ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Biometría de voz en la seguridad de la información en las notarías públicas peruanas, 2017

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:
Maestro en Ingeniería de Sistemas con mención en Tecnologías de la Información

AUTOR:
Br. Cienfuegos Solís Jorge Luis

ASESOR:
Mg. Visurraga Agüero Joel Martin

SECCIÓN:
INGENIERÍA

LÍNEA DE INVESTIGACIÓN:
TELECOMUNICACIONES

LIMA - PERÚ
2017

_____

Dra. Violeta Cadenillas Albornoz

Presidente

_____

Dr. César Humberto Del Castillo Talledo

Secretario

_____

Dr. Joel Martín Visurraga Agüero

Vocal

Dedicatoria

A mis hijos, de quien siempre esperaré algo mejor que lo que hace esta persona, como semilla de conocimiento para las nuevas generaciones.

A toda persona que desee comparar sus conocimientos con un nuevo enfoque y utilidad de la voz y para todos aquellos que su imaginación les permita graficar el sonido de un saludo o dibujar el énfasis de una conversación.

Agradecimiento

A Dios, por mantener todavía vivo en mí, la curiosidad y el deseo de estudiar lo que es seguro para algunos y un manantial de dudas para otros.

Quien cree todo lo que ve, ve solo todo lo que cree. La amplitud de posibilidades de solución depende tan solo de mentes que conciben el planteamiento de un problema no como algo ya resuelto sino como el inicio del encuentro con "la solución".

Declaración de Autoría

Yo, Jorge Luis Cienfuegos Solís, estudiante de la Escuela de Postgrado, Maestría de Ingeniería de Sistemas, de la Universidad César Vallejo, Sede Lima; declaro el trabajo académico titulado “Biometría de voz en la seguridad de la información en las notarías públicas peruanas, 2017”, presentada, en 85 folios para la obtención del grado académico de Maestro en Ingeniería de Sistemas con mención en Tecnologías de la Información, es de mi autoría.

Por tanto, declaro lo siguiente:

He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajos académicos.

No he utilizado ninguna otra fuente distinta de aquellas expresamente señaladas en este trabajo.

Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o título profesional.

Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.

De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinen el procedimiento disciplinario.

Lima, 23 de setiembre del 2017

_____

Jorge Luis Cienfuegos Solís

DNI: 09250121

Presentación

Señores miembros del jurado calificador: Dando cumplimiento a las normas del Reglamento de Grados y Títulos para la elaboración y la sustentación de la Tesis de la sección de Postgrado de la Universidad Cesar Vallejo, para optar el grado de maestro en Ingeniería de Sistemas con mención en Tecnologías de la Información, expongo ante ustedes la tesis titulada: Biometría de voz en la seguridad de la información en las notarías públicas peruanas, 2017. La investigación persigue demostrar la mejora que se consigue con la Biometría de voz en el proceso de seguridad de la información en las notarías públicas peruanas, 2017.

La investigación está presentada en ocho capítulos, donde: el primer capítulo correspondiente a introducción, detalla la realidad problemática, en los ámbitos internacional, nacional, local e institucional. De igual forma consta de los trabajos previos relacionados a la Tesis de investigación en los ámbitos internacional y nacional, las teorías relacionadas al tema, así como la formulación del problema, la justificación del estudio y la especificación de las hipótesis y los objetivos. El segundo capítulo correspondiente a método, describe el tipo de investigación, diseño de investigación, la definición conceptual y operacional de las variables a usar, el manejo de la población, muestra y muestreo, las técnicas e instrumentos de recolección de datos (su validez y confiabilidad), los métodos de análisis de datos y los aspectos éticos. En el tercer capítulo se exponen los resultados obtenidos, en el cuarto capítulo la discusión, en el quinto capítulo las conclusiones, en el sexto capítulo las recomendaciones y en el séptimo capítulo la propuesta. El octavo capítulo detalla las referencias bibliográficas usadas en la presente investigación para culminar con la parte final de la investigación que corresponde a los anexos.

Señores miembros del jurado espero que esta investigación se ajuste a las exigencias establecidas por la Universidad y merezca su aprobación.

El autor

Índice

Índice de Tablas

Índice de Figuras

Resumen

La Tesis de Investigación que se presenta corresponde a la Línea de Investigación de Telecomunicaciones y plantea la aplicación de la Biometría de Voz en el proceso de la Seguridad de la Información cuando se realiza en el entorno de las Notarías Públicas peruanas en el 2017.

El objetivo principal es demostrar en que forma la Biometría de Voz mejora el proceso de la Seguridad de la Información. Para ello se trabaja como herramienta tecnológica o variable independiente a la Biometría de Voz y al proceso o variable dependiente donde se aplica la herramienta tecnológica, la Seguridad de la Información. Así mismo para medir cuantitativamente la mejora que ofrece la Biometría de Voz, se utilizaron los indicadores de medición: grado de fiabilidad y grado de eficiencia. Además haciendo uso de Tablas y Gráficas provenientes del Software de IBM SPSS, que sirvió de herramienta para el uso de coeficientes estadísticos, permitió establecer entre otras cosas la mejora existente que se produce cuando se realiza la aplicación de la Biometría de Voz en el proceso de la Seguridad de la Información.

El tipo de investigación: Aplicada es la que corresponde a la presente Tesis. De igual forma el tipo de diseño correspondiente es: el diseño del tipo pre experimental. Al ser este tipo de diseño, se usó en los datos cuantitativos como metodología de investigación la técnica de la observación.

Palabras Claves: Biometría de Voz, Seguridad de la Información, Proceso.

Abstract

The Research Thesis presented corresponds to the Telecommunication Research Line and proposes the application of Voice Biometrics in the Information Security process when it is carried out in the Peruvian Public Notaries' environment in 2017.

The main objective is to demonstrate to what extent Voice Biometrics improves the Information Security process. For this purpose, we work as a technological tool or independent variable to Voice Biometry and to the process or dependent variable where the technological tool, Information Security is applied. Likewise, to measure quantitatively the improvement offered by Voice Biometry, the measurement indicators were used to measure the degree of reliability and degree of efficiency. In addition, using Tables and Graphs from the IBM SPSS Software, which served as a tool for the use of statistical coefficients, allowed to establish, among other things, the existing improvement that occurs when the application of Voice Biometrics in the process of Information Security.

The type of research: Applied is the one that corresponds to the present Thesis. In the same way the corresponding design type is: the design of the pre-experimental type. As this type of design, the technique of observation was used in quantitative data as research methodology.

Key Words: Voice Biometrics, Information Security, Process.

I. Introducción

1.1. Realidad Problemática

Internacional

Hablar de la Seguridad de la Información en términos de modernidad tecnológica en la actualidad es introducir en este tema a instituciones del nivel de la World Wide Web Consortium (W3C). Como lo podemos apreciar en Aucanshala y Senteno (2016, p.1), el cual evidencia el comportamiento o tendencia que está siguiendo la W3C en este tema en la actualidad; es decir, comprobar que la tendencia tecnológica es pedir algo más efectivo como seguridad que una simple contraseña o clave que nos permita acceder o aperturar el ingreso a la información en la Web. La tendencia empuja a que sea el reconocimiento biométrico la asistencia en la cual puedan depositar seguridad las instituciones públicas y privadas cuando se trate de autenticación de alguna persona que va a acceder a algún tipo de información. Este panorama como lo menciona Gartner (2016) en su introducción resalta la importancia que toma la Biometría como tecnología de autenticación relacionada con la identidad de alguien sobre otros métodos que pudieran usarse. Y esto se menciona a sabiendas de la limitaciones en la implementaciones que se realizan en el consumidor de los métodos biométricos, como por ejemplo el caso de las huellas digitales, donde todos de alguna u otra manera aceptan la masividad de su uso como método biométrico de autenticación por las ventajas únicas que ellas representan. Si solamente observásemos el crecimiento obtenido en el uso del Sistema AFIS (Automated Fingerprints Identicate System) a nivel mundial, notaríamos que la Biometría es la tecnología de identificación de mayor tendencia en la actualidad. En tal sentido la Biometría de Voz, busca ser un complemento de seguridad que pueda percibir el usuario cuando se intenta suplantar su identidad por querer accederse a una determinada información, como nos lo hace saber el Instituto de Ingeniería Eléctrica y Electrónica (IEEE) a través de una serie de estándares que relacionan los tipos de biometría existentes en la actualidad con el correspondiente código de imágenes que permite manejar el rasgo biométrico. De tal forma por ejemplo en Ruiz et al. (2016, p.244-245), donde nos informa de una Arquitectura genérica para Datos Biométricos, nos indica el estándar ANSI/NIST-ITL 1-2011, para imágenes de iris, el cual solamente permite JPEG 2000 (Estándar ISO/IEC

15444:2004) y PNG (Estándar ISO/IEC 15948:2004). Así mismo en dicho artículo se menciona el registro Tipo 11 del estándar ANSI/NIST-ITL 1-2011 en donde ubica al rasgo de voz como un elemento más dentro de la arquitectura propuesta.

Nacional

El Seminario Internacional de Biometría organizado por el Registro Nacional de Identificación y Estado Civil en Lima (RENIEC) a nivel nacional el seis, siete y ocho de Agosto del 2014, puede quizás ser uno de los últimos mejores referentes de tendencias relacionados con la Biometría a nivel nacional. En dicho Seminario se puso de manifiesto cuán importante es involucrarse en este tema, al ser la forma tecnológica actual de identificación de alguien y no sólo una original idea que surge del mercado, como nos lo hace notar PhD Bradford J. Wing (RENIEC-DH, 2014, p.8), Presidente de los Estándares del Consejo Nacional de Ciencia y Tecnología de la Casa Blanca quien casualmente en dicho Seminario expuso el tema relacionado al uso de los estándares correctos y la calidad de los mismos, además de disertar sobre la biometría facial. Así mismo la Mg. Ariel Freideberg, Vicepresidenta de Desarrollo de Negocios en el equipo Biometría de voz de Nuance Comunications, expuso todo lo relacionado a Biometría de Voz. Es evidente observar que es el RENIEC el eje sobre el cual se desenvuelve la Tendencia Tecnológica en la seguridad de la información. Bastaría con ver los cambios tecnológicos últimos producidos en el RENIEC, como por ejemplo la identificación de personas cuya identidad se desconozca Peralta (2015, p.283), o quizás por el lado de la seguridad de la información, donde se autorizó a el RENIEC la adquisición del Sistema Automático de Impresiones Dactilares AFIS y su posterior actualización mediante la Resolución Jefatural 293 (2013). Se puede por lo tanto concluir sin temor a equivocarse que el gobierno en su conjunto ha considerado sumamente importante todo lo concerniente al manejo y uso de la biometría como herramienta tecnológica segura para la identificación de las personas.

Local

El incremento de estafas y robos producidos últimamente en la mismas instituciones bancarias, véase el reporte periodístico El Comercio (19 de abril de

2014), sucedido en la capital de la República, nos lleva casi en forma obligada a tomar a la tecnología biométrica como la alternativa más segura en la verificación de la identidad de una persona, tal como nos lo menciona Llatas (2015, pp.17-21). La Biometría de Voz, por el momento utilizada discretamente en el ámbito local por instituciones particulares, trata de crecer con mayor nivel de expectativa por el menor margen de error que manifiesta al relacionarla con la identificación dactilar, como nos lo hace notar Loyola (2015, pp.26-27).

Institucional

Las Notarías Públicas peruanas han permitido el acceso a la biometría como herramienta en el ámbito legal desde hace algunos años. Esto se evidencia notoriamente al observarse la modernización que en los últimos años ha tenido el Registro Nacional de Identificación y Estado Civil en Lima (RENIEC) en aspectos relacionados a mecanismos de actualización de Identificación de personas lo que a su vez ha permitido mejorar los Sistemas de seguridad en los diversos trámites que se realizan en las Notarías Públicas Peruanas. El proceso de mejora, claramente se nota en el cambio originado en el Documento Nacional de Identidad (DNI) como lo manifiesta Peralta (2015, p.283). La Biometría ha entrado de una forma tan vigorosa, que se han creado una serie de conflictos por la obligatoriedad que se va teniendo en algunas instituciones públicas para la realización de algunas transacciones o registros públicos en la Superintendencia Nacional de Registros Públicos (SUNARP), véase Mendoza (2016). Así por ejemplo, si consideramos que la actualización o el registro inicial de un predio, son uno de los trámites que con mayor frecuencia se realiza en las Notarías Públicas Peruanas, la cual supone una identificación previa de las personas involucradas en dicho trámite. Los niveles de Seguridad de la información que manejan las Notarías Públicas Peruanas se ven aseguradas mediante el uso de la biometría en los actuales Documentos Nacionales de Identidad. Lo que se viene observando así mismo es que la tendencia del uso de la biometría en estas instituciones sigue el camino del uso de la biometría de la forma multimodal, es decir donde el proceso de identificación de identidad viene a resultar ser reconocimientos biométricos de más de un tipo de biometría. El objetivo con la Biometría de voz en las instituciones o empresas es que cualquier persona pueda

disponer tanto de una huella dactilar como de una huella de voz, para que a través de lectoras de huellas biométricas, como nos lo dice Mallqui (2015, p.9), permita mejorar la seguridad de la información en las Notarías Públicas Peruanas. Observar los diagramas del capítulo VII: Propuesta, sobre todo los referidos a los puntos 7.3 y 7.4, correspondientes a Arquitectura de Tecnología de Información y Prototipeo respectivamente, donde se expone y explica la implementación de la Biometría de voz en las Notarías Públicas Peruanas.

1.2. Trabajos Previos:

Internacional

Según Escajedo (2015) en su Investigación "Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas" realizado en la Universidad de Alicante de España, cuyo propósito fue estudiar la situación en que se encuentra los sistemas biométricos contemporáneos, para bajo ese contexto poder solucionar dos preguntas: La primera de ellas fue saber hasta qué punto y de qué manera ofrecían las tecnologías de reconocimiento biométrico la posibilidad de identificar a un ser humano como único en el mundo y la segunda pregunta era averiguar las razones que estaban permitiendo y cuales deberían impedir la posibilidad de construir infraestructuras de reconocimiento biométrico "que aseguren la identificación en todo momento". La investigación le permitió concluir en la existencia de una coincidencia por parte del reconocimiento biométrico contemporáneo como del reconocimiento biométrico tradicional, la cual es la intención de medir la singularidad de cada persona respecto de un rasgo biológico (estático o dinámico) que nos lo manifestó Escajedo como universal y permanente en los humanos, por otro lado aseveró que las tecnologías de reconocimiento biométrico responden a una necesidad y surgen de la evolución que viene experimentando la ciencia forense en su aplicación con las mejoras que aportan el desarrollo de las tecnologías de computación, finalmente afirmó que todavía no se da una terminología establecida relacionada a las tecnologías de reconocimiento biométrico.

