Kingdom National Policing Improvement Agency, Bundeskriminamt* (Alemania), *Visa Information System, Western Identification Network*, entre otros [39].
- ISO/IEC 19794-x (normas) e ISO 29794-x (conformidad).
- CBEFF – *Common Biometric Exchange File Format* [40].
- INCITS 381 (imágenes de huellas dactilares), INCITS 378 (plantillas de huellas dactilares), INCITS 385 (imágenes faciales) [41].

De manera específica, en este relevamiento se puso énfasis en los estándares para los rasgos de iris y voz, cuyos procesos específicos para el reconocimiento se describen más adelante.

Los estándares que rigen actualmente el área de reconocimiento del iris existen por una parte, en Estados Unidos a través del ANSI/INCITS (*American National Standards Insititute/InterNational Committee for Information Technology*) [42] y por otra, a escala internacional por medio de ISO/IEC (*International Organization for Standardization/International Electrotechnical Commission*) [43]. Por la parte americana, el estándar permite un formato de intercambio de datos del iris (ANSI/INCITS 379-2004). Referente al estándar internacional, éste admite la permuta de datos biométricos (ISO/IEC 19794-6:

2005) siendo la parte 6, el intercambio de datos de la imagen del iris. Ambos estándares indican a los fabricantes de esta tecnología biométrica cómo dar formato a los datos de sus sistemas o cómo interpretar los datos que entran a sus sistemas. También definen, en el caso del iris, dos formatos de datos para representar una imagen del mismo.

En noviembre de 2011, el Instituto Americano Nacional de Estándares (NIST) publicó la norma ANSI/NIST (Instituto Nacional de Estándares y Tecnología)-ITL 1-2011 [38], titulada Formato de datos para el intercambio de huellas dactilares, faciales, y otra información biométrica, que define el contenido, formato y unidades de medida para el intercambio de información que puede ser utilizada en la identificación biométrica de una persona. Este estándar, comprendido entre los estándares de formato de intercambio de datos biométricos, especifica un conjunto común de elementos de información necesarios para soportar múltiples tecnologías biométricas y fomentar la interoperabilidad de aplicaciones basadas en programas de sistemas biométricos al permitir el intercambio de los datos. Las normas ANSI/NIST-ITL se usan ampliamente y admiten diversos tipos de datos biométricos y demográficos.

A partir del año 2005, desde el gobierno nacional argentino se impulsó la adopción de estándares internacionales en materia de biometría que permitieran compartir la información entre los organismos de competencia en la materia, así como entre los gobiernos provinciales y la Nación. De acuerdo con Pedro Janice, el Director de la Oficina Nacional de Tecnologías de la Información (ONTI) de la Jefatura de Gabinete de Ministros, la adopción de los estándares del tipo ANSI-NIST en materia de comunicaciones de datos biométricos para la identificación fue un paso estudiado y asimilado viendo los beneficios que este tipo de comunicación brindaba en la interoperabilidad de los sistemas [40].

Sin embargo, el estado actual de la tecnología permite solamente interoperabilidad a través de la transmisión de la imagen del iris completo; por lo que requiere un almacenaje con exceso de datos y un ancho de banda importante, introduciendo fuentes de errores adicionales a través de procesos de transmisión de datos muy grandes. Las organizaciones nacionales e internacionales de estándares están trabajando para continuar la progresión de los estándares en una dirección, para facilitar el crecimiento y la interoperabilidad.

En cuanto a la interoperabilidad informacional, es decir, a la comprensión de la información intercambiada, se sabe que la eficiencia en la recuperación de la información de carácter público está condicionada por aspectos relacionados con la estructuración de la información (lenguajes de marcado) y con la representación del conocimiento (metadatos). En este sentido *eXtensible Markup Language* (XML) supone un verdadero avance, dado que sus prestaciones potenciales son capaces de posibilitar una interoperabilidad sintáctica y semántica real. La norma ANSI/NIST-ITL 2011 contempla el formato XML para reflejar las nuevas necesidades en materia de intercambio de datos y define unos 20 tipos de registro para su uso en el intercambio de información biométrica (como ser, rostros, dedos, palmas de las manos, huellas latentes, iris) y datos relacionados (por ejemplo, la fecha y la hora de la captura). Las reglas de codificación XML propuestas en el estándar NIST-ITL se ajustan al Modelo Nacional de Intercambio de Información (NIEM) [44], que facilita la interoperabilidad para el intercambio de información entre múltiples agencias gubernamentales.

Con respecto a biometría de voz, esta modalidad biométrica presenta algunos desafíos únicos que no se encuentran en otras formas de reconocimiento humano, tales como las huellas dactilares, el iris o el rostro. La voz humana, generalmente contiene a la vez habla y los sonidos no vocales, se propaga a distancias variables a través del aire u otro medio para llegar a transductores acústicos (por lo general micrófonos) de fase y amplitud variable.

El ANSI/NIST-ITL se encuentra trabajando en la elaboración de un suplemento del estándar ANSI/NIST-ITL 1-2011, para hacer frente a un vacío en dicha norma a fin de facilitar el intercambio de datos de voz con fines de investigación y forenses [45]. Las grabaciones de voz a las que refiere el registro tipo 11 de la norma deben ir acompañadas de la documentación, cuando esté disponible, para soportar

una amplia gama de potenciales transacciones. Esta documentación ("metadatos") puede ser dividida en cuatro tipos básicos: 1) Metadatos administrativos; 2) Metadatos del hablante; 3) Metadatos de contenido y 4) Metadatos de la tecnología de audio.

Por consiguiente, el objetivo en la creación de este tipo de registro es crear tantos campos de metadatos no redundantes como sea posible para permitir la transmisión de la documentación de interés potencial en el futuro, incluso si los metadatos podrían ser recuperados de la grabación de audio en sí. La mayoría de estos campos contenidos en los registros tipo 11 son opcionales, porque gran parte de los metadatos potencialmente relevantes pueden ser desconocidos por los diversos organismos que participan en la transacción.

V.II Métodos actuales, rendimiento y comparación de los sistemas biométricos

En este apartado se expondrá el modelo general de funcionamiento de los sistemas biométricos, así como los parámetros existentes a tener en cuenta para el reconocimiento y que permiten medir la efectividad de los mencionados sistemas.

Parámetros biométricos

Los parámetros biométricos se componen de índices que permiten medir la efectividad de un sistema biométrico de identificación y verificación (*detection and identification rate*). Las tasas de error para verificación permiten valorar cuantitativamente la velocidad, precisión u otras características de un sistema o algoritmo biométrico. Algunas de las curvas que generan estas tasas son mostradas en la Figura 2.