La investigación elaborada por Escajedo es un trabajo bastante exhaustivo sobre biometría ya que lo presenta como tesis doctoral, resultando ser una piedra angular del trabajo de investigación que he realizado. En su tesis es muy enfático al asegurar que las tecnologías de reconocimiento biométrico se presentan mediante el resultado del comportamiento en el tiempo que ha venido experimentado la ciencia forense que ha asimilado las mejoras experimentadas en el crecimiento de todas las innovaciones tecnológicas últimamente introducida en los ámbitos de sistemas y cómputo.

Según Cárdenas (2015) en su Tesis "Diseño de la Estrategia de Implementación de un Sistema de Prevención del Fraude en el Sector Financiero, mediante el uso de Biometría Facial y por Voz" realizado en el Sistema Nacional de Comunicaciones Financieras de Chile, cuyo propósito fue elegir la mejor tecnología de biometría facial y por voz que se acomoden mejor a las condiciones técnicas, de seguridad, legal y de negocio al sector financiero de Chile. La investigación le permitió concluir que el marco legal nacional es el factor limitante para el uso adecuado de los software biométricos existentes en el mercado, así mismo concluyó que a través de la metodología de exploración de nuevas tecnologías, se estudiaran los beneficios del uso de este tipo de biometría y de qué manera son herramientas en la prevención de fraude en el sistema bancario, de igual forma alertó que es de suma importancia estar constantemente actualizando y entregando mejoras a los software, debido a que los cambios tecnológicos se dan a cada momento y por tanto no se puede esperar que los resultados del proyecto sean los calculados si detrás no existe un apoyo de mejora y de actualización. Por esta razón aseveró que el Sistema Nacional de Comunicaciones Financieras de Chile tiene una responsabilidad no menor en el éxito del servicio a ofrecer. Por esta misma razón afirmó que parte de la estrategia consiste en trabajar con personal que esté direccionado a los sistemas biométricos facial y por voz.

Cárdenas realiza una tesis que trae todos los conocimientos que lo involucra con el tópico de la biometría de voz, aportando de esta manera puntos de vistas diferentes y sumamente útiles para la tesis que he realizado. Él señala

las ventajas del uso de este tipo de biometría y las formas de aporte en la prevención de fraude en el sistema bancario chileno, señalando que es el marco legal nacional el que limita los alcances del uso de estas tecnologías.

Según Anguiano, Chávez y Vásquez (2011) en su Investigación "Sistema de Seguridad activado por medio de la Voz Humana" realizado en la Escuela Superior de Ingeniería Mecánica del campus Zacatenco - México D.F., cuyo objetivo fue diseñar un sistema de seguridad basado en el reconocimiento de voz humana, para autenticar a una persona. La investigación les permitió concluir que el tono fundamental de una persona es una característica única que se presenta y que en pocos casos, diferentes personas tendrán el mismo tono fundamental, por lo que nos permite identificar la voz de cada individuo a partir de esta característica, asimismo concluyeron que el sistema es vulnerable a cualquier cambio de tonalidad de la voz del usuario, es decir el sistema no reconoce al usuario original si este cambia la tonalidad de su voz (más grave o más agudo), por lo que según ellos, se obliga a utilizar el mismo tono de voz con el que se hallan hecho las grabaciones almacenadas en la base de datos para que el sistema pueda reconocerlo, asimismo concluyen que el correcto funcionamiento del sistema depende del estado de cansancio de las cuerdas bucales del usuario, por lo que el usuario original necesita estar relajado y con la garganta descansada para que el sistema pueda reconocer su voz.

La investigación realizada por Anguiano, Chávez y Vásquez está inmersa en la temática de la biometría de voz, propósito central de la tesis que he realizado. Ellos afirman que el grado de fiabilidad de un Sistema de seguridad en base a voz depende del estado de cansancio de las cuerdas bucales del usuario, por lo que el usuario original necesita estar relajado y con la garganta descansada para que el sistema pueda reconocer su voz.

Según Gonzáles (2013) en su Investigación "Sistema de Identificación Biométrica basado en Huella Dactilar mediante Binarización sobre Plataformas Android" realizado en la Universidad Carlos III de Madrid - España en base al conocimiento del lenguaje C# en el área de obtención de imágenes ya

implementadas y al manejo del algoritmo Bozorth3, cuyo objetivo general fue que el común del público acceda fácilmente cuando se enfrenta a dispositivos Android en los cuales el sistema de identificación biométrica ha sido convenientemente introducido. La investigación le permitió concluir que el proyecto realizado resulta bastante prometedor, ya que la identificación a través de la huella dactilar realizado entre personas se realiza con una gran dosis de funcionabilidad. Sin embargo es necesario recalcar que existe una limitación con la aplicación Fprint App desarrollada para el sistema operativo Android, ya que esta aplicación requiere de imágenes de huellas digitalizadas para tener un funcionamiento fiable, situación que en la actualidad no se presenta, no llegándose a cumplir totalmente con la verificación e identificación de candidatos a través de la huella dactilar.

Gonzales con su tesis realizada encaja en el marco de la biometría de huella dactilar. Él nos precisa que en base al manejo adecuado del lenguaje C# en el área de los métodos de obtención de imágenes ya implementadas adecuadamente y al conocimiento del algoritmo Bozorth3 lograrán un rápido entendimiento de su uso pudiéndose volcar para todo tipo de público.

Según Morán (2016) en su Investigación “Plan de Seguridad Informática en base a parámetros de la norma ISO/IEC 27002 para mejorar la Seguridad de la Información en el Departamento de Tecnologías de Información y Comunicación del Gobierno Autónomo Descentralizado Provincial De Santo Domingo de los Tsáchilas” realizado en Santo Domingo de los Tsáchilas - Ecuador, cuyo objetivo general fue implementar un Plan de Seguridad Informática en base a parámetros de la norma ISO/IEC 27002 para mejorar la Seguridad de la Información en el Departamento de Tecnologías de Información y Comunicación del Gobierno Autónomo Descentralizado Provincial De Santo Domingo de los Tsáchilas. La investigación le permitió concluir que si se cumple al 100% las reglas y las seguridades establecidas en este plan informático para el GAD Provincial, no se garantiza que no existan problemas e inconvenientes, ya que no existe la posibilidad que haya 0 errores en cualquier situación no solo en el ámbito informático, pero si es de ayuda para combatir los complicaciones que se pueden

venir en el futuro, asimismo se concluye que la tecnología cada día cambia, por esta razón el GAD Provincial, debe estar constantemente actualizada, en temas de tecnologías, telecomunicaciones y políticas de seguridad aplicando procedimientos y manuales para la estandarización de procesos, asimismo concluyó que las políticas de seguridad informática realizada para el caso de estudios, establece avances en cuanto a la gestión de la seguridad del departamento de tecnologías, ya que realiza una reducción de riesgos y vulnerabilidades.

Moran nos hace notar con su tesis que los conocimientos vertidos se involucran con la seguridad de la información, descripción útil en la tesis que he realizado. Nos hace resaltar que si se cumple al 100% las reglas y las seguridades establecidas en este plan informático para el GAD Provincial, no se garantiza que no existan problemas e inconvenientes en la seguridad de la información, pero si nos afirma que sería de ayuda para combatir las complicaciones de seguridad que se puedan venir en el futuro.

Nacional

Según Aguilar (2016) en su Investigación "Implementación de un modelo simplificado de firma digital basado en la tecnología PKI y la innovación por protocolos caso de estudio: Municipalidad de Miraflores" realizado en la Municipalidad de Miraflores – Lima, cuyo objetivo principal fue la de implementar un modelo simplificado de firma digital basado en tecnología PKI y la invocación por protocolos dentro de la Municipalidad de Miraflores. La investigación le permitió concluir que la implementación de un componente de firma digital web dentro de la municipalidad ha sido posible considerando la tecnología del 4identity, algoritmo de firma digital RSA, algoritmo de Hash SHA2 y el contenedor criptográfico tipo token iAM, asimismo se ha podido evitar cualquier tipo de independencia de tecnología Java, ActiveX, navegador web, que dificulta la integración y la accesibilidad a las aplicaciones web, y de esta manera asevera el autor se cumplió lo que denominó como objetivo secundario #1, asimismo explica el autor que lo anterior pudo realizarse mediante la integración en cualquier navegador haciendo uso de la invocación por protocolos de una aplicación nativa

y el uso de un token criptográfico, cumpliéndose de esta manera en su investigación el objetivo secundario #2 y #5 simultáneamente.

Aguilar desarrolla una tesis que se encuentra involucrada en el ámbito de la seguridad de la información y permite rescatar puntos de vista útiles para la tesis. Nos afirma que el tratamiento de un modelo simplificado de firma digital que tome como implementación base la tecnología PKI nos permite mejorar considerablemente la seguridad de la información al aumentar el grado de dificultad con la web en la forma de cómo acceder e integrarse a ella.

Según Llatas (2015) en su Tesis "El registro biométrico dactilar con el sistema AFIS y el control del delito" realizado en la Pontificia Universidad Católica del Perú que trabajó directamente con las dependencias judiciales y policiales, centrándose en la Oficina de la Escena del Crimen de la Dirección Ejecutiva de Criminalística de la PNP de donde se acopiaron los expedientes materia de la investigación, tuvo como objetivo realizar la implementación del sistema AFIS para el registro biométrico dactilar como un ejemplo de aplicación de tecnología avanzada para brindar un respaldo científico y tecnológico a las labores de investigación que lleva a cabo la Policía Nacional del Perú. Las conclusiones que se desprendieron de esta investigación apuntaron a las dificultades que se encuentran en la implementación del sistema AFIS para el registro biométrico dactilar. A pesar que se pueda considerar lo bastante fácil aparentemente su aplicación, no evitaron que se manifieste los problemas que se enmarcan dentro del enfoque 'top-down'. Si a lo anterior se aúna el hecho que el sistema AFIS policial enfrentó problemas radicales como la capacitación correcta tanto de los peritos como de la adecuada gestión de espacios, se pudo entender que sean los causantes de la desmotivación con que trabajan los peritos redundando en la efectividad de sus dictámenes periciales.

Llatas desarrolla una tesis circunscrita en el ámbito de la biometría y la seguridad de la información, temas bases de la investigación realizada. Nos manifiesta los niveles de dificultad que experimenta el registro biométrico dactilar cuando se implementa el sistema AFIS, a pesar de ser aparentemente sencilla

los problemas llegan a presentarse ante la falta de capacitación correcta de los peritos por ejemplo y el manejo de los espacios adecuados donde implementarse.

Según Rodrigo y Muñante (2015) en su Investigación “Sistema de Identificación y Clasificación de Inculpados” desarrollado en la Universidad de Ciencias Aplicadas en Lima-Perú, cuyo objetivo principal fue la de disminuir los actos de corrupción a través de un manejo optimizado de los procesos de administración penitenciaria en todo el territorio peruano, automatizando los mecanismos de identificación y clasificación de los inculpados en el INPE. La investigación le permitió concluir que la dificultad mayor que encuentra para la realización de su objetivo estriba en que se debe realizar, lo que no sucede con eficiencia en la actualidad, la retroalimentación de los usuarios finales para crear como una especie de base de medidas y rangos de calificación para que la evaluación sea más fiable y el producto se acerque más al estándar ISO/IEC 9126 al evaluar las características de calidad, logrando de esta manera que cualquier fallo que se pudiera presentar sea menos traumante y de menor costo.

Rodrigo y Muñante desarrollan una tesis que se encuentra involucrada en el ámbito de la seguridad de la información y permite rescatar puntos de vista útiles para la actual tesis realizada. Ellos manifiestan que el sistema de identificación y clasificación de inculpados tomando como referencia el estándar ISO/IEC 9126 permite detectar y corregir fallos a un menor costo e impacto.

Según Briceño (2012) en su Investigación “Diseño e Implementación de un Sistema de Reconocimiento de Palabras en un FPGA basado en el algoritmo de LPC” realizado en la Universidad Nacional de Ingeniería en Lima. Perú, cuyo objetivo general fue realizar el reconocimiento de palabras habladas por un locutor en particular, utilizando un sistema basado en un procesador configurable en dispositivo FPGA, realizando la comparación con patrones de voz guardados anteriormente en un dispositivo de almacenamiento. La investigación le permitió concluir que el sistema previamente entrenado con un hablante puede reconocer otros hablantes siempre y cuando pronuncien las palabras con la misma entonación (tonalidad de la voz y acentuación en la pronunciación). Esto se debió

a que el algoritmo de codificación de la voz LPC, usado en el proyecto, se usa también para caracterizar el tono de voz de los hablantes, asimismo el sistema desarrollado es transportable a FPGA's Altera de diferentes densidades que puedan contener el procesador Nios II usado en el proyecto. La portabilidad del sistema se puede dar con FPGA's de diferentes fabricantes, si todo el desarrollo se hubiera hecho usando un lenguaje de descripción de hardware estandarizado (VHDL o Verilog). Aunque el Nios II está elaborado en lenguaje de descripción de hardware, su arquitectura utilizó una definición de bajo nivel, que explota las características únicamente en FPGA's de Altera.

Briceño desarrolla una tesis que se encuentra involucrada en el ámbito de la biometría de voz basado en el algoritmo de LPC y permite rescatar puntos de vista útiles para la tesis que he realizado. Briceño nos precisa que el sistema previamente entrenado con un hablante puede reconocer otros hablantes siempre y cuando pronuncien las palabras con la misma entonación.

Según Loyola (2015) en su Investigación "La Espectrografía de Voces en el Peritaje de Identificación del Hablante" realizado en la Universidad de Huánuco. Perú mediante un estudio descriptivo y explicativo de tipo no experimental con una población de 30 profesionales encargados de delitos de corrupción de funcionarios, cuyo objetivo principal fue el demostrar que el uso de espectrogramas de las voces si influyen en la identificación positiva del locutor y por consiguiente mejoran la calidad y eficacia probatoria de los dictámenes e informes periciales. La investigación le permitió concluir que no todos los peritos manejan programas informáticos especiales, desconociendo además del uso de espectrogramas de las señales de voces en la identificación de los investigados por delitos de corrupción de funcionarios, asimismo se logró establecer que los policías en las pesquisas y Fiscales no verifican el perfil del perito convocado, además de no participar en la toma de muestras de voces a los denunciados o investigados por falta de conocimiento de esta nueva especialidad del crimen.

Loyola desarrolla una tesis que se encuentra involucrada en el ámbito de la biometría de voz y la seguridad de la información temas pilares en la tesis que he

realizado. Loyola nos evidencia que la espectrografía de voces mejora la calidad y eficacia probatoria de los dictámenes e informes periciales, lamentablemente no ejecutado en su totalidad ya que los policías y Fiscales en las pesquisas no toman muestras de voces a los investigados por falta de conocimiento del tema.

1.3. Teorías relacionadas al Tema

1.3.1. Teorías

Teoría General de Sistemas

Von Bertalanffy propone la necesidad de reorientar el conocimiento desde la física sub atómica hasta la historia, por el rumbo de una Teoría General de Sistemas y expone algunos de los hitos en este esfuerzo de reorientación (Ramírez, 1999, p.10).

Teoría de Control

El tema de investigación busca relacionar una herramienta tecnológica con un proceso al cual lo mejore, llevando implícito un control del primero sobre el segundo. Un control de acceso, nos lleva a interpretar una teoría de control, que se puede interpretar como un tipo de tecnología donde la misión del producto implantado es limitar el acceso a un sistema donde los recursos pueden ser físicos, o de un control virtual, como por ejemplo control de acceso de una red de comunicaciones, control de acceso a una página Web (Navarro, 2014, p.4).

1.3.2. Bases teóricas de la Biometría de Voz

Definición de la Biometría de Voz

Escajedo (2015) consideró que la Biometría vocal o Biometría de Voz:

> viene a ser una característica biométrica dinámica en virtud de que es necesario un intervalo de tiempo para poder realizarse su

> captura. La voz de una persona mantiene una serie de tonos distintivos a lo largo de toda su vida a pesar de los cambios que en ella experimenta como por ejemplo el estado de ánimo, el tipo de conversación o el cambio de edad (p.111).

Alvez et al. (2015) indicó que la biometría de voz:

> es una 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 de fase y amplitud variable como los micrófonos (p.56).

Según Poblete (2014) indicó que la Biometría de Voz viene a ser:

> un sistema de autentificación de la identidad de una persona basado en características biométricas como la voz, el iris o la huella digital, se considera más seguro y más personal, que otro sistema que se base en *password* o bien, en tarjeta magnética. Esto se debe al hecho que tales características biométricas pertenecen a la propia persona y ellas no se pueden olvidar o extraviar, lo cual sí puede suceder con los otros métodos. Además, la voz, opuesta a las anteriores características biométricas, permite que el reconocimiento se realice en forma remota, siendo también, fácil de transmitir a través de un canal de comunicación tal como un canal telefónico. En los últimos años, las tecnologías de voz, se han integrado como interfaz de comunicación entre las personas y las máquinas, en diversas aplicaciones, por ejemplo, en sistema de telecomunicaciones, robótica y multimedia. Esto permite que las tecnologías de voz evolucionen, en velocidad de funcionamiento, confiabilidad y eficiencia, junto con la propia evolución de las otras tecnologías de telecomunicaciones y multimedia (p.1).

Según Masana de Bouffard (2016) indicó que la Biometría de Voz es:

> el método más adecuado para realizar pagos de forma segura por vía telefónica. Ya que, no hay dos individuos que suenen idénticamente igual porque la forma del tracto vocal, el tamaño de la laringe y los otros órganos son los que permiten que la producción de la voz sea diferente. A parte de estas diferencias físicas, cada locutor tiene características distintas en la forma de hablar, incluyendo el acento, el ritmo, la entonación, por ejemplo. Características útiles para la verificación de locutor (p.8).

Dimensiones de la Biometría de Voz

Las dimensiones de la Biometría de Voz que mejor se ajustan a este proyecto de investigación son: Reconocimiento, Verificación e Identificación, donde;

Reconocimiento

Según Alvez et al. (2015) definió reconocimiento como: "un término genérico y no necesariamente quiere decir verificación o identificación. Todos los sistemas biométricos realizan un reconocimiento para volver a conocer a una persona que ya ha sido enrolada previamente" (p.51).

Según Sánchez (2012) reconocimiento es: averiguar "¿quién es?, comparando la información dejada por la variedad de usuarios del sistema en forma de patrones almacenables con la muestra que se desea averiguar" (p.8).

Para Rueda (2011) reconocimiento:

> viene a ser una forma de conversión de la señal de voz en su característica de segmentos consecutivos hacia una secuencia en el tiempo de una serie de vectores de parámetros, cumpliéndose en la totalidad de sistemas de reconocimiento automático del habla (p.17).

Verificación

Para el caso de Verificación Alvez et al. (2015) conceptúo: “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” (p. 51).

Escajedo (2015) indicó que la Verificación: “con frecuencia se da a entender que la verificación biométrica nos permite saber “que un individuo es quien dice ser”” (p.129).

Cerame (2014) indicó que verificación es:

> el resultado de la comparación entre la identificación suministrada junto con el rasgo biométrico por alguna persona que asevera tener cierta identidad. Realizándose para ello una deliberación para tratar de demostrar a manera de puntuación lo que el usuario afirma poseer, donde el sistema a partir de un determinado valor dará crédito o no a lo expresado por el usuario (p.8).

Identificación

Para el caso de Identificación Alvez et al. (2015) lo conceptúo así: “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” (p. 51).

Según Escajedo (2015) el proceso de determinar la identidad de una persona o identificación lo conceptúo como:

> un segundo tipo de servicio de reconocimiento mediante Biometría es el de determinación de la identidad de las personas en sentido estricto. Estos sistemas, con base a la información almacenada, tratan de determinar quién es una persona. Captada su información

> biométrica, ésta se compara con los patrones de todas las personas que fueron enroladas en búsquedas de coincidencias (1 a n) (p.131).

Cerame (2014) indicó que identificación es;

> un manejo de la base de datos tratando de buscar el rasgo biométrico proporcionado por un usuario dentro de la totalidad de modelos almacenados de tal forma que permita dar como resultado de dicha búsqueda una identificación o rechazo de lo que el usuario ha suministrado (p.131).

Evolución de la Biometría

Existe un consenso en considerar que los primeros estudios sobre Biometría, se comenzaron a realizar a finales del siglo XIX, sin saber claro está que se estaba considerando a la Biometría como tal, como lo indicó Aguirrezabala (2015).

> Alphonse Bertillon desarrolló con el objeto de identificar criminales a través de, hasta donde se tenga conocimiento, los primeros estudios antropométricos realizados. Empleando para ello un método que lo concebía como un sistema de caracterización de individuos, concretando de esta manera en 1880 el primer estudio Biométrico realizado (p.1).

Así mismo Aquirrezabala (2015) indicó que este método;

> que basaba su seguridad y sus bajas tazas de error en la forma de escoger convenientemente la característica a verificar así como el nivel que se tomaba como aceptación del proceso de verificación. Consistía en la formación de unas plantillas de datos, las cuales eran manejadas de diversas maneras según era el rasgo característico que se estaba investigando obteniéndose así una variedad de tipos de características del individuo. En esa época se consideraba que para llevar a cabo este proceso era necesario que el sistema conociese previamente al usuario a verificar o identificar.

> La modernidad en la actualidad prácticamente ha sustituido el reconocimiento por huella dactilar por otros métodos de reconocimiento biométricos que conllevan mayor seguridad en sus resultados así como una mayor comodidad para el usuario al que se le va a aplicar el reconocimiento biométrico.
>
> Tampoco hay que olvidar que hace muy pocos años recién han surgido las alternativas de reconocimiento biométrico, constituyéndose prácticamente durante muchos años como el único método de reconocimiento biométrico al que usaba la huella dactilar (p.2).

La línea de tiempo que se muestra a continuación nos da un alcance del desarrollo en el tiempo de la biometría, en ella podemos notar que la geometría de la mano se constituyó como sistema de reconocimiento biométrico a inicios de 1974.

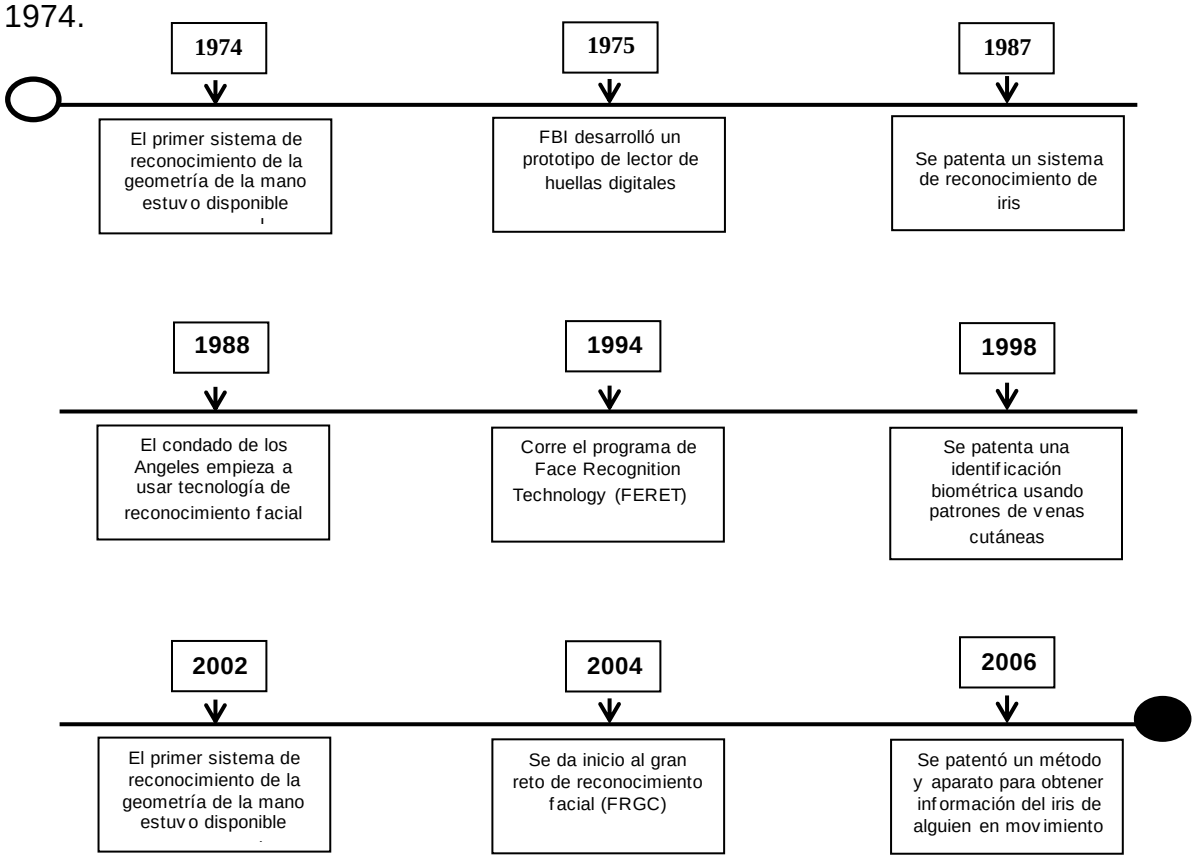


Figura 1. Línea de tiempo de la historia de la biometría

El reconocimiento facial comienza a implementarse en el condado de los Ángeles en 1988 para posteriormente en el año 2004 dar inicio al gran reto de reconocimiento facial (FRGC).

Otra fecha sumamente representativa en la línea de tiempo es 1975, cuando el FBI desarrolla un prototipo de lector de huellas digitales.

Funcionamiento de un Sistema Biométrico

Si bien es cierto la Biometría de Voz es nuestra herramienta tecnológica en el presente proyecto de investigación, dicho sistema biométrico sigue los lineamientos de funcionamiento de un sistema biométrico general, el cual consiste en tomar como punto de inicio un rasgo biométrico de una determinada persona y culmina como una muestra asignable de una identidad individual en base al reconocimiento de patrones. Tal como nos lo indica Cerame (2014).

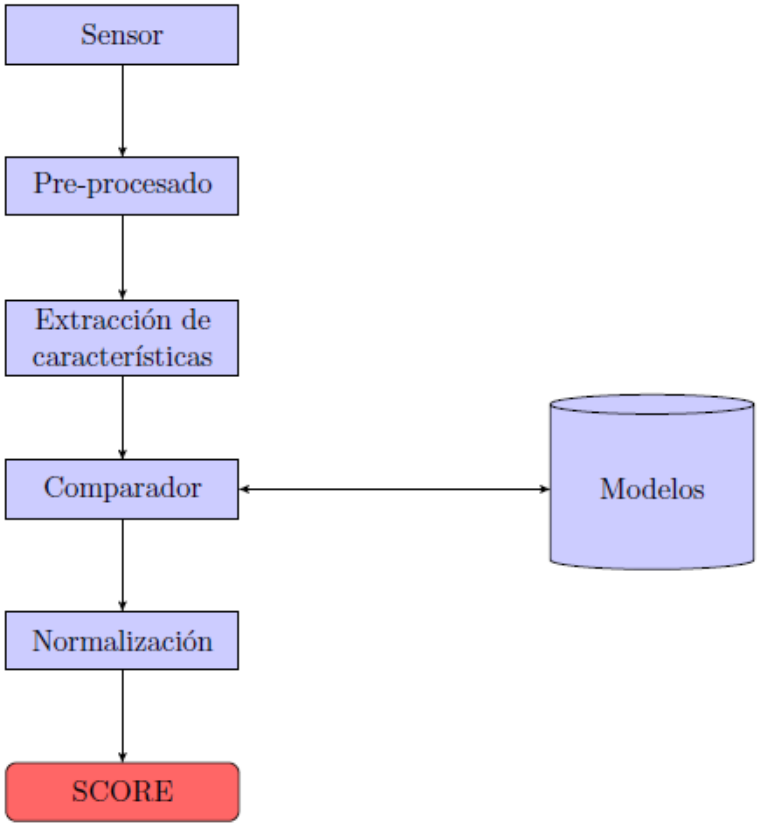


Figura 2. Diagrama del funcionamiento de un sistema biométrico
Tomado de Cerame, 2014, p.7.

Así mismo Cerame (2014), nos hace notar que existen dos formas diferentes en que opera un sistema biométrico:

El procedimiento de verificación o detección donde la persona dice tener una identidad. Es donde el sistema trata de demostrar que la identidad que dice es realmente suya.