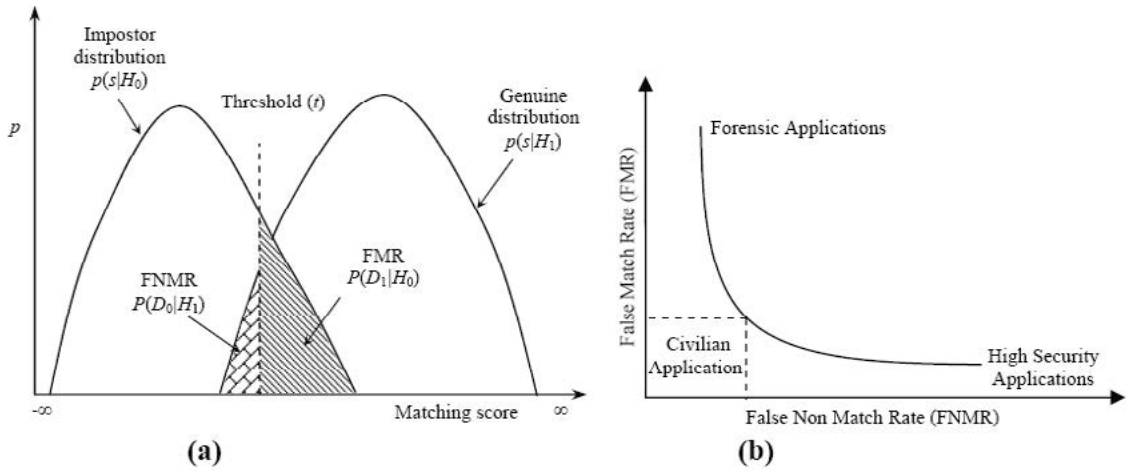

Figura 2: Tasas de error de un sistema biométrico [14].

Los principales parámetros biométricos se detallan a continuación:

FAR (False Accept Rate). Es la probabilidad de que un sistema biométrico identifique incorrectamente un individuo o falle a la hora de rechazar a un impostor. Para un sistema de verificación positiva, la FAR puede obtenerse del cociente entre el número de aceptaciones falsas (impostores) dividido entre el número total de intentos o test de verificación del impostor. Una tasa de FAR buena es entre 0,1-2,0% y una tasa mala es una que sea mayor al 15%.

FMR (*False Match Rate*). Es la tasa de comparaciones incorrectas positivas que realiza un algoritmo de comparación para un único intento de comparación con la plantilla. Para sistemas biométricos que utilizan sólo un intento para decidir la aceptación, la FMR es la misma que la FAR. Cuando se combinan

varios intentos para decidir la aceptación la FAR es más relevante a nivel del sistema que la FMR.

FNMR (False Non-Match Rate). Es la tasa de comparaciones incorrectas negativas por medio de un algoritmo de comparación para un único intento de comparación con la plantilla. Para sistemas biométricos que sólo utilizan un único intento para decidir la aceptación, la FNMR es la misma que la FRR. Cuando se combinan varios intentos para decidir la aceptación, la FRR es más relevante a nivel del sistema que la FNMR. Se obtiene dividiendo el número de comparaciones reales con puntuación más baja por el número total de comparaciones reales.

FRR (False Reject Rate). Es la probabilidad de que un sistema biométrico falle a la hora de identificar a un individuo sobre el cual se efectúa el alta. Para un sistema de verificación positiva, el FRR puede estimarse utilizando el cociente entre el número de rechazos falsos (de personas auténticas) dividido entre el número total de intentos o test de verificación de la persona que se inscribe. Una tasa de FRR buena es 0% y una tasa mala es una que sea mayor al 50%.

FTA (Failure to Acquire Rate). Es la proporción de intentos para los que un sistema biométrico sea incapaz de capturar una muestra de suficiente calidad. Las razones pueden ser la incapacidad para capturar, la calidad insuficiente de la muestra (por ejemplo, datos de la muestra demasiado ruidosos), o el número insuficiente de las características (por ejemplo, muy pocas minucias). Se puede ajustar mediante el aumento o disminución de los umbrales de calidad. Cuando un sistema biométrico permite varios intentos, la FTA mide el fallo de captura sobre esos múltiples intentos.

FTE (Failure to Enroll Rate). Es la proporción de la población de usuarios para los que el sistema biométrico es incapaz de generar plantillas de referencia de calidad suficiente. Es equivalente a la FTA para el proceso de inscripción de datos biométricos de un individuo y depende de los procedimientos utilizados en la inscripción (que puede diferir de los procedimientos utilizados posteriormente para la identificación). Incluye a aquellos que por razones físicas o de comportamiento son incapaces de presentar la característica biométrica requerida (por ejemplo alguien que se haya quemado las manos o una persona drogada que afecta a su comportamiento). La FTE es la probabilidad de que un usuario dado sea imposible inscribirse en un sistema biométrico debido a la insuficiente distinción de muestras biométricas. Los usuarios incapaces de proporcionar datos biométricos como amputados no son contabilizados normalmente en la tasa FTE del sistema. Una tasa buena de FTE es 0,2% y una tasa mala es una que sea mayor al 15%.

ATV (Ability to Verify). Es uno de los parámetros más importantes a la hora de realizar una prueba de rendimiento de un sistema biométrico. Nos permite determinar la proporción de usuarios para los que el sistema funciona correctamente. La fórmula de cálculo de ATV es:

ATV = (1 − FTE) * (1 − FRR)

Junto con las FAR, el ATV muestra información importante sobre tres temas clave para los sistemas de autenticación biométrica: costo, seguridad y conveniencia.

Costo: Si algunos usuarios no pueden ser autenticados por el sistema biométrico, un proceso de autenticación alternativo será necesario. Podría ser una alternativa basada en una contraseña de autenticación, en cualquier caso, se incrementan los costos.

Seguridad: Si el ATV es bajo, muchos usuarios no están siendo verificados por el sistema de autenticación biométrico. A menos que los mecanismos alternativos de autenticación sean tan seguros como el sistema biométrico, la seguridad del sistema resulta degradada.

Conveniencia: Un ATV bajo indica que el sistema biométrico es difícil de usar, ya que muchos usuarios no pueden registrar o autenticar con éxito. Si bien el ATV se podría incrementar mediante la reducción de las normas para el registro y el umbral para la autenticación de los usuarios, esto daría lugar a una alta FAR. Del mismo modo, la FAR se podría reducir incrementando el registro y el umbral para la

autenticación, pero el ATV sería bajo. Por esta razón, ambos indicadores deben ser considerados en conjunto, y no sólo uno o el otro.

UMBRAL (Threshold). El umbral de decisión es un valor por el cual el sistema biométrico al realizar una comparación de los datos biométricos extraídos al individuo con las plantillas almacenadas en la base de datos biométrica, ayuda a determinar el nivel de similitud de esta comparación. Es decir, es un tipo de referencia que determina la consistencia de un patrón. Este valor puede ser ajustado dependiendo del nivel de seguridad requerido para el sistema biométrico.

TAR (True Accept Rate). Esta medida representa el grado en que el sistema biométrico es capaz de emparejar correctamente la información biométrica de la misma persona. Lo que se busca al desarrollar un sistema biométrico es maximizar esta medida. Para cada valor umbral, el TAR es el porcentaje de positivos verdaderos (porcentaje de genuinos) que se encuentran por encima del umbral. Para cada valor umbral, la FAR es el porcentaje de falsos positivos (porcentaje de impostores) que se encuentran por encima del umbral.

EER (Equal Error Rate). Con un valor de umbral lo suficientemente bajo, pocos usuarios o ninguno serán rechazados, por lo que la FRR será baja. La mayoría o todos los impostores serán aceptados, por lo que la FAR será alta. Luego, cuando el umbral se incrementa más usuarios genuinos serán rechazada y menos impostores serán aceptados. En algún punto los valores de FRR y FAR serán iguales. En ese puno surge la tasa de error igual (EER), que puede ser útil como un valor único para permitir la comparación entre diferentes sistemas de autenticación biométrica.