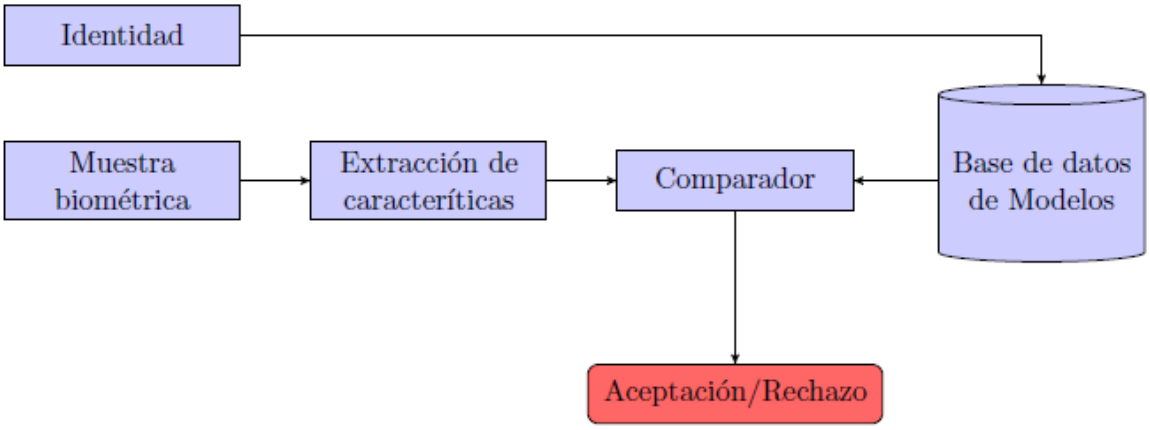


Figura 3. Diagrama del Procedimiento de Verificación de un Sistema Biométrico General.
Tomado de Cerame, 2014, p.8.

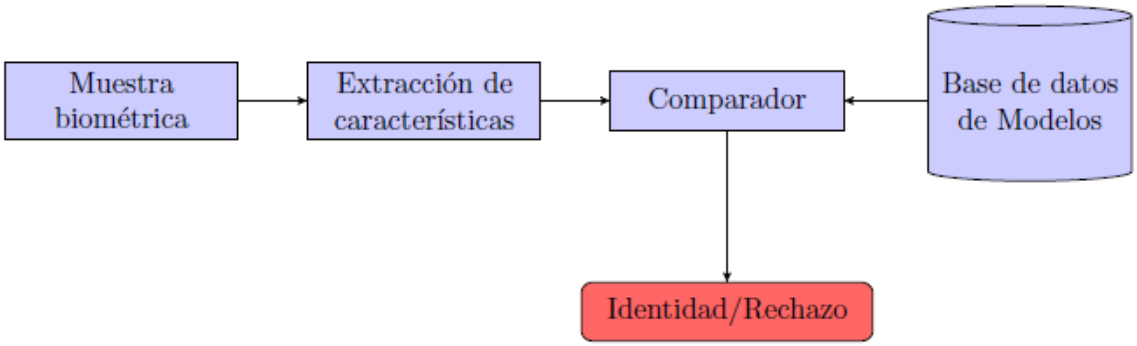


Figura 4. Diagrama del Procedimiento de Identificación de un Sistema Biométrico General.
Tomado de Cerame, 2014, p.9.

El procedimiento de identificación, es aquel que haciendo uso de una muestra biométrica proporcionada por la persona le permite establecer si ella, que debe estar incluida en una base de datos previamente almacenada o enrolada, cumple con el procedimiento de identificación o no se encuentra en la base de datos, llamándose para este caso: rechazo (pp.7-9)

Condiciones mínimas para el establecimiento de un Patrón Biométrico

No existen dos cuerpos humanos iguales. Esta aseveración nos puede conducir a conclusiones erradas en Biometría, concretamente en el tema de rasgos biométricos. Si considerásemos que al no ser los dos cuerpos mencionados anteriormente iguales, por lo tanto sus partes cualesquiera que sean de igual forma no pueden ser iguales y por consiguiente al no ser iguales pueden constituir *Rasgos Biométricos* que permitan realizar *una comparación de ellos.* Sin embargo esta conclusión resultaría errada, porque no es suficiente encontrar al azar cualquier parte de un cuerpo humano a comparar, sino que la parte escogida debe reunir ciertas características que le permita al realizar un reconocimiento biométrico poder obtener un resultado científicamente viable. Tal como nos lo describió Alvez et al. (2015);

> 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. Un proyecto debe considerar al seleccionar el patrón biométrico, que el mismo debe responder mínimamente a las siguientes características:
>
> *1. Universalidad:* Todo individuo debe poseerla.
> *2. Distinción:* Debe ser exclusivo para cada persona y diferente al momento de efectuar una comparación con algún otro individuo. Una persona sólo puede registrarse si posee el rasgo biométrico necesario.

3. Permanencia: No debe cambiar con el transcurrir en el tiempo. La característica biométrica debe permanecer la mayor cantidad de tiempo sin alteración alguna.

4. Registración: Debe ser sujeto a poder efectuársele una medición, 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:

5. 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.

6. Fiabilidad: También conocido como rendimiento o nivel de exactitud. La fiabilidad de un sistema viene a ser la probabilidad de que ese sistema funcione o desarrolle una cierta función, bajo condiciones fijadas y durante un período de tiempo determinado. Esta característica, nos hace ver la precisión del reconocimiento, los recursos requeridos y el entorno operativo.

7. 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.

8. Resistencia a ataques: Expresa la forma anticipada de preparar un sistema biométrico, analizando sus puntos vulnerables y fortaleciéndolos para evitar un riesgo de violación al sistema.

9. Aceptabilidad: Corresponde a la parte higiénica y el grado de aceptación cultural para la mayoría de las personas, desde el punto de vista de perjuicio que pudiera causarles.

10. Costo aceptable: El costo que demanda para el individuo que se acerca a que le realicen una identificación biométrica no debe ser de tal magnitud que le permita argumentar que no puede realizar dicha medición biométrica por casualmente tener un costo elevado.

De igual forma los costos que signifiquen el mantenimiento y administración de datos de ben ser lo suficientemente coherente para llevarse a cabo, para que de esta manera se tengan unas plantillas biométricas de respaldo. Generalmente la elevación de costos se evidencian cuando se evalúan por separado los costos que representan el software y hardware de cualquier sistema biométrico.

11. No intrusiva: Se refiere al hecho de que la información biométrica obtenida no suponga una molestia del individuo en cuestión, en la medida que para efectuar dicha medición se tenga que tener un contacto físico no deseado por el usuario.
12. 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 (pp. 52-53).

Tipos de Biometría

La clasificación se obtiene partiendo de una premisa aceptada por el consenso mundial, en el cual se afirma que el humano tiene dos rasgos que pueden ser medibles: sus rasgos físicos y sus rasgos de comportamiento. Bajo este criterio, puntualmente se acepta que existen dos tipos de Biometría;

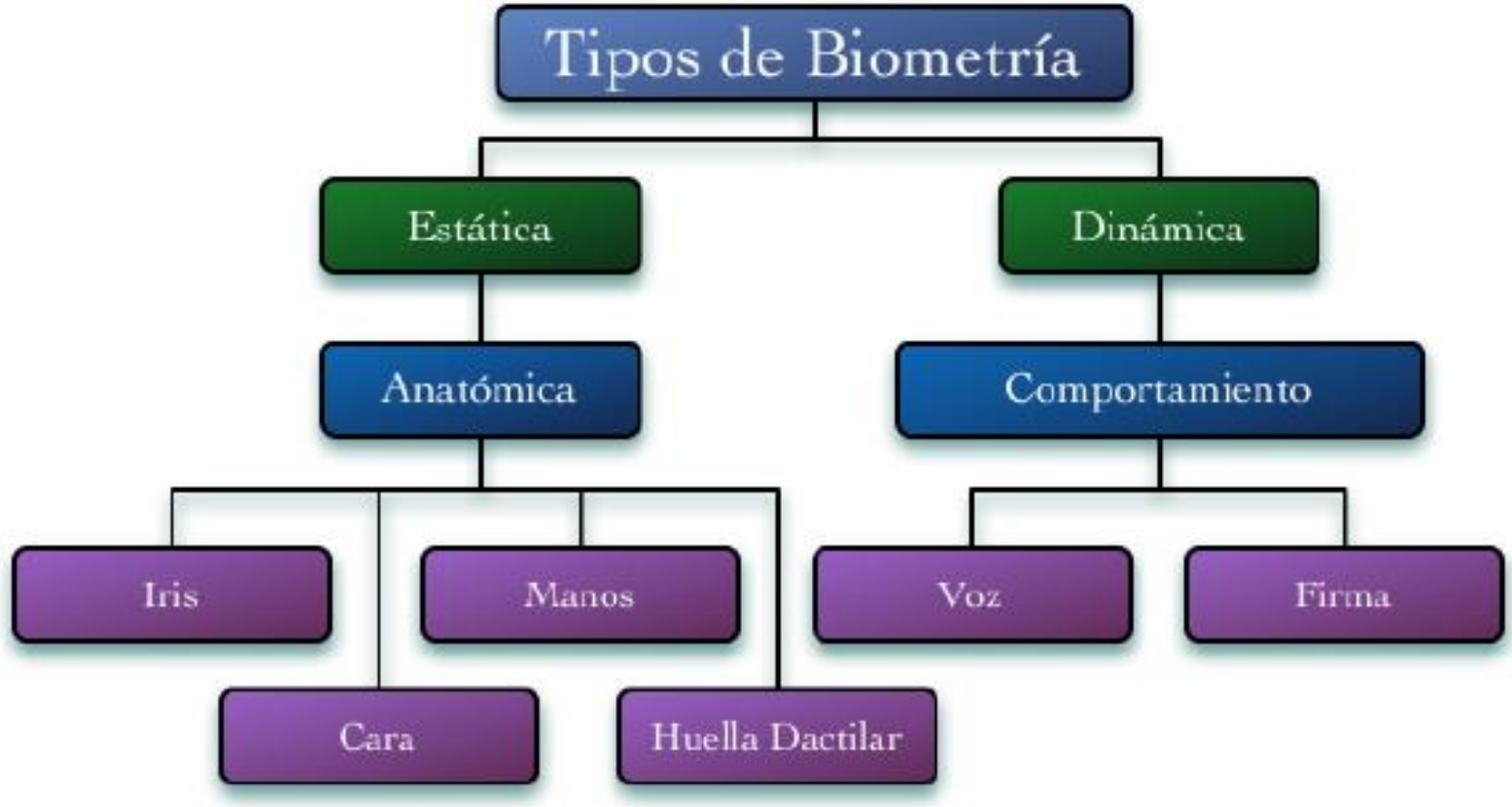


Figura 5. Tipos de Biometría
Tomado de Aguirrezabala, 2015, p.3.

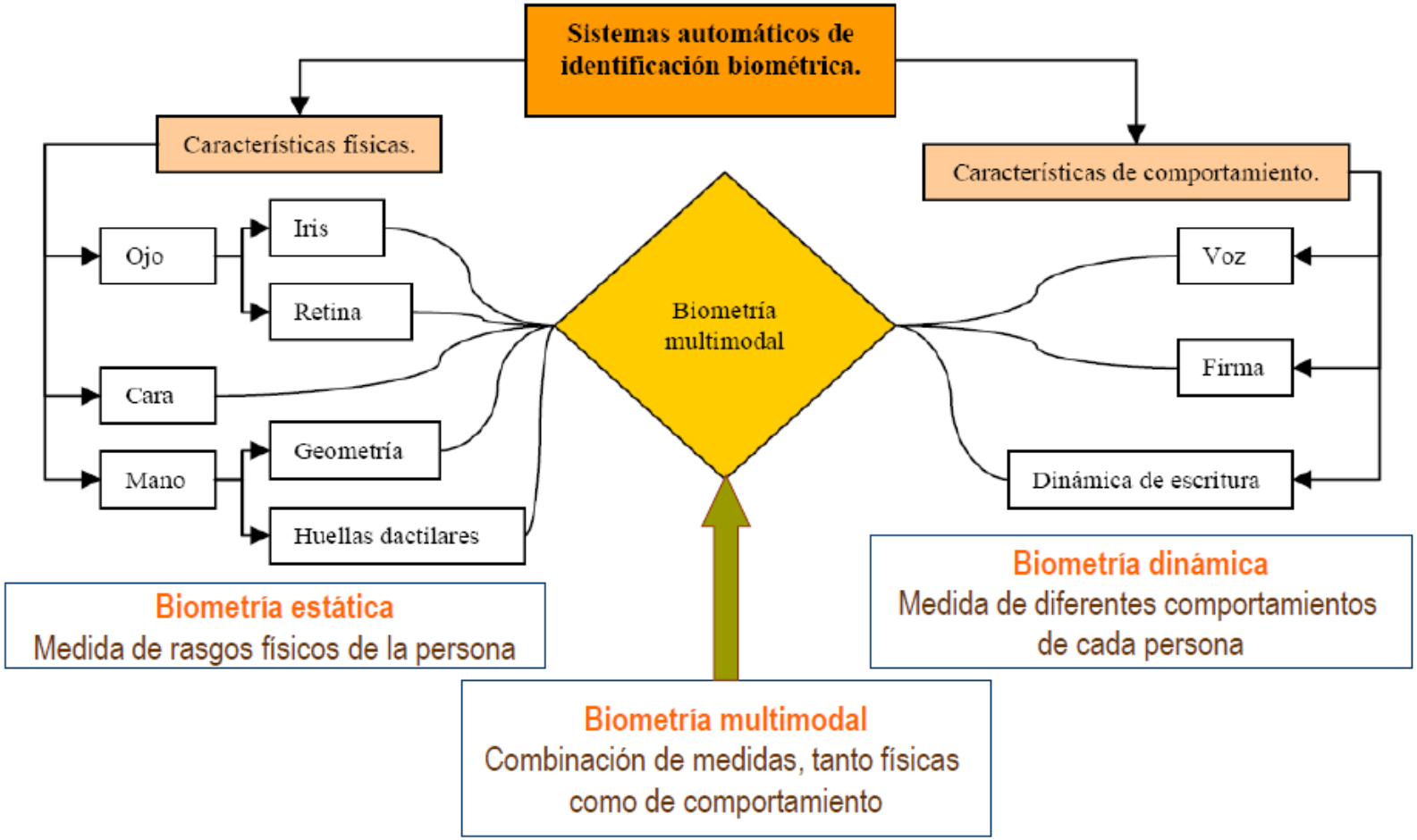


Figura 6. Tipos de Biometría donde se incluye la opción de Biometría multimodal Tomado de Sánchez, 2012, p.5.

> una en donde el estudio del rasgo biométrico es una característica que posee el individuo que se circunscribe a un rasgo anatómico y exclusivo de esa persona, en este caso se está hablando de Biometría Estática. En cambio cuando la característica biométrica va por una manifestación de movimientos corporales que cumplen con ser exclusivos de la persona en cuestión y que permiten ser medibles, se está entonces hablando de Biometría Dinámica, que es donde se circunscribe la Biometría de Voz (Aguirrezabala, 2015, p.3).