Entonces, la tasa EER es el punto en que las curvas de la FRR (o FNMR) y de la FAR (o FMR) son idénticas. Las curvas de FRR y FAR se dibujan sobre un eje de abscisas que es el umbral de tolerancia. Las curvas FAR y FRR no son independientes, se encuentran inversamente relacionadas, cuando una crece la otra decrece. Se expresa en tanto por ciento. Un punto de trabajo con 1% de FNMR y 0,00000025% de FMR es equivalente a un EER de 0,0005%. La EER no representa un punto de operación óptimo de un sistema biométrico, se utiliza para la comparación del rendimiento de autenticación de los sistemas biométricos. Cuanto más bajo es el EER o el CER, se considera que el sistema es más exacto.

LRGI (Likelihood Ratio of Genuine to Impostor). Otro de los parámetros biométricos utilizados es BGI (Ganancia biométrica contra impostores), que representa la relación entre la salida y la entrada, para cada modalidad biométrica o algoritmo utilizado. Este parámetro se calcula como:

$$BGI = \frac{\text{Probabilidad de ser un impostor dadas las evidencias biométricas}}{\text{Probabilidad de ser un impostor, sólo con el conocimiento previo}}$$

Sin embargo, la mayoría de las veces, una muy buena aproximación a la BGI es el recíproco de la relación de posibilidades reales para Impostor (LRGI). Esta métrica es usada en gran cantidad de algoritmos de reconocimiento de patrones biométricos existentes en los dispositivos biométricos. Este se calcula como el cociente de dividir la probabilidad de ver la evidencia de un impostor dividido entre la probabilidad de verlo a partir del sujeto genuino esperado.

$$LRGI = \frac{\text{Probability of seeing the evidence from an impostor}}{\text{Probability of seeing it from the expected genuine subject}}$$

ROC (Receiver Operating Characteristic). Es la curva formada por los puntos de coordenadas (FAR, TAR o FRR) sobre unos ejes de coordenadas cartesianas cuyo eje de las abscisas corresponde a la

tasa de error FAR y el eje de ordenadas el de TAR (o FRR). Sirve para mostrar el rendimiento de precisión medida de un sistema biométrico.

Tasa de fallas de captura (FTC). La probabilidad de que el sistema no puede detectar una entrada biométrica cuando se presenta correctamente.

Capacidad de la plantilla. Corresponde al número máximo de conjuntos de datos que puede almacenarse en el sistema.

Las tasas de errores son medidas de dos maneras: a) por la cantidad de personas con permiso que son rechazadas (tasa de falso rechazo) y b) por la cantidad de personas sin permiso que son aceptadas (tasa de aceptación indebida). La mayor preocupación se centra con el segundo tipo, pero en implementaciones prácticas el primer problema genera muchos inconvenientes.

La FAR debe ser suficientemente baja en un rango que suele establecerse entre el 0.0001% y el 0.1%. Hay que tener en cuenta que la tasa real de entradas no autorizadas resulta del producto de la FAR por la probabilidad de que un sujeto no autorizado alcance el dispositivo de control e intente el acceso. Si el sistema se complementa con un elemento físico (como una tarjeta magnética o un código numérico), el intruso debe, poseer la tarjeta correspondiente, una copia de la misma o bien conocer el código de acceso [15].

La FRR debe también mantenerse baja para evitar el descontento de los usuarios y la ineficiencia del sistema. Por ejemplo, en un recurso con 1000 accesos diarios, una FRR del 1% se producirá 10 incidencias diarias.

La validación de las tasas proporcionadas por los fabricantes no es fácil a causa de los porcentajes tan bajos que se manejan, exigiendo el examen supervisado de miles de accesos para obtener resultados significativos estadísticamente.

Rendimiento y comparación de los sistemas biométricos

Todos los sistemas biométricos y las tecnologías que los mismos emplean, poseen al momento de su aplicación, beneficios y desventajas. Comparar sistemas de manera descontextualizada, ya sea sobre el funcionamiento, usabilidad o cualquier otro criterio, es erróneo, ya que no refleja correctamente, que la identificación biométrica es sólo parte de un sistema mayor. Además, no existe mucha información disponible que sea confiable, comparable y reciente. Sin embargo, al tener una visión de las potencialidades o limitaciones probables de cada sistema, se puede arribar a una conclusión sobre qué aplicaciones son factibles, o qué clase de combinaciones multi-biométricas funcionarán mejor en una situación en particular.

El funcionamiento de los distintos sistemas biométricos desarrollados se ve influenciado por diversos factores que pueden afectar su rendimiento. En cuanto a los factores que afectan directa o indirectamente a los sistemas biométricos, se pueden establecer dos grandes grupos:

a) Aquellos inherentes al propio dispositivo o tecnología empleada, denominados también ambientales. Se incluyen en este grupo la luz, ruidos, temperatura, ruido electromagnético, humedad, suciedad y contaminantes, variaciones de voltaje, golpes y vibraciones (Tabla 1).

b) los correspondientes a los factores ajenos a los dispositivos, que de una u otra manera afectan a todos los sistemas, denominados requisitos, características o criterios de evaluación: En este grupo se destacan las siguientes características: universalidad, fiabilidad, facilidad de uso, prevención de ataques, aceptabilidad, permanencia, costo, unicidad, capacidad de almacenamiento y tamaño del lector.

Al momento de seleccionar un sistema biométrico y su correspondiente tecnología, se deben tener en cuenta requisitos que debe contener la aplicación de dicho sistema y los efectos que genera sobre

la población donde se implemente. Si bien estos requisitos, características o criterios de evaluación, pueden modificarse sutilmente de un sistema a otro, se puede mencionar como aplicables a todos los sistemas los siguientes: costo, grado de precisión, causas de error, grado de estabilidad, conveniencia, velocidad, conectividad y compatibilidad, nivel de seguridad, detección de vida, tamaño del lector, requisitos y capacidad de almacenamiento, secretismo de la aplicación, facilidad de uso, aceptación de usuarios, adecuación de usuarios y formación de los mismos.

Tabla 1: Factores ambientales relacionados con algunos de los sistemas biométricos.

Sistema biométrico / **Factor ambiental**	**Huellas dactilares**	**Iris**	**Reconocimiento facial**	**Reconocimiento palmar**	**Reconocimiento de la voz**
Luz	X	X	X	X	
Ruido					X
Temperatura	X			X	
Ruido electromagnético	X	X	X	X	X
Humedad	X			X	
Suciedad y contaminantes	X	X	X	X	
Variaciones de voltaje	X	X	X	X	X
Golpes y vibraciones	X	X	X	X	X

Los sistemas biométricos reúnen diferentes características o criterios que pueden ser medidos de diferentes maneras a los efectos de poder establecer estudios comparativos entre los distintos sistemas biométricos. A partir de las características más relevantes de los sistemas biométricos, se establece una comparación entre los sistemas biométricos más desarrollados (Tabla 2).