Según Escajedo (2015) los Tipos de Biometría más frecuentemente usados, son los siguientes:

> *Tipo 1. Biometría Facial:* Existe un consenso en afirmarse que es el rostro la parte del cuerpo humano que aloja la mayor cantidad de rasgos que permite reconocer a una persona. Así mismo la cabeza es la estructura más compleja en todos los animales pues ella contiene el sistema nervioso central, los ojos y las estructuras auditivas internas. Además contiene las vías de acceso de los sistemas digestivo y respiratorio. Por otro lado la coloración que tiene los ojos que pudiera modificarse en los primeros meses de vida mantiene un color que depende en gran medida de la

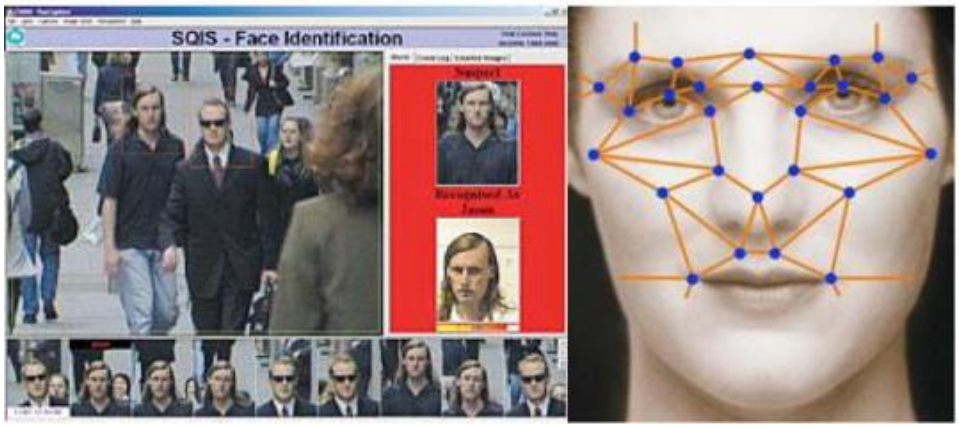


Figura 7. Reconocimiento Facial
Tomado de Sánchez, 2012, p.4.

cantidad de melanina que se posea la persona. Así mismo el rostro juega un importante papel en la comunicación e interacción con los demás, como también en la transmisión de la identidad y de la emoción. Por este motivo resulta sumamente interesante estudiar, la habilidad que posee el cerebro humano para procesar los rostros desde muy temprana edad, lo cual es ampliamente atractivo para los científicos y los filósofos.

Tipo 2. Biometría de Iris: Viene a ser el equivalente del diafragma de una cámara fotográfica. Al ser el iris un órgano interno es protegido por la córnea que es una membrana sumamente sensible y transparente. El iris le da la coloración a los ojos. Los músculos del iris controlan la dilatación de la pupila que comunica la cámara anterior y posterior del ojo. Los recién nacidos presentan una coloración en los ojos azul grisáceo que pudiera modificarse en los primeros meses de vida, mantiene sin embargo un color que depende en gran medida de la cantidad de melanina que se posea la persona Si existiera poca cantidad de este elemento los ojos mantendrían esa coloración. Por otro lado el análisis de la textura del iris es sumamente

Figura 8. Escáner de iris
Tomado de Navarro, 2014, p.46.

Importante para la identificación de una persona, ya que tiene un carácter permanente e inalterable en cada individuo. Además proporciona un patrón de medición al suministrar más de 250 puntos diferenciables y digitalizables. Y algo muy importante a considerar que es el hecho de que resulta sumamente peligroso, hasta el punto de perder la visión, si se pretende alterar este patrón que es característico para cada persona. Por esta razón se puede afirmar que es prácticamente imposible encontrar a dos personas que tengan la misma estructura geométrica del iris.

Tipo 3. Biometría de las Manos:

El patrón de medición está constituido por las características de las manos, es decir el registro de su altura, anchura y longitud como también la información que proporciona los dedos en cuanto se refiere a los nudillos, los distintos puntos de articulación. Todo esto en conjunto constituye el patrón del cual se realiza el proceso de comparación no de cada uno de las características mencionadas sino del conjunto de ellas, por esta razón se acostumbra a mencionar frecuentemente a este tipo de reconocimiento biométrico como geometría manual (pp.86-94).

Figura 9. Reconocimiento por geometría de la mano
Tomado de Navarro, 2014, p.50.

Figura 41.

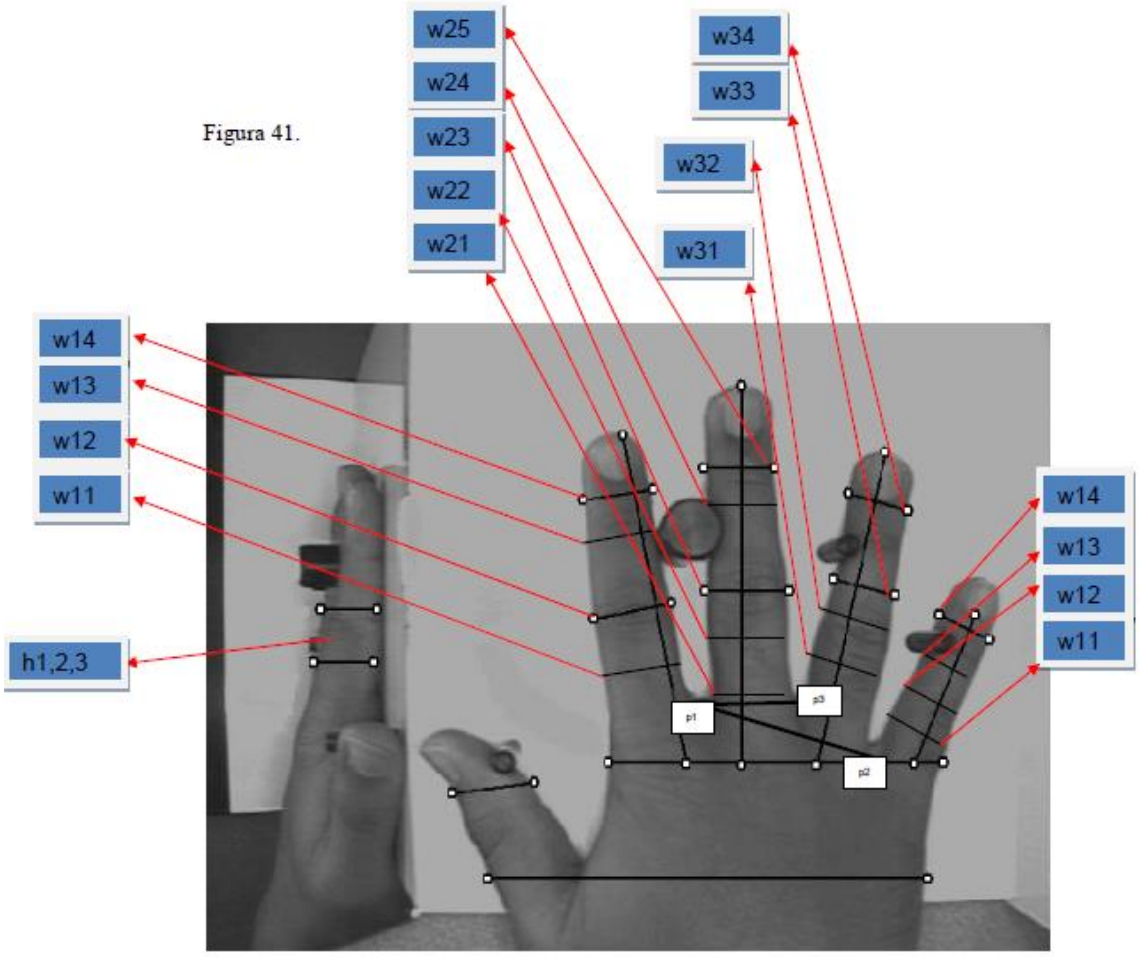


Figura 10. Detalle reconocimiento geometría de la mano.
Tomado de Navarro, 2014, p.52.

Además de los tipos mencionados se encuentran estos otros que nos lo menciona Navarro (2014);

Tipo 4. Biometría de Retina:

Para este tipo de reconocimiento se utiliza un escáner que mide el patrón de venas en el fondo del ojo proyectando una luz infrarroja a través de la pupila.

Tipo 5. Biometría por Huella Dactilar:

La huella dactilar tiene una característica única que la distingue de cualquier otro ser humano, siendo la ciencia que estudia dicho

fenómeno la Dactiloscopia (que viene de las palabras griegas *daktilos*, dedos, y *skopein*, examen).

Inmutabilidad: Las huellas dactilares no sufren cambio alguno en sus características a lo largo de la vida de un ser humano ya sea por desarrollo físico ni por enfermedades, cómo curiosidad aun sufriendo quemaduras en las huellas dactilares, éstas se regeneran en unos 15 días.

Figura 11. Escáner de retina
Tomado de Navarro, 2014, p.45.

Diversidad Infinita: Las huellas dactilares son únicas e irrepetibles, incluso con gemelos idénticos, esto es debido a que el proceso genético de creación de las huellas dactilares en los seres humanos es un proceso aleatorio y por lo tanto no existen ningún tipo de correlación.

A parte de estos aspectos hay que tener en cuenta que hay algunos aspectos relativos a la huella dactilar que hay que tener en cuenta a la hora de analizar una muestra y son características

implícitas de la huella dactilar y se conocen cómo rugosidades (pp.36-45).

Figura 12. Dactilograma natural – sobre la yema del dedo
Tomado de Navarro, 2014, p.39.

Figura 13. Dactilograma artificial - latente con reactivo
Tomado de Navarro, 2014, p.40.

Finalmente además de los tipos mencionados se encuentra el que nos mencionó Aguirrezabala (2015);

> *Tipo 6. Biometría de Voz:*
> Hay que tener presente que son varios los parámetros a considerar para ajustar convenientemente un tipo de software que pudiera evaluar lo más acertadamente posible la biometría de voz. Los elementos no deseados como enfermedades del individuo, estado de ánimo, edad, ruidos de fondo pueden darnos valores inexactos de medición que junto con las características básicas de la voz como el pitch, el tono, el ritmo del habla, podrían generar una irregularidad a la hora de tratar de medir o evaluar biométricamente a una persona usando su voz
>
> La Biometría de Voz se clasifica en dos tipos:
>
> 1.- Dependiente de texto.
>
> 2.- Independiente del texto.
>
> Cuando se usa determinados comandos o palabras aisladas para activar o seleccionar algún tipo de dispositivo o habilitar alguna función determinada, como por ejemplo la apertura de una chapa eléctrica o el reemplazo del teclado Dual Tone Multiple Frequency, se está refiriendo al tipo uno, Dependiente del Texto. Su implementación al igual que el segundo tipo supone una comparación con una información previa, acá sin embargo no se persigue saber quién lo dice sino más bien si coincide lo que se dice, con lo que se encuentra almacenado como base de datos.
>
> Cuando se usa el lenguaje natural o uno circunscrito a determinadas formaciones de gramática se está hablando del tipo Independiente del Texto.
>
> Existe además la forma biométrica de voz que permite evitar el memorizar claves o seguros de texto, ya que supondría que la propia voz sería el elemento cerrojo que pudiera aperturar o cerrar algún mecanismo. Para este caso la biometría adopta el nombre de Biometría independiente del texto (p.4).

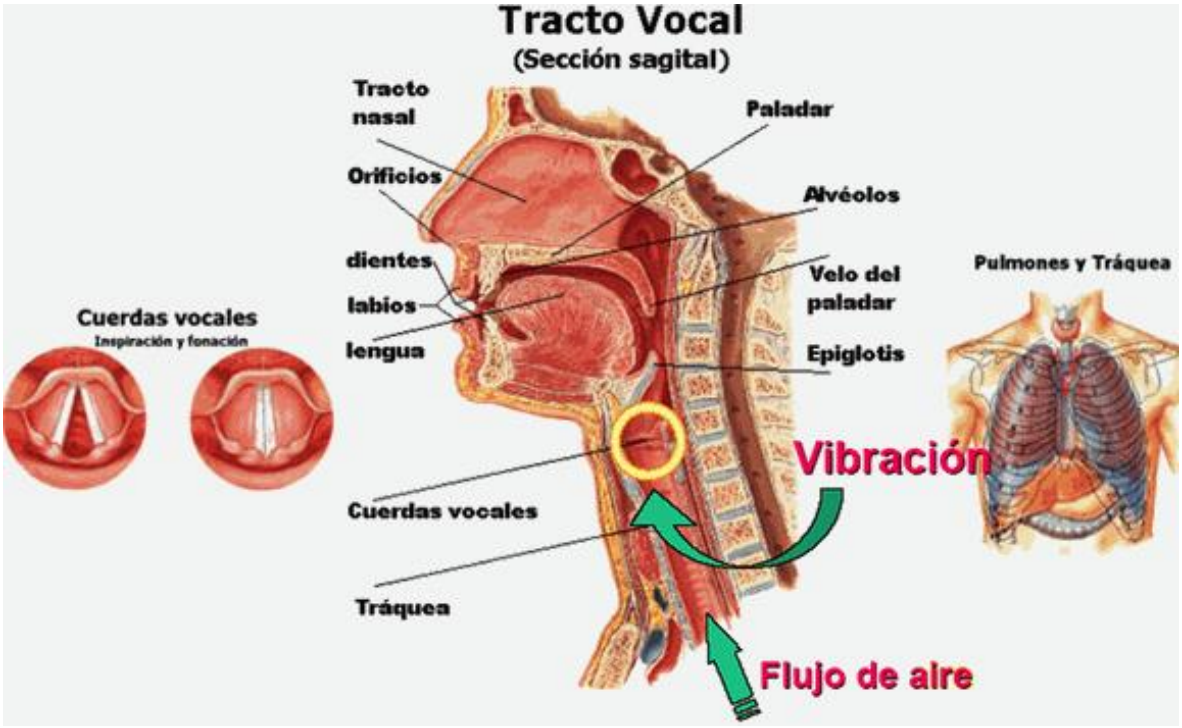


Figura 14. Partes que forman el aparato fonador.
Tomado de Aguirrezabala, 2015, p.34.