Tabla 2: Evaluación comparativa de algunos sistemas biométricos [13] [23] [32] [36].

Sistema biométrico / **Característica**	**iris**	**Huella dactilar**	**Geometría de la mano**	**Escritura y firma**	**Voz**	**Rostro**
Universalidad	*Alta*	*Alta*	*Alta*	*Alta*	*Media*	*Media*
Fiabilidad	*Muy alta*	*Alta*	*Alta*	*Media*	*Alta*	*Alta*
Facilidad de uso	*Media*	*Alta*	*Alta*	*Alta*	*Alta*	*Alta*
Prevención de ataques	*Muy alta*	*Alta*	*Alta*	*Media*	*Media*	*Media*
Aceptabilidad	*Media*	*Media*	*Alta*	*Muy alta*	*Alta*	*Muy alta*
Permanencia	*Alta*	*Alta*	*Media*	*Baja*	*Media*	*Media*
Costo	*Muy alto*	*Medio*	*Alto*	*Bajo*	*Bajo*	*Medio*
Tamaño del lector	*Muy grande*	*Medio*	*Grande*	*Pequeño*	*Pequeño*	*Grande*

Estas mediciones son realizadas a través de diferentes pruebas y del análisis de los parámetros biométricos descriptos anteriormente.

Existen también problemas prácticos asociados con la biometría. Algunas de estas tecnologías aún no están en el mercado. Adicionalmente, no en todos los mercados estas tecnologías son igualmente efectivas, y es frecuentemente difícil determinar cuál es la que más se ajusta a una aplicación determinada. De la misma forma, la comparación objetiva entre diferentes tecnologías es difícil de conseguir. Esto es porque aún no hay conclusión sobre cuestiones como la capacidad de las mismas para resistir daños debidos al medio ambiente por tiempos prolongados, tales como la suciedad o el vandalismo [46].

V.III Estudio de campo y diagnóstico en organismos estatales

En este apartado, se presenta un estudio de campo en instituciones públicas, en particular el realizado en la Municipalidad de Concordia (con quien se firmó un acuerdo específico de colaboración para con el proyecto), para determinar las áreas claves que requieren o deberían requerir procesos de identificación. Se plantea un diagnóstico de las dificultades de los procedimientos actuales en estas áreas para establecer las necesidades de implementación de sistemas biométricos.

Para un conocimiento más acabado, del tipo y tamaño de la organización, es conveniente explicitar algunas características organizacionales del Municipio de la ciudad de Concordia, provincia de Entre Ríos. Muchas de las diversas actividades que competen al ámbito del municipio, se desarrollan en lugares físicos dispersos y separados geográficamente. Cabe mencionar que existen dependencias cuyo lugar de tarea está separado del edificio del Palacio Municipal y distribuidas por la ciudad de Concordia.

Del análisis realizado tomando como base el relevamiento realizado y las entrevistas con responsables, surgen como áreas prioritarias dentro de un programa de administración de seguridad a dos áreas dependientes de la Secretaría de Economía y Hacienda: Tesorería y Dirección de Informática. La primera, se seleccionó, debido a que administra recursos de vital importancia y presenta un entorno funcional que no asegura las medidas suficientes para conformar un sistema de acceso adecuado. La segunda se encarga de administrar información sensible para el municipio, y se encuentra en una zona de mayor afluencia de personas.

Estas oficinas dependen de la Secretaría de Economía y Hacienda que es la encargada de generar, recaudar y administrar los recursos que el municipio necesita para la prestación de los servicios públicos, de salud y desarrollo humano y para las inversiones de infraestructura necesarias en todo el territorio. El desarrollo informático como lo es la página web, software específico y a medida, adecuaciones a los sistemas informáticos, son realizadas exclusivamente con agentes municipales.

A los efectos de relevar datos significativos sobre la visión del personal vinculados con los temas de seguridad, y los riesgos a los que se encuentran expuestos en situaciones que pudieran comprometer el normal funcionamiento de sus tareas se confeccionó un formulario de entrevista, con 14 ítems que incluyeron temáticas tales como gestión de la información, protección de los datos, normas de seguridad, y cuestiones relacionadas con los sistemas y dispositivos existentes para la identificación de las personas con acceso a dichos sectores. Fueron entrevistadas doce (12) personas del área informática (90% de la planta total) y seis (6) personas del sector tesorería (75% del total).

Además, se realizó un estudio del ambiente físico de las instalaciones del Data Center teniendo en cuenta especialmente las normas de seguridad en las Tecnologías de la Información (ISO 27.002). En el momento de este estudio, la situación del Data Center presentaba diversas falencias relacionadas con los aspectos vinculados con la seguridad en general, incluyendo el control de acceso de personas en particular.

En base a las observaciones realizadas en las instalaciones, el relevamiento efectuado a través de entrevistas a informantes claves y a entrevistas al personal de Tesorería y Dirección de Informática res-

pecto a la identificación de personas que acceden a sus oficinas, se detectó la siguiente problemática:

- Carencia en los niveles de protección de los equipamientos informáticos afectados a la Dirección de Informática del Municipio. El equipamiento actualmente no cuenta con un ambiente físico adecuado como tampoco con mecanismos de acceso seguros.
- Desconocimiento y falta de normas referidas al acceso e identificación de personas a dependencias claves en la administración pública local por parte de sus agentes.
- Falta de inversión en tecnología de control de acceso biométrico para la identificación de las personas que accedan a los sectores antes mencionados.

Por otra parte, también utilizando como campo la Municipalidad de Concordia, en este trabajo se realizó un estudio comparativo de los sistemas biométricos. En esta actividad se analizaron diferentes factores de los sistemas biométricos, y se concluyó, que los rasgos candidatos para la evaluación son: huella dactilar, iris, rostro y geometría de la mano. También, se destacó la importancia de fusión de diferentes rasgos en dispositivos multi-biométricos.

Otra cuestión importante que se tuvo en cuenta para la elección de los dispositivos, es que los mismos cuenten con proveedores y servicio técnico dentro de la provincia.

En base a las características requeridas y al presupuesto del proyecto, se planteó la adquisición de un dispositivo de geometría de la palma de la mano y un dispositivo multi-biométrico (de rostro y huella dactilar). Los dispositivos de iris no se pudieron adquirir porque el valor de mercado se incrementó en los últimos años de manera significativa. Por lo que se tomó la decisión de implementar un sistema de reconocimiento propio. Si bien se culminó el software, no se pudo terminar el prototipo debido a la falta de ofertas del dispositivo de captura por parte de los proveedores.

Por lo antes expuesto, el estudio comparativo se realizó tomando como base el dispositivo mono-biométrico (geometría de la palma de la mano: utilizando el dispositivo HANDPUNCH 1000) contra un dispositivo multi-biométrico (de rostro y huella dactilar: para el cual se empleó el dispositivo ZKSOFTWARE IFACE 202).

Este equipamiento fue instalado en las dependencias de Tesorería y la Dirección de Informática de la Municipalidad de Concordia, áreas éstas que por su función ya fueron previamente definidas como estratégicas en el proyecto en lo que a identificación de personas se refiere. Ambos dispositivos fueron sometidos a pruebas de acceso durante un mes por el personal involucrado en dichas oficinas y, en base a las características analizadas, se pudieron establecer los siguientes resultados comparativos:

Tabla 3: Comparación de características entre dispositivos.