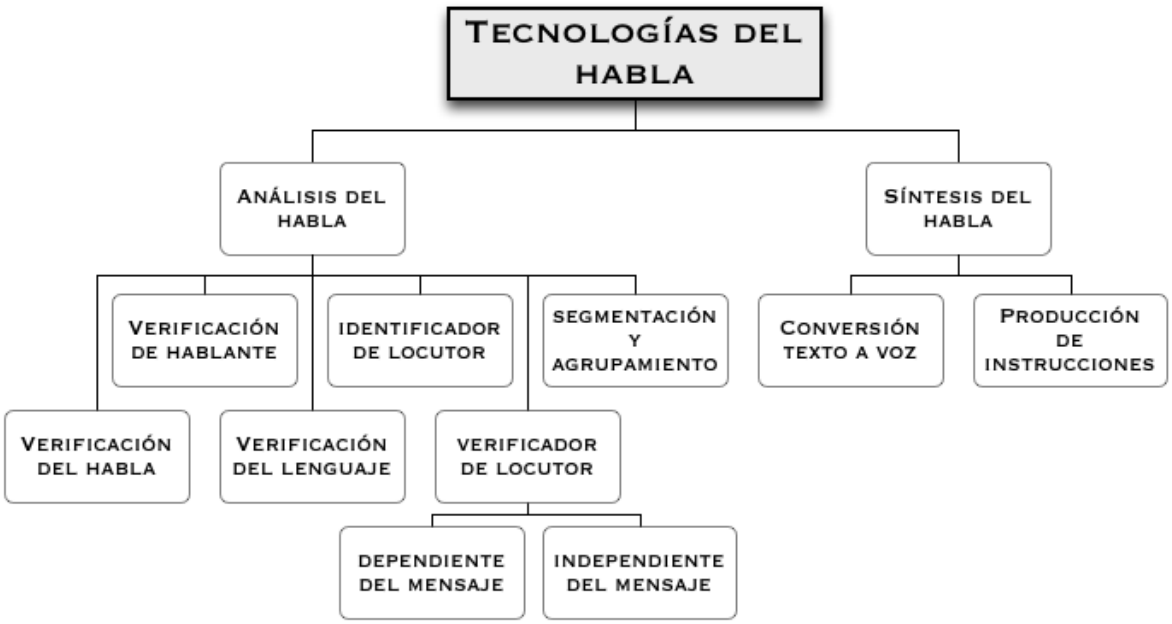


Figura 15. Tecnologías del habla relacionas con la Biometría
Tomado de Aguirrezabala, 2015, p.22.

Características de la Biometría de Voz

Las características más saltantes como indicó Aguirrezabala (2015) son:

Costo bastante reducido.

De aceptación generalizada y de fácil usabilidad.

De una concepción sin artificialidad, ya que cuando nos llaman por teléfono lo primero que se nos ocurre es reconocer a nuestro interlocutor.

El teléfono fijo o celular permite hacer simple y fácil la captura y transmisión de la voz.

Permite que la identificación se pueda realizar sin la presencia en el mismo lugar de la persona. No habiendo otra biometría que tenga esta característica.

Ocupan poco espacio en el almacenaje en tarjetas SD, teléfonos, FPGAs, y otros medios similares.

Al no necesitarse usar las manos ni la vista, permite que la identificación biométrica se centre solo en la interfaz vocal, liberando al usuario para que pueda realizar simultáneamente otras actividades junto con el reconocimiento biométrico.

Por otro lado hay que reconocer la existencia de inconvenientes y dificultades que generan en algunos casos el hecho de que no sea aconsejable su uso, así tenemos:

No ostenta la etiqueta de ser la biometría de mayor seguridad.

El cambio que se suscita en la voz humana por efecto de la edad, enfermedad o estados de ánimo.

Spoofing.

Está condicionado a los cambios que pudieran presentarse en los elementos conductores de la voz, como el micrófono, el propio canal de transmisión y su relación con el ruido.

Información no deseada como ruido de fondo.

La posibilidad que exista un reconocimiento inadecuado cuando la persona a identificarse con esta biometría se encuentre tan distante del punto de evaluación.

Inconvenientes que se presentan al hablar por parte del usuario:

Hay que tener claro que es imperativo tener una muy buena referencia de modelo de voz, la cual debe ser clara y limpia.

Si uno analiza bien este tipo de Biometría de Voz puede darse cuenta que presenta un mayor grado de comodidad para el usuario que otros tipos de biometría, la captura de los patrones biométricos por ejemplo le demanda menos molestia al usuario, ya que la captura del patrón biométrico se realiza por la grabación de la señal de voz. Sin embargo de igual forma que fácilmente se captura información con este tipo de biometría, esa captura de patrón biométrico por señal fácilmente puede ser alterada consciente o inconscientemente al efectivizarse el ruido de fondo por ejemplo o una modificación del tono de voz del usuario. De allí que el porcentaje de acierto no permita todavía tener un rendimiento del 100% y actualmente se ubique entre el 60 y 99.9% de acierto (Aguirrezabala, 2015, p.4-6).

Cifras o Estadísticas de la Biometría

Bajo la perspectiva distributiva de la tecnología biométrica en el mercado mundial actual, se tiene el esquema mostrado en la figura 16

Si considerásemos la Seguridad de la Información en función de las Tasas de error producidas por el uso de la Biometría unimodal, se tendría;

	FRR	FAR
Huella	2%	0,1%
Iris	0,03%	0,001%
Cara	0,5%	0,001%
Mano	3%	3%
Voz	10-20%	2-5%

Figura 16. Tasas de error en Biometría unimodal
Tomado de Sánchez, 2012, p.74.

Sobre el mismo tema Sánchez (2012) indicó:

> en el cuadro anterior se puede explicar en base a una determinada población de usuarios, por ejemplo; si se tuviera un lugar con 200.000 usuarios diarios, se distribuiría así: bajo el concepto de erróneamente rechazados: 4.000 usuarios si hacen uso de la identificación con la huella, 60 si lo hacen con el iris, 1.000 con la cara, 6.000 con la mano y 30.000 (aprox.) si hacen uso sólo de la voz.
>
> Bajo el concepto de erróneamente aceptados: 200 si lo hacen con la huella, dos iris, dos cara, 6.000 mano y 7000 (aprox.) si hacen uso sólo de la voz (p.74).

Por otro lado si analizáramos el rendimiento de los sistemas biométricos y considerásemos los siguientes parámetros involucrados, como nos lo indica Sánchez (2012), donde la Tasa de falsos positivos TFP, también llamado False Match Rate FMR viene a ser la proporción de muestras falsamente asignadas a un usuario al que no le pertenecen. Y la Tasa de falsos negativos TFN, también llamado False Non Match Rate FNMR viene a ser la proporción de muestras falsamente rechazadas como pertenecientes al cliente al que pertenecen (p. 13).

Además, Sánchez (2012) refiriéndose a las Curvas de rendimiento dijo:

> que la Curva ROC (Receiver Operating Characteristics), nos permite mostrar la variación de la TFP y la tasa de verdaderos positivos (1-TFN) con respecto a un determinado umbral. Y la Curva DET (Detection Error Tradeoff), muestra el número de desviaciones normales en la distribución normal estándar correspondiente a las probabilidades de falsos positivos o falsos negativos (p.15).

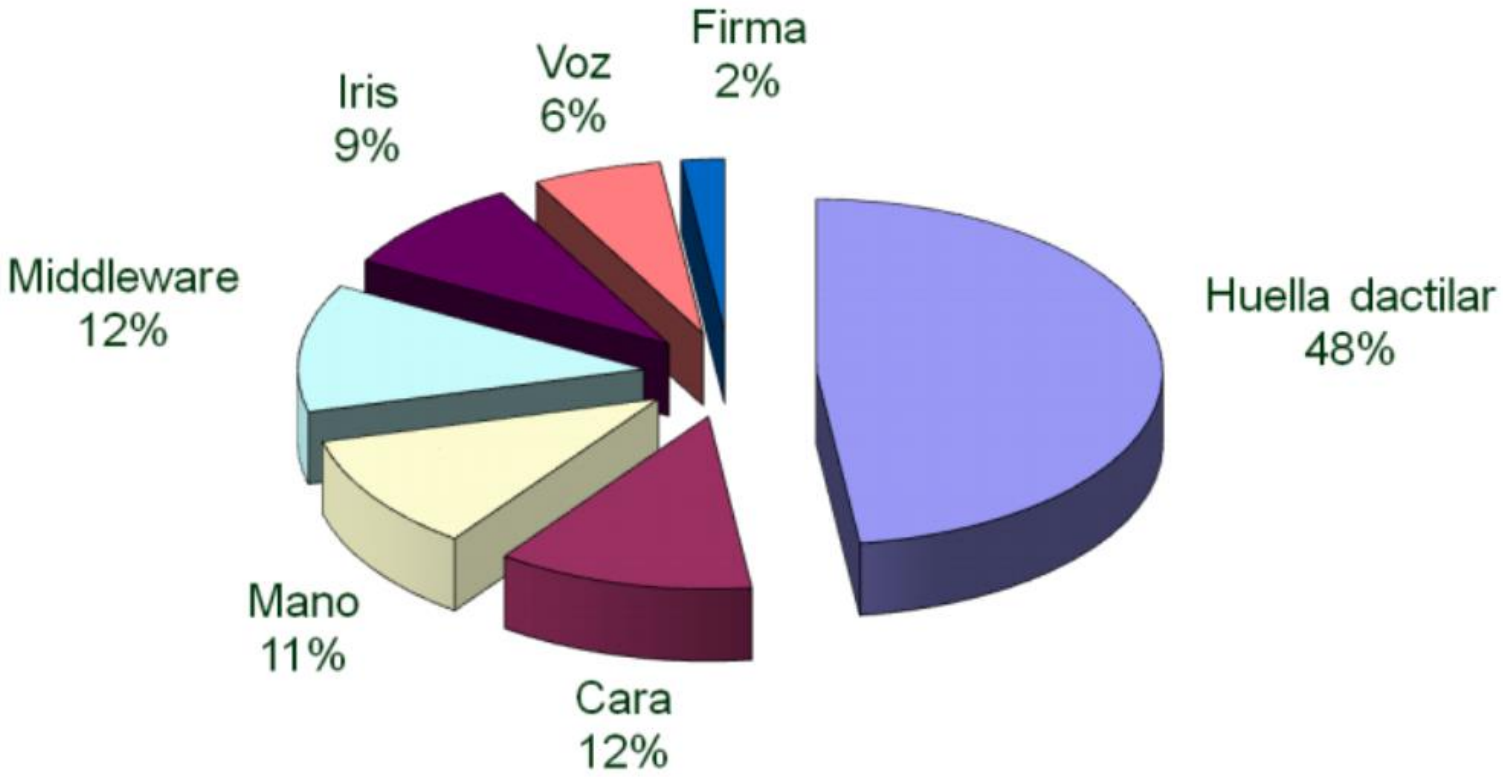


Figura 17. Cuota de mercado en tecnología biométrica
Tomado de Aguirrezabala, 2015, p.10.

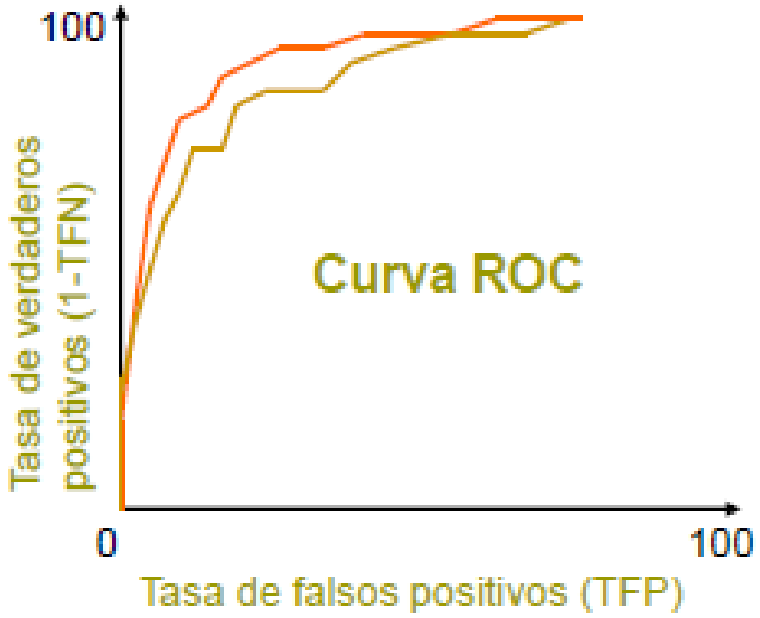


Figura 18. Curva ROC en Biometría
Tomado de Sánchez, 2012, p.15.

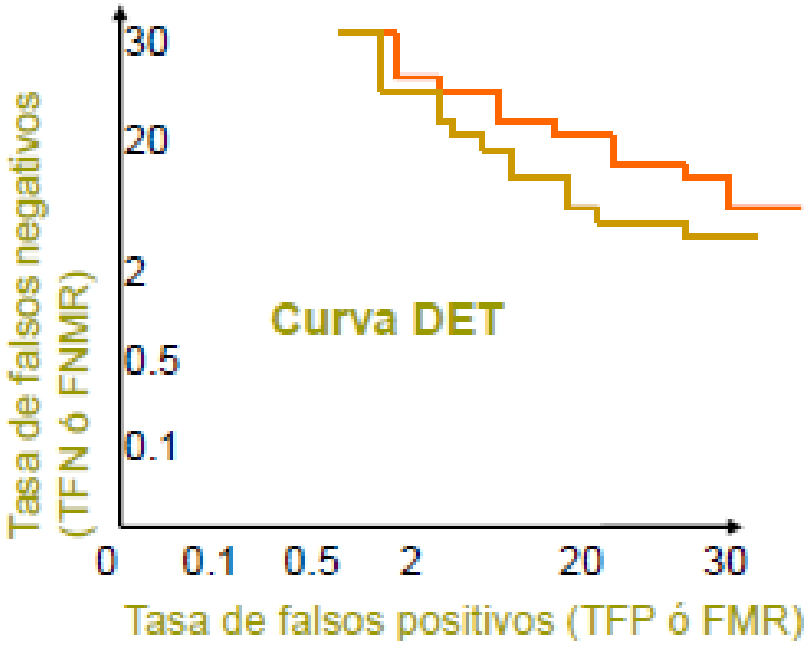


Figura 19. Curva DET en Biometría
Tomado de Sánchez, 2012, p.15.