Sistema Biométrico / Característica	**Geometría de la mano (mono-biométrico)**	**Huellas y rostro (multi-biométrico)**
Fiabilidad	Alta	Muy alta
Resistencia a ataques	Alta	Muy alta
Aceptabilidad	Alta	Muy alta
Costo	Alto	Medio

Por lo expuesto, en el caso estudiado, con los dispositivos involucrados y con las pruebas realizadas, se concluye que el sistema multi-biométrico presenta actualmente mayores beneficios para su implementación. La razón de esto, radica en que al incorporar dos sistemas de identificación en un mismo dispositivo, los parámetros de medición mejoran notablemente el rendimiento y la exactitud de la comparación.

Cabe destacar además y de acuerdo a los relevamientos efectuados durante el desarrollo del proyecto, los dispositivos de geometría de la mano en un futuro podrían perder en la industria, el mercado que actualmente poseen. Las razones, radican fundamentalmente en que los mismos tienen un costo alto, una permanencia media del rasgo de lectura y que los factores ambientales lo afectan en forma negativa respecto a otros dispositivos.

V.IV Implementación de soluciones basado en estándares

En base al diagnóstico realizado, se realizaron las siguientes recomendaciones: a) Realizar una planificación a mediano y largo plazo, que implemente medidas correctivas de las situaciones planteadas; b) Adecuar el ambiente físico y el hardware, como ser, la instalación de equipos y adopción de medidas de seguridad ambientales (control de incendios, control de temperatura, etc.) y el análisis de diferentes tecnologías de control de acceso a utilizar; y c) En el caso específico del Data Center, disponer de una sala específica para ese fin, con acceso biométrico. Dado el estudio comparativo y de campo realizado se recomienda el sistema multi-biométrico de huella y rostro.

Se debe destacar, que parte de estas recomendaciones se empezaron a ejecutar en la Municipalidad, particularmente en el Data Center.

También se propuso el desarrollo de sistemas biométricos propios, a fin de implementar un sistema confiable de control de acceso de personas a las oficinas, que permita la identificación y el registro de los accesos basado en reconocimiento de iris.

El Sistema de Reconocimiento de Iris (SRI) contempla dos grandes etapas: la Generación de plantillas o imagen del iris codificada (IrisCode) y los procesos de Comparación y Decisión. En el diagrama presentado en la Figura 3, se resumen los pasos involucrados en la obtención de las características del iris y su correspondiente codificación. En el proceso de comparación y decisión se utilizó la Distancia de Hamming como medida de validación de códigos.

Si bien se culminó el software, no se pudo terminar el prototipo debido a la falta de ofertas del dispositivo de captura por parte de los proveedores, por lo que no pudo ser testeado en el estudio de campo. Cabe destacar que, tal como fue previsto en los objetivos del proyecto, se trabajó en una arquitectura basada en estándares orientados a la interoperabilidad entre aplicaciones. Particularmente, se trabajó con el formato de datos para el intercambio de imágenes de iris adecuado a la norma ANSI/NIST ITL-2011, como se detalla en el siguiente apartado.

Desarrollo basado en estándares

Con el propósito de favorecer la interoperabilidad entre organismos y/o aplicaciones, el desarrollo del módulo de generación de registros ANSI/NIST-ITL 1-2011 fue encarado como un servicio Web, es decir, como una aplicación accedida remotamente usando protocolos de Internet, y XML como mecanismo de mensajes. En la Figura 4, se muestra el esquema general de cómo se relacionan los módulos de procesamiento de imágenes y reconocimiento de iris, con los módulos para el procesamiento de registros de transacciones. Mediante el uso de esta arquitectura, aplicaciones clientes desarrolladas en diferentes lenguajes de programación, y ejecutadas sobre diversas plataformas, pueden utilizar los servicios web para intercambiar datos biométricos en redes como Internet.

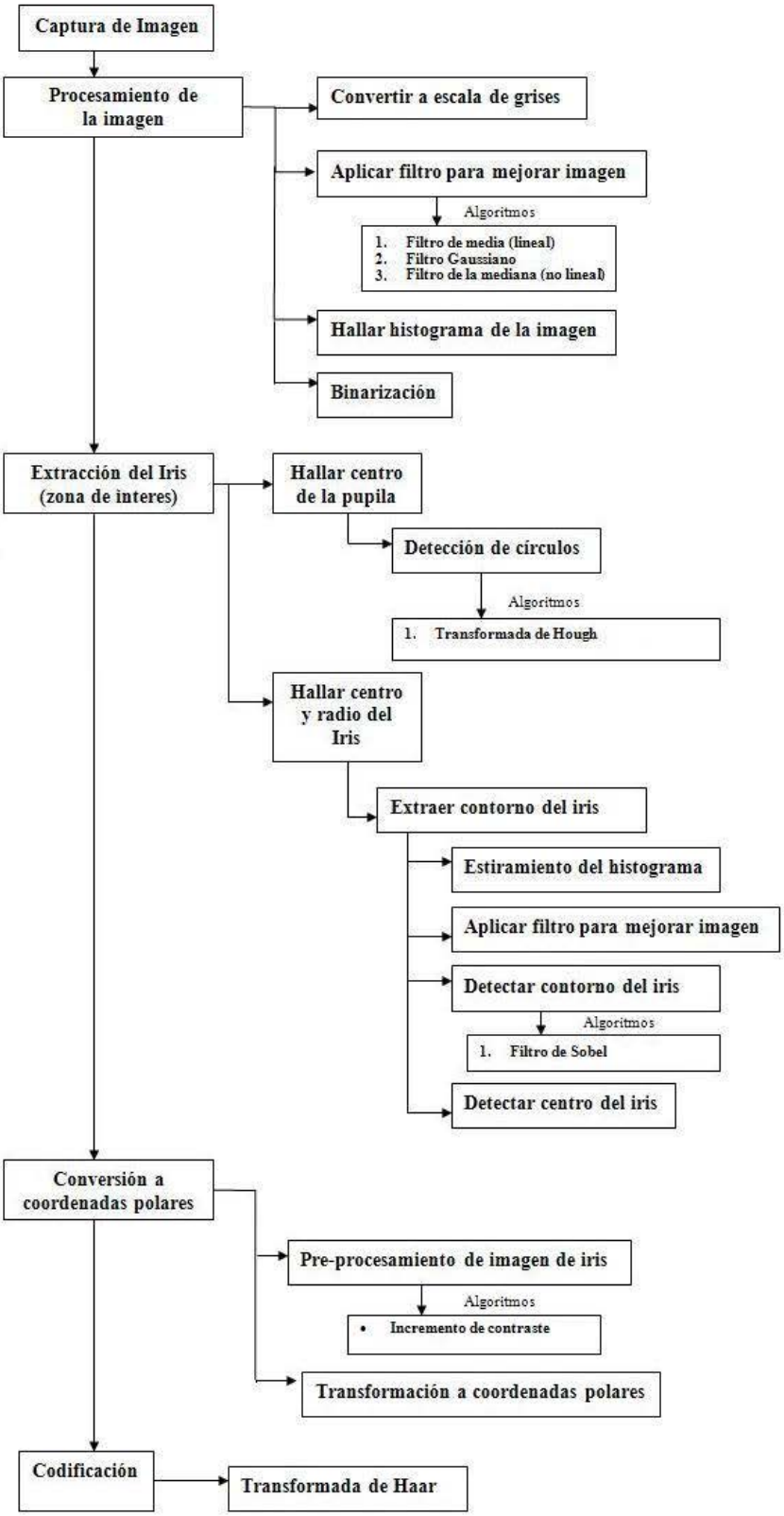

FIGURA 3: Etapas para la codificación del iris.