En base a lo anteriormente explicado se tiene la siguiente estadística en biometría:

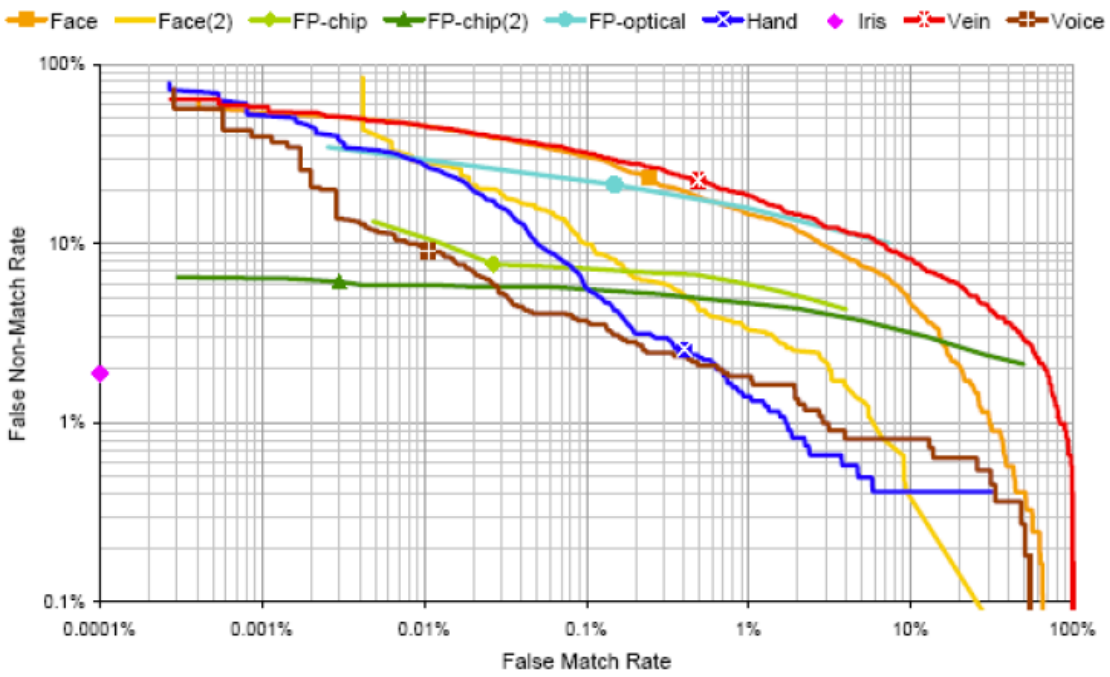


Figura 20. Curva DET para los diversos Tipos de Biometría
Tomado de Sánchez, 2012, p.16.

Nótese que las coloraciones de la figura 20 muestran los tipos de biometría considerados. Así tenemos que en rojo tenemos Biometría de Venas, en marrón Biometría de Voz, en violeta Biometría de Iris, en azul Biometría de Manos, en marrón Biometría de la Cara, etc.

Si considerásemos ahora que la Tasa de Falsa Aceptación (FAR) es la proporción de veces que se acepta a un falso sujeto como usuario del sistema y que la Tasa de Falso rechazo (FRR) es la proporción de veces que se rechaza a un auténtico sujeto del sistema, se tendrá entonces que la Tasa de Igual Error se obtiene cuando:

$$FAR = FRR \qquad \text{(Sánchez, 2012, p. 13)}$$

En base a la información que nos proporciona Sánchez (2012) se puede realizar un cuadro comparativo estadístico que relaciona los Tipos de Biometría.

Característica	*Nivel de Seguridad*	*Facilidad de uso*	*Costo*
ADN	Alto	Baja	Alto
Dinámica de Escritura	Medio	Alta	Bajo
Firma	Medio	Alta	Bajo
Geometría de la mano	Medio	Alta	Alto
Huella dactilar	Alto	Alta	Bajo
Iris	Alto	Media	Alto
Reconocimiento Facial	Medio	Media	Bajo
Retina	Alto	Baja	Alto
Voz	Bajo	Bajo	Bajo

Figura 21. Cuadro estadístico que relaciona los Tipos de Biometría Adaptado de Sánchez, 2012, p.12.

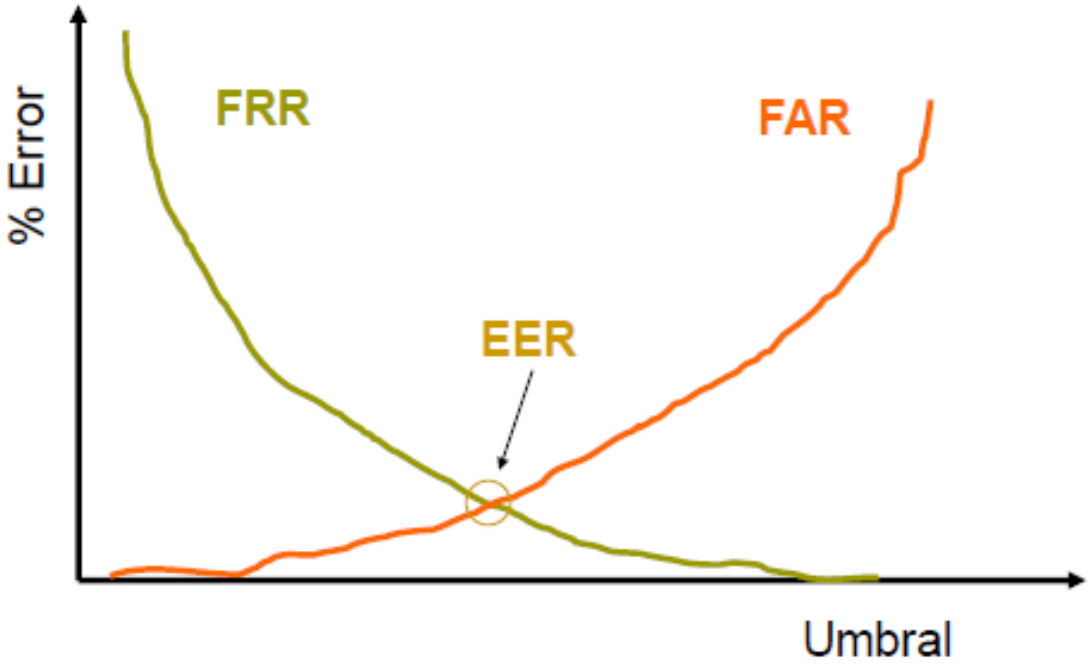


Figura 22. Tasa de Igual Error (ERR) en Biometría Tomado de Sánchez, 2012, p.14.

1.3.2. Bases teóricas del Proceso Seguridad de la Información.

Definición del Proceso Seguridad de la Información

Gómez y Andrés (2012) indicó que Seguridad de la Información es: "La preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio" (p. 20).

Según Marcos (2015) indicó que la Seguridad de la Información:

> mantiene una confidencialidad, integridad y disponibilidad a través de un sistema para toda la información. Con esto se busca ubicar las fragilidades y peligros que pudieran estar sometidos la variedad de activos que estén relacionados en este entorno, de igual forma se toma como objetivo la identificación de controles que reduzcan los riesgos que pudieran ser una amenaza a la misión de la organización (p.3).

Según Ayala (2015) Seguridad de la Información se conceptúa como "todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de tos sistemas tecnológicos que permiten resguardar y proteger la información" (p.23).

Según Morán (2016) Seguridad de la información "se usa para aperturar accesos y no cerrarlos, con el obvio razonamiento de aperturar sólo a quien se le debe aperturar" (p.11).

Dimensiones del Proceso Seguridad de la Información.

Las dimensiones del Proceso Seguridad de la Información que mejor se ajustan a este proyecto de investigación son: Confidencialidad, Integridad y Disponibilidad, donde:

Confidencialidad

Según Marcos (2015), Confidencialidad es “Mantener unas restricciones para autorizar el acceso a la información y divulgación de la misma, y que se incluyan medios para la protección de la intimidad personal y la propiedad de la información” (p.73).

Según Mejía (2015) Confidencialidad se debe conceptuar como: “otro de los principios básicos de la seguridad informática que esta debe garantizar que la información sea extraída e interpretada solo por el usuario de destino” (p.15).

Según Asato, J. y Rosales, E. (2011) se debe entender como Confidencialidad al hecho de que: “La información sólo podrá ser consultada por los usuarios autorizados” (p.54).

Integridad

Según Marcos (2015), indicó que la Integridad es: “Protección contra la modificación de información de forma incorrecta o destrucción de la misma, e incluye asegurar la ‘’information non-repundiation” y su autenticidad” (p.73).

Según Asato, J. y Rosales, E. (2011) aseveró que la Integridad se debe entender como “La información sólo puede ser modificada por quien está autorizado y esta modificación será de manera controlada” (p.54).

Según Mejía (2015) la Integridad: “busca mantener los datos sin modificaciones no autorizadas. La vulnerabilidad de la integridad tiene distinto significado según se produzca en un equipo o en una red informática” (p.14).

Disponibilidad

Según Marcos (2015), La dimensión Disponibilidad es: “Garantizar el acceso a la información cuando sea necesario, así como el uso de la misma” (p.73).

Según Asato, J. y Rosales, E. (2011) en términos de seguridad de la información, Disponibilidad lo conceptúo como: “Debe estar disponible al momento en que se necesite” (p.54).

Según Mejía (2015) aseguró que Disponibilidad es:

> El tercer pilar básico de un sistema seguro, se da cuando los usuarios pueden acceder a la información en el momento adecuado para los usuarios que la requieran. La violación de la disponibilidad también se da de forma distinta en equipos y redes (p.15).

Estándares del Proceso Seguridad de la Información

Existe un marco de referencia en normatividad en cuanto a seguridad de la información, usada en toda organización pública o privada al cual se le denomina Serie ISO 27000, del cual se puede considerar a la ISO 27001 como la norma más trascendente de la serie. Una representación de la evolución histórica que ha seguido esta norma con su inicio como norma BS 7799 de BSI, donde BSI viene a ser British Standards Institution, se observa en el gráfico siguiente. Es conveniente señalar que la BSI mundialmente es la institución pionera de normalización. Por otro lado conveniente es resaltar que mientras BSI es británica y que su aparición lo hizo en 1901, su equivalente en España es AENOR (Marcos, 2015).

Igualmente Marcos (2015), sobre la norma ISO/IEC 27000 nos dijo que;

> dicha norma resalta la predominancia que tienen los sistemas de gestión de seguridad de la información y como tal hay que constantemente realizarles mejoras a dichos sistemas mediante un monitoreo y mantenimiento. Así mismo nos informa que la serie 27000 es la norma compendio de las anteriores publicaciones realizadas de las normas con sus revisiones respectivas y los límites de acción y el fin que cumple cada una de ellas: así tenemos la publicada el 14 de Enero del 2014 como tercera edición, la publicada el primero de Diciembre del 2012 como segunda edición y

> la publicada el primero de Mayo del 2009 por vez primera como primera edición. Como puede verse la serie 27000 como norma evoluciona con una sucesiva publicación de tres ediciones (p.11).

Modelos del Proceso Seguridad de la Información

Existen varios modelos que pueden ejemplificar el Proceso de Seguridad de la Información, la figura siguiente representa uno de ellos:

Figura 23: Pilares Fundamentales de la Seguridad de la Información. Tomado de Morán, 2016, p.15.

Si a ello le agregamos el hecho de que autenticidad es una palabra que engloba según Montenegro, C.; Gaona, E. & Gaona, P. (2012) un sinnúmero de características relacionadas con la seguridad en los sistemas de información y

dado que la autenticidad es uno de los pilares donde se apoya las Plataformas actuales.

Tenemos sin embargo que los mecanismos presentados en gran parte de plataformas Learning Content Management Systems, (LCMS), no dejan analizar convenientemente los contenidos compartidos en ellas, el concepto de "autenticidad".

De allí que se planteé un Modelo de seguridad informático sobre plataformas de aprendizaje virtual LCMS, con contenidos en base a especificaciones dadas por Sharable Content Object Reference (SCORM), que permita garantizar la autenticidad de contenidos a través de conceptos de firmas digitales e identificación de protocolos y mecanismos que sirvan de garantía para este forma de actividades.

La realización se conceptúa esgrimiéndose alternativas de modelos de seguridad, a partir del análisis de los mecanismos de seguridad informáticos usados actualmente sobre la mayoría de plataformas LCMS, de la misma manera que la identificación de componentes y variables bajo el criterio del desarrollo de contenidos a través de las especificaciones SCORM. Por otro lado;

> Tiene cierto tiempo de manejo el concepto de web of trust, no olvidemos que está a la par con el inicio del mecanismo Pretty Good Privacy, para seguridad de correos electrónicos (Zimmermann, 1995), que conceptúa la idea de dar por aceptado la identidad de un usuario cuando el mismo sea reconocido por algún otro usuario del sistema que permita de esta manera dar garantía para ser aceptado bajo el esquema de comunicación de la plataforma que están compartiendo. (pp.51- 54).

1.3.3. Definición de Términos básicos

Acreditación: “Dícese de un cuerpo de certificación que con relación a las normas que emita un ente de acreditación en el ámbito ISO/IEC 27001 lo cumple, por mencionar un caso: ENAC con AENOR” (Marcos, 2015, p.127).

Biometría: “Es el estudio de métodos de reconocimiento de humanos basados en la extracción de alguna de sus características intrínsecas, ya sean físicas (huellas, iris, venas de la mano, etc.) o de comportamiento (la firma, el paso, el tecleo, etc.)” (González, 2013, p.11)

Centroide Espectral: “Característica del sonido en relación a su forma espectral. Señalamiento del lugar donde se ubica la mayor concentración de espectro” (Aguirrezabala, 2015, p.40).

Certificación: “Viene a ser la situación que se presenta al afirmarse con seguridad por parte de un ente de certificación independiente que el sistema de gestión con relación a ISO/IEC 27001es conforme” (Marcos, 2015, p.127).

Escala Mel: “Permite acercar al oído humano la resolución frecuencial. Establece una relación entre la frecuencia percibida (eje y) y la frecuencia real (eje x)” (Aguirrezabala, 2015, p.42).

Fidelidad: “Comparación de una muestra biométrica y su fuente, con relación a su Grado de similitud” (Cerame, 2014, p.13).

Filtro de Pre-énfasis: “Usado para elevar el espectro de la señal 20 dB por década en forma aproximada” (Rueda, 2011, p.46).

Fonemas: “Representaciones de sonidos del habla, en donde la representación no va por el lado físico del sonido sino más bien por la abstracción mental que se tiene de él” (Rueda, 2011, p.34).

Habla: “Señal acústica, obtenida de las ondas salientes de la boca y las fosas nasales de un locutor como ondas de presión” (Rueda, 2011, p.23).

Legibilidad: “Es la forma de claridad que presenta un texto cuando se lo lee, dícese también de la facilidad del entendimiento de una documentación al ser leída” (Marcos, 2015, p.128).