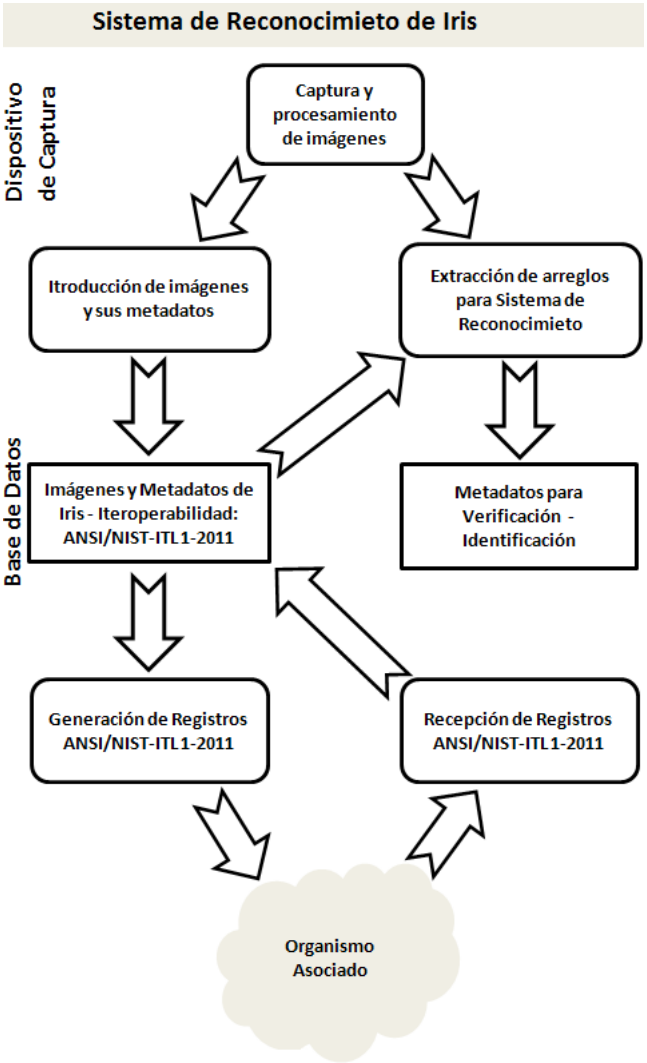

Figura 4: Esquema simplificado del Sistema de Reconocimiento de Iris, con módulos de generación de registros de transacciones ANSI/NIST-ITL 1-2011.

Por otra parte, para probar la fiabilidad de la aplicación desarrollada, se realizaron ensayos utilizando imágenes de iris de la base de datos CASIA [47], y como indicadores de performance se utilizaron el FAR (*False Accept Rate*) y el FRR (*False Reject Rate*).

En las pruebas realizadas utilizando una muestra de la base de datos CASIA, tanto el FAR como el FRR arrojan resultados de 0,01. Para obtener estos resultados se ajustó al valor Umbral (valor límite en las distancias de Hamming obtenidas de las plantillas en que se acepta o rechaza una verificación) considerando la distribución de valores de estas distancias de las muestra observada. Teniendo en cuenta que una tasa de FAR es buena si es menor a 0,015 y una tasa de FRR buena es menor a 0,05, los valores obtenidos se consideran aceptables.

Los resultados obtenidos, muestran que el sistema es bueno basado en los indicadores FAR y FRR con las muestras seleccionadas de la base de datos CASIA. Sin embargo, esto se obtiene ajustando el umbral a los valores de la muestra utilizada. Esto es, las distancias obtenidas entre la plantilla de un individuo X, con plantillas obtenidas con imágenes de iris del mismo individuo (quien dice ser), respecto a las distancias de plantillas obtenidas del iris de otros individuos (impostores), no son significativamente diferentes (Figura 5).

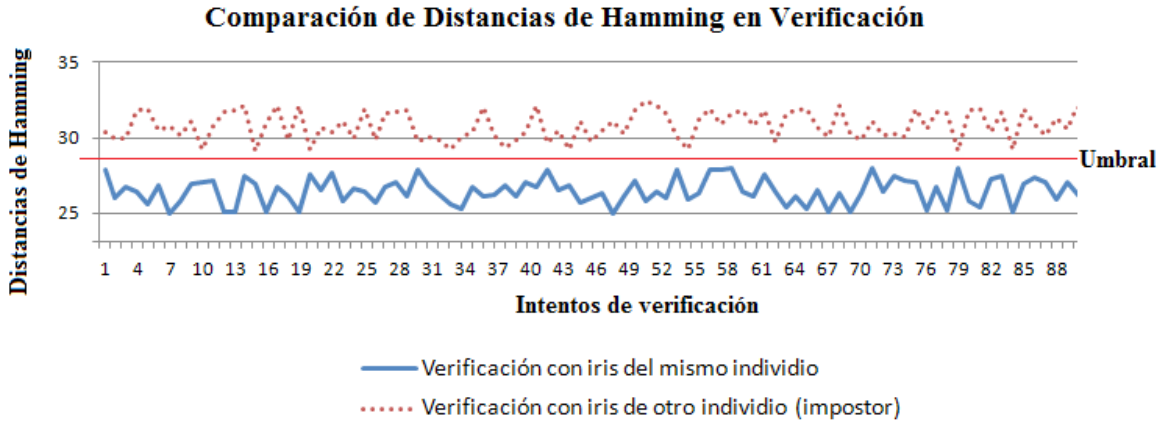

Figura 5: Distancia entre verificaciones. Establecimiento del umbral.

De esto se desprende, que en un sistema de tiempo real, estos indicadores pueden desmejorar, dado que no se puede estar adaptando los valores de los umbrales como se realizó con la muestra seleccionada. Por este motivo, se considera conveniente, como trabajo futuro, buscar otras alternativas para mejorar a fiabilidad y la robustez del sistema de reconocimiento.

VI. Conclusiones

En el presente proyecto se trabajó en el análisis de las dificultades en los procedimientos de autentificación de personas en organismos públicos y en la implementación de posibles soluciones a través de la utilización de sistemas biométricos.

En primer lugar, se realizó un relevamiento bibliográfico de los principales trabajos en el área, se definieron conceptos y terminología básica y las ventajas que dichos sistemas introducen frente a los métodos tradicionales de autentificación. Se expuso el modelo general de funcionamiento de los sistemas biométricos, así como los parámetros existentes y a tener en cuenta para el reconocimiento y la clasificación de los sistemas. También se analizaron los sistemas biométricos estáticos y dinámicos y se determinaron y clasificaron los factores que afectan al rendimiento de estos sistemas.

De este primer estudio se puede concluir que, si bien de las tecnologías biométricas analizadas no existe una modalidad biométrica que mejor se adapte para todas las implementaciones, la huella digital es uno de los sistemas más fiables y, además, se utiliza en numerosas aplicaciones por ser rápido y de bajo costo. De los sistemas de huella dactilar, los más resistentes y fiables son los que están basados en un escáner o sensor óptico. Como una de las principales contras de este sistema, es la susceptibilidad a ser engañado a través de diferentes artilugios (dedo de goma, imagen húmeda, etc.) y puede presentar problemas de universalidad (hay personas que tienen gastados los dedos).

Como una de las alternativas biométricas más confiables según la bibliografía, están los sistemas de reconocimiento de iris. Estos sistemas han tenido un amplio desarrollo en los últimos años. Las principales ventajas que tienen sobre las huellas dactilares son: los patrones de iris son invariables en el tiempo y su falsificación es muy difícil. Cabe destacar además, que no se tiene la necesidad de contacto directo con el dispositivo de captura, lo que lo hace menos intrusivo, y extiende la vida útil del dispositivo.

Otro de los sistemas que se destaca entre los analizados, es el de reconocimiento por geometría de mano. Si bien sus tasas de falsos positivos no son excelentes, son muy usados para el control de

acceso físico y de asistencia de personal, sobre todo por su robustez (para ser utilizado en talleres o otras áreas donde los dispositivos de huellas pueden dañarse o ensuciarse fácilmente).

Un sistema que ha registrado un gran avance en la última década, es el de reconocimiento facial. Este sistema, es uno de los menos intrusivos ya que el usuario puede estar sometido a un sistema de reconocimiento facial sin saberlo. Esta técnica, combinada con otras de encriptación, ha sido ampliamente utilizada en Internet, para resolver el problema de la autenticación de los usuarios, servidores, páginas y sitios. Sin embargo hay factores que pueden dificultar el reconocimiento facial: las dimensiones y características de la cara dependen del ángulo, expresión y edad; también la barba y anteojos pueden dificultar el reconocimiento.

En lo que refiere a los sistemas biométricos dinámicos, los más destacados son el reconocimiento de voz y de firma.

El reconocimiento de voz, gracias al compromiso de los investigadores y el apoyo de instituciones públicas y privadas, ha conseguido un importante avance en la tecnología de la computación y comunicación. Sin embargo, los cambios de voz debidos a cualquier enfermedad, ronquera o ruidos externos pueden traer dificultades en el reconocimiento de la voz. Los sensores de adquisición (micrófonos) son económicos, y en el caso de acceso telefónico, ya sea fijo o móvil, no se requiere ningún hardware específico adicional, puesto que el propio micrófono del teléfono realiza la función de captura. En cambio, otros rasgos como huella, iris, geometría de la mano, entre otros, implican la necesidad de adquirir un equipo adicional, no siempre con precio razonable.

La verificación dinámica de la firma es un sistema biométrico que puede integrarse fácilmente a los sistemas existentes debido a la disponibilidad y difusión de digitalizadores de firma y aceptación del público a la recolección de características. Sin embargo, este sólo puede usarse con propósitos de verificación y la variabilidad intra clase puede provocar un rendimiento no del todo ideal para algunas aplicaciones.

Más allá de las ventajas de algunos sistemas mencionados anteriormente, las tendencias actuales en reconocimiento biométrico, ponen énfasis en la combinación de tecnologías en sistemas multimodales; particularmente, qué mejoras posibles se pueden lograr en estas combinaciones. Uno de los problemas principales para los investigadores en sistemas multimodales, es la escasez de bases de datos multimodales para testear sus algoritmos.

Teniendo en cuenta este análisis y las primeras conclusiones respecto a los diferentes rasgos biométricos, se realizó un estudio comparativo de campo en la Municipalidad de Concordia con quien existe un acuerdo marco de colaboración y asistencia y un convenio específico con el presente proyecto.

En base a las características requeridas y al presupuesto con el que cuenta el proyecto, se planteó la adquisición de un dispositivo de geometría de mano y un dispositivo multi-biométrico (de rostro y huella dactilar).

En base a las pruebas realizadas con los dispositivos involucrados se concluye que el sistema multi-biométrico presenta actualmente mayores beneficios para su implementación. La razón de ello, radica en que al incorporar dos modalidades de identificación en un mismo dispositivo, los parámetros de medición mejoran notablemente el rendimiento y la exactitud de la comparación.

Por último se realizó un diagnóstico de las dificultades de los procedimientos actuales en áreas claves de la Municipalidad de Concordia y se establecieron las necesidades de implementación de sistemas de control de acceso y otros aspectos relacionados con la seguridad en estas áreas. Parte de las recomendaciones realizadas ya se están ejecutando en el área de informática de la Municipalidad (como se menciona en el apartado V.III).

También se propuso el desarrollo de sistemas biométricos propios (como es el reconocimiento del iris, que se menciona en el apartado V.IV). Si bien se culminó el software, no se pudo terminar el prototipo debido a la falta de ofertas del dispositivo de captura por parte de los proveedores, por lo que no

pudo ser testeado en el estudio de campo. Cabe destacar que, tal como fue previsto en los objetivos del proyecto, se trabajó en una arquitectura basada en estándares orientados a la interoperabilidad entre aplicaciones. Particularmente, se trabajó con el formato de datos para el intercambio de imágenes de iris adecuado a la norma ANSI/NIST ITL-2011. Mediante el uso de esta arquitectura, aplicaciones clientes desarrolladas en diferentes lenguajes de programación, y ejecutadas sobre diversas plataformas, pueden utilizar los servicios web para intercambiar datos biométricos en redes como Internet.

Referencias Bibliográficas

1. Benedetto M. Identificación de personas a través de sistemas biométricos. [tesis de Maestría en Sistemas de Información]. Entre Ríos: Universidad Nacional de Entre Ríos, Facultad de Ciencias de la Administración; 2009.
2. Cole S. Suspect Identities: A History of Fingerprinting and Criminal Identification. Cambridge, MA, USA: Harvard University Press; 2001.
3. Mc Mahon Z. Biometrics: History. Indiana University: Indiana University Computer Science Department; 2005. Accesible en URL: http://www.cs.indiana.edu/~zmcmahon/biometrics-history.htm. Consultada en noviembre 2009.
4. Daugman J. How iris recognition works. Cambridge, U.K.: University of Cambridge, The Computer Laboratory; p. 21–30. Accesible en URL: http://www.cl.cam.ac.uk/~jgd1000/irisrecog.pdf. Consultada en noviembre 2009.
5. Jain A, Ross A, Prabhakar S. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology; 2004. 14(1): 4–20.
6. Maltoni D, Maio D, Jain A, Prabhakar S. Handbook of Fingerprint Recognition. NY: Springer; 2003.
7. Ching-Liang S. Hand Shape Recognition by Hand Shape Scaling, Weight Magnifying and Finger Geometry Comparison. Heidelberg: Springer-Verlag Berlin. MIRAGE; 2007. p. 516-524.
8. Gross R. Face Databases. In: Li S, Jain A, editors. Handbook of Face Recognition. United States of America: Springer Science+Business Media, Inc; 2005. p. 1-22
9. Bertolín J, Bertolín T. Análisis en torno a la tecnología biométrica: parámetros de precisión-rendimiento. Revista Española de Electrónica. 2007; 630: 56-67.
10. Tapiador Mateos M, Siguenza Pizarro J. Tecnologías biométricas aplicadas a la seguridad. Madrid: Ra-Ma; 2005.
11. Miller B. Everything you need to know about biometric identification. Personal Identification News 1988 Biometric Industry Directory. Washington DC: Warfel & Miller, Inc.; 1988.
12. Wayman J. A definition of biometrics. San Jose State University: National Biometric Test Center Collected Works; 2000; p. 1997–2000.
13. Colaboradores de Wikipedia. Biometría. Wikipedia: La enciclopedia libre. Accesible en URL: http://es.wikipedia.org/wiki/Biometr%C3%ADa. Consultada en noviembre de 2009.
14. Kimaldi. Área de conocimiento: Biometría. Accesible en URL: http://www.kimaldi.com/area_de_conocimiento/biometria/que_es_la_biometria. Consultada en marzo de 2010.
15. Partnerzone Seguridad. Seguridad biométrica. Prolifera la adopción de sistemas de seguridad biométricos. Accesible en URL: http://www.linux-itt.com/2008/10/prolifera-la-adopcin-de-sistemas-de.html. Consultada en marzo de 2010.
16. Casal G, Rovolta M, compiladores. Biometrías. Herramientas para la Identidad y la Seguridad Pública. Jefatura de Gabinete de Ministros. Presidencia de la Nación. Buenos Aires, Argentina: Gráfica Barsa; 2010.
17. Woodward J, Orlans N, Higgins P. Biometrics. New York: McGraw Hill Osborne; 2003.
18. Biometrics and Standards. ITU-T Technology Watch Report. Accesible en URL: http://www.itu.int/dms_pub/itu-t/oth/23/01/T230100000D0002PDFE.pdf. Consultada en diciembre 2009.
19. Wayman J. Technical testing and evaluation of biometric identification devices. In: Jain A, Bolle R, Pankanti S, editors. Biometrics: Personal Identification in Networked Society. San Jose, CA: Kluwer Academic Press; 2002. P. 345-368.

20. Sociedad Española de Biometría. Accesible en URL: www.iata.csic.es/IBSREsp/. Consultada en diciembre 2009.
21. Biometrics Institute. Biometrics Institute Information. Biometrics Institute Limited 2008. Accesible en URL: http://www.biometricsinstitute.org/. Consultada en febrero 2010.
22. International Biometric Industry Association. Biometrics and Human Identity Authentication. International Biometric Industry Association 2008. Accesible en URL: http://www.ibia.org/biometrics/. Consultada en diciembre 2009.
23. Biometrics at the frontiers: assessing the Impact on Society (UE). Technical Report Series. For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE). European Communities; 2005. Accesible en URL: www.europeanbiometrics.info/ images/resources/21_936_file.pdf.
24. Plataforma Biométrica Homini. Hominí S.A.; 2004. Accesible en URL: http://www.homini.com/ new_page_1.htm.
25. IBG BiometricStore; 2008. Acessible en URL: http://www.ibgweb.com/.
26. Mentes curiosas. NEO; 2006. Accesible en URL: http://www.neo.uol.com.ar/ edicion_0006/nota_02.htm.
27. Zhang D, Jing X, Yang J. Biometric Image Discrimination Technologies Computational Intelligence and its applications series. United States of America: Idea Group Inc.; 2006.
28. Wayman J. Biometrics – Now and Then: The development of biometrics over the last 40 years. Biometrics in the Reflection of Requirements: Second BSI Symposium on Biometrics. Bonn: SecuMedia; 2004.
29. Biometrics: Department of Defense. Biometrics 101. Accesible en URL: http://www.biometrics.dod.mil/bio101/assets/images/bio101/fingerprint_diagram.jpg. Consultada en 2011.
30. Bromba M. Bioidentification: Frequently Asked Questions. Accesible en URL: http://www.bromba.com/faq/fpfaqe.htm#Fingerprint-Sensoren. Consultada en 2010.
31. Jain A, Bolle R, Pankanti S. Personal Identification in a networked Society. Massachusetts: Kluwer Academic Publishing; 1999.
32. Galvis Traslaviña C. Introducción a la Biometría. Accesible en URL: http://www.monografias.com/ trabajos43/biometria/biometria3.shtml. Consultada en 2011.
33. International Organization for Standardization (ISO). Stages of the development of International Standards. Accesible en URL: http://www.iso.org/iso/standards_development/processes_and_procedures/stages_description.htm.
34. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). Accesible en URL: http://www.standardsinfo.net/ info/livelink/fetch/2000/148478/6301438/aboutstd.html.
35. World Standards Services Network (WSSN). Accesible en URL: http://www.wssn.net.
36. Gutierrez C, Gallagher P. Secure Hash Standard (SHS). Federal Information Processing Standards Publication (FIPS). PUB 180-3. Accesible en URL: disponible en: http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf.
37. NSTC Subcommittee on Biometrics and Identity Management. NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards. Accesible en URL: http://www.biometrics.gov/Standards/ NSTC_Policy_Bio_Standards.pdf.
38. Wing B. Information Technology: American National Standard for Information Systems Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information. ANSI/NIST-ITL 1-2011; 2011.
39. Thill E. Biometrías 2. 1ra ed. Buenos Aires: Jefatura de Gabinete de Ministros. Presidencia de la Nación; 2011.
40. Podio F, Dunn J, Reinert L, Tilton C, Struif B, Herr F, et al. Common Biometric Exchange File Format (CBEFF). NISTIR 6529-A; 2004. Accesible en URL: http://csrc.nist.gov/publications/nistir/NISTIR6529A.pdf.
41. International Committee for Information Technology (INCITS). Accesible en URL: http://www.incits.org.
42. Information Technology - Iris Image Interchange Format. ANSI INCITS 379-2004; 2004.
43. Information Technology - Biometric data interchange formats - Part 6: Iris Image Data. ISO/IEC 19794-6:2005. 1st ed; 2005.

44. Roberts W, Liebeskind S, Kindl M. National Information Exchange Model Naming and Design Rules. NIEM Technical Architecture Committee (NTAC). Versión 1.3; 2008. Accesible en URL: https://www.niem.gov/ documentsdb/Documents/Technical/NIEM-NDR-1-3.pdf.
45. SUPPLEMENT: VOICE RECORD. Investigatory Voice Biometrics Committee Report. ANSI/NIST-ITL 1-2011. Draft Version 5a. ; 2013. Accesible en URL: http://www.nist.gov/itl/iad/mig/upload/ANSI_NIST-ITL-1-011_Supplement_ V5a.docx.
46. Fuenmayor G. Avances en técnicas biométricas y sus aplicaciones en seguridad. Facultad de Ingeniería de la Universidad Central de Venezuela; 2007. Accesible en URL: http://neutron.ing.ucv.ve/comunicaciones/Asignaturas/DifusionMultimedia /Tareas%202006-1/Tecnicas%20biometricas.pdf
47. CASIA. CASIA iris image database. Chinese Academy of Sciences: Institute of Automation. Accesible en URL: http://www.sinobiometrics.com.