Nivel Acústico: “Reconocimiento producido en el oído por una comunicación oral, dícese también del grupo de características importantes de una señal acústica recibida ante el envío de un determinado emisor“(Rueda, 2011, p.39).

Nivel Fonético: “Información sustancial en forma secuencial que se obtiene del nivel acústico que termina siendo ser una secuencia de fonemas mediante una traducción“(Rueda, 2011, p.40).

Nivel Fonológico: “Información que brindan los fonemas de una determinada lengua después que la información fonética de las palabras son analizadas por un conjunto secuencial de términos léxicos“(Rueda, 2011, p.40).

Nivel Léxico: “Información que se obtiene de una comunicación al identificarse en una determinada lengua las palabras usadas” (Rueda, 2011, p.40).

Nivel Sintáctico: “Información correspondiente a las reglas gramaticales que relaciona las palabras en el nivel léxico realizando de esta manera un estudio descriptivo y analítico del lenguaje” (Rueda, 2011, p.40).

Nivel Semántico: “Información correspondiente a la comprensión del mensaje recibido encontrando el exacto sentido de las palabras. Nivel equivalente a la información que brinda un diccionario sobre las palabras” (Rueda, 2011, p.40).

Nivel Pragmático: “Información correspondiente al sentido del mensaje recibido tomando en consideración el ámbito y la situación en que se realiza la comunicación“(Rueda, 2011, p.40).

Nivel Prosódico: “Información complementaria y de estructura no jerárquica con los demás niveles anteriormente tratados” (Rueda, 2011, p.40).

Sistema: “Referencia que por lo general se hace al sistema de gestión de la seguridad de la información para ISO/IEC 27001, el cual se implementa cuando se cumple algunos requisitos que esgrime la norma” (Marcos, 2015, p.127).

Sonido: “Viene a ser una onda de presión longitudinal obtenida en base a compresiones y expansiones del aire en dirección paralela a la aplicación de energía” (Rueda, 2011, p.21).

Voz: “Viene a ser el combinar algunos rasgos físicos y conductuales en las personas. La fisionomía del sistema, como el tracto vocal, labios, boca y cavidad nasal es la que determina las características de la voz de una persona” (Cerame, 2014, p.6).

1.4. Formulación del problema

El problema se concentra en el hecho de que en nuestra realidad peruana, la forma extendida de evitar la suplantación de identidad de alguien es en primera instancia disminuida con la verificación del Documento Nacional de Identidad. Y cuando se pretende aumentar el grado de verificación se hace uso de la Biometría Dactilar, habiéndose convertido en la actualidad como el medio más seguro y extendido no solo para evitar la suplantación de la identidad sino para evitar poner en peligro la seguridad de la información de alguien o algo.

Sin embargo todos sabemos la forma tan fácil de falsificar un Documento Nacional de Identidad así como el uso del látex como generador de huellas dactilares postizas. Por estas razones es necesario el planteamiento masivo y no sectario de una nueva herramienta tecnológica en el Perú que persiga lo mismo, sabiendo que los países vecinos al nuestro ya lo vienen usando desde hace algunos años. La presente investigación plantea a la Biometría de Voz como

herramienta tecnológica y la implementa en el proceso de la Seguridad de la Información en las Notarías Públicas Peruanas, 2017.

Problema general

¿Cómo la biometría de voz mejora el proceso de la seguridad de la información en las notarías públicas peruanas, 2017?

Problemas específicos:

¿De qué forma la biometría de voz mejora el grado de fiabilidad en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017?

¿De qué forma la biometría de voz mejora el grado de eficiencia en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017?

1.5. Justificación del estudio

Justificación teórica

El trabajo de investigación incrementará el nivel de información que se tiene en la actualidad de la biometría de voz, su aplicación en la seguridad de la información, así como la correlación de la biometría de voz aplicada y la seguridad de la información en los usuarios de las Notarías Públicas peruanas.

Justificación práctica

Logrará que se manifiesten las mejoras que se obtienen al aplicar la biometría de voz en el proceso de seguridad de la información en las notarías, asimismo conocer la relación de la biometría de voz y la seguridad de la información en las notarías públicas peruanas.

Justificación epistemológica

Toda tesis contribuye a la investigación de un tema específico, en el caso de la tesis realizada la trascendencia estriba en la poca y en algunos casos ninguna aplicación realizada sobre el contexto Notarías Públicas Peruanas, lo que nos lleva a reflexionar los aportes que esta tesis deja para el campo de la gestión pública en general, sirviendo en algunos casos como un nuevo enfoque al proceso de la seguridad de la información.

Justificación legal

La tesis se justifica legalmente al poner de manifiesto con su presentación el marco de acción de "la ley promulgada el 21 de octubre y publicada el 22 de octubre del 2013 en El Peruano como Ley 30096 o *Ley de delitos informáticos,* la cual a manera de información de dicha Ley se puede decir que experimentó una modificación: la Ley 30171 promulgada el nueve de marzo y publicada el 10 de marzo del 2014 en El Peruano como *Ley que modifica la Ley 30096"* (Villavicencio, 2014, p.284).

Justificación técnica

Es un clamor tecnológico evitar las suplantaciones de identidad producidas por inadecuadas identificaciones de un usuario especialmente en nuestro contexto, que es una Notaría Pública.

Los métodos clásicos de autenticación como el uso de elementos físicos llámese llaves, tarjetas magnéticas, etc. o las famosas claves o passwords presentan una serie de inconvenientes de seguridad. Si a esto le añadimos que la tendencia tecnológica mundial es el uso de alternativas a estos elementos.

Y justo el uso de la biometría como mecanismo alternativo de seguridad en la información evita que las claves o passwords puedan olvidarse o que los

elementos físicos puedan robarse, ya que por el contrario los datos biométricos que son los rasgos que uno lleva consigo no pueden olvidarse y menos perderse.

1.6. Hipótesis

Hipótesis general

Existe una mejora significativa al aplicar la biometría de voz en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

Hipótesis específicas

La biometría de voz mejora significativamente el grado de fiabilidad en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

La biometría de voz mejora significativamente el grado de eficiencia en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

1.7. Objetivos

Objetivo general

Demostrar la forma en que la biometría de voz mejora el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

Objetivos específicos

Determinar la forma en que la biometría de voz mejora el grado de fiabilidad en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

Determinar la forma en que la biometría de voz mejora el grado de eficiencia en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

II. Método

2.1. Diseño de investigación

Tipo de Investigación

El tipo de investigación de la tesis es el de la Investigación Aplicada. Y esto es así, porque si examinamos lo que nos manifiesta Hernández (2014), se notará que el tipo de Investigación Aplicada, evalúa, compara, interpreta, establece precedentes y determina causalidad y sus implicaciones, características que se ajustan a las acciones que se pueden realizar con los planteamientos cuantitativos que se manejan en esta investigación (p.42).

Diseño de Investigación

La realización de la Tesis tiene el tipo de diseño pre experimental. Considerando que los cambios propuestos en tecnología de la información deben ser deseables y factibles.

Diseño Pre experimental

El nombre Pre experimental obedece a la forma de recolección de datos. Los mismos que cuando son datos cuantitativos se logra a través de una Ficha de Observación. Estas Fichas de Observación permiten basado en los indicadores de mi variable independiente recoger datos cuantitativos y procesarlos utilizando el software SPSS, teniéndose como resultado el Análisis Descriptivo, el cual se muestra a través de Tablas y Diagramas de Barras. De igual forma se ha utilizado el Test de Shapiro - Wilk, para poder analizar la normalidad de los datos.

Se utilizará la Distribución t de Student para el análisis inferencial de la variable cuantitativa, discreta y dependiente: Seguridad de la Información. Una medición previa de la variable dependiente a ser utilizada antes de la aplicación de la variable independiente (Pre - Test). Luego se efectúa la aplicación de la variable independiente a los sujetos de la muestra. Para posteriormente realizar

una nueva medición de la variable dependiente después de la aplicación de la variable independiente (Post - Test).

Esquema de Diseño:

Pre – Prueba	Aplicación de la	Pos – Prueba
Grupo O1	Biometría de Voz	Grupo O2

Especificaciones:

Donde: O_1 = Evaluación del proceso de Seguridad de la Información.

X = Aplicación de la Biometría de Voz y

O_2 = Evaluación del proceso de Seguridad de la Información.

2.2. Variables, operacionalización.

Variable Independiente: Biometría de Voz

Definición Conceptual

Según Escajedo (2015) la Biometría vocal o Biometría de Voz;

> viene a ser una característica biométrica dinámica en virtud de que es necesario un intervalo de tiempo para poder realizarse su captura. La voz de una persona mantiene una serie de tonos distintivos a lo largo de toda su vida a pesar de los cambios que en ella experimenta como por ejemplo el estado de ánimo, el tipo de conversación o el cambio de edad (p.111).

Variable Dependiente: Seguridad de la Información

Definición Conceptual

Según Gómez y Andrés (2012) la Seguridad de la Información es "la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio" (p.20).

Definición Operacional

Tabla 1

Matriz de Operacionalización de la variable Proceso de Seguridad de la Información

Dimensión	Indicador	Unidad de Medida	Instrumento	Fórmula
Integridad	Grado de Fiabilidad en la Seguridad de la Información	Porcentaje (%)	Ficha de Observación (Pre test y Post test)	GF = [1 - (Te / Tr)] * 100 GF = Grado de Fiabilidad (%). Tr = Nro. de trámites realizados y validados. Te = Nro. de trámites realizados y validados con error de identificación.
	Grado de Eficiencia en la Seguridad de la Información	Porcentaje (%)	Ficha de Observación (Pre test y Post test)	GE = [1 - (Tc / Tr)] * 100 GE = Grado de Eficiencia (%). Tr = Nro. de trámites realizados y validados. Tc = Nro. de trámites realizados y validados con consulta externa.

2.3. Población y Muestra

Población

Según Hernández, Fernández y Baptista (2014), población “es el conjunto de todos los casos que concuerdan con determinadas especificaciones” (p.174).

La plana laboral, tanto del área usuaria como del área técnica de las notarías públicas ubicadas en los distritos de Miraflores, San Isidro, San Borja y Santiago de Surco, de las cuales se escogerán una de cada uno de los distritos mencionados, son los elementos constitutivos de lo que entiendo por llamar Población. Cuyo cálculo estadístico me determina el valor apropiado de trabajo de:

P = 40 (Observaciones)

Muestra

Si entendemos a la muestra como una parte de la población, cuya selección evidencie que es una parte significativa de esta, estaríamos siendo consecuentes con la forma de trabajo que se está siguiendo en esta Tesis en cuanto a la muestra tomada. Así nos lo recuerda Hernández, Fernández y Baptista (2014, p.173).

Y bajo ese concepto es que me permito tomar como muestra:

M = 40 (Observaciones)

Muestreo

El tipo de Muestreo no corresponde al tipo probabilístico ni al no probabilístico, ya que la muestra se considerará del tipo Censal pues el investigador seleccionó el 100% de la población al considerarlo un número manejable de Observaciones en las Notarías Públicas. En este sentido Ramírez (1997) afirma que la muestra censal es aquella donde todas las unidades de investigación son consideradas como muestra.

Tabla 2

Observaciones realizadas en las notarías públicas escogidas como representativas: Población identificada por notaría y según área de trabajo asignada (área usuaria y área técnica).

Ubicación donde se realizaron las Observaciones	Observaciones Realizadas		
Notarías de	Área Técnica	Área Usuaria	Total
Santiago de Surco	5	5	10
Miraflores	4	6	10
San Isidro	6	4	10
San Borja	3	7	10
		Población	40

Tomado del Área de Recursos Humanos de Notaría (2017)

Tamaño de la Muestra:

Dado que el tipo de Muestreo es del tipo Censal, la parte que se refiere al cálculo de la magnitud de la muestra se ejecutó bajo el concepto vertido por Ramírez vertido anteriormente. Es decir si el:

Tamaño de la población (40 Observaciones)

Entonces la magnitud de la muestra viene a ser:

M = 40 (Observaciones)

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad.

Se tomó en consideración en esta investigación como forma de recolección de datos, el uso de la técnica e instumento metodológico mostrado en la Tabla siguiente .

Tabla 3

Técnicas de Recolección de datos

Tipo de dato a Recolectar	Técnica	Instrumento
Cuantitativo	Observación	Ficha de Observación

Para lo cual se trabajó con un grupo de datos muestrales en dos eventos temporales. Uno llamado Pre Test, en donde la ficha de observación recoge datos antes de aplicarse la herramienta tecnológica: Biometría de voz. Y otro instante de tiempo, llamado Post Test en donde se recopila datos luego de haberse aplicado la Biometría de voz.

Técnica

La técnica usada para la recolección de datos en esta investigación fue la Observación o Registro, para lo cual se hicieron uso de dos indicadores: grado de fiabilidad y grado de eficiencia, pertenecientes a la dimensión Integridad de la variable Seguridad de la Información. Las observaciones se efectuaron en notarías públicas ubicadas en Lima Metropolitana.

Instrumento

Se utilizaron las Fichas de Observación Pre Test y Post Test como instrumento de medición para el caso de recolección de datos cuantitativos de acuerdo a la técnica definida como observación.

El trabajo inicial con las fichas se efectuó para tomar datos cuantitativos sin haberse aplicado la herramienta tecnológica biometría de voz en el proceso seguridad de la información (Fichas de Observación Pre Test).

Luego como segunda medición, se recolectan datos cuantitativos después de aplicar la herramienta tecnológica biometría de voz en el proceso seguridad de la información (Fichas de Observación Post Test).

Para la representación del instrumento Ficha de Observación utilizado, se consideran las Tablas 4 y 5 mostradas

Tabla 4

Ficha Técnica del Instrumento de recolección de datos cuantitativos – Indicador Grado de Fiabilidad en la Seguridad de la Información

Nombre del Instrumento:	Ficha de Observación de Medición del Indicador Grado de Fiabilidad en la Seguridad de la Información.
Autor:	Jorge Luis Cienfuegos Solís
Año:	2017
Descripción:	
Tipo de instrumento:	Ficha de Observación.
Objetivo:	Medir el Grado de Fiabilidad en la Seguridad de la Información
Historial:	Propuesto por el autor
Número de datos a recolectar:	10
Aplicación:	Directa

.

Tabla 5

Ficha Técnica del Instrumento de recolección de datos cuantitativos – Indicador Grado de Eficiencia en la Seguridad de la Información

Nombre del Instrumento:	Ficha de Observación de Medición del Indicador Grado de Eficiencia en la Seguridad de la Información.
Autor:	Jorge Luis Cienfuegos Solís
Año:	2017
Descripción:	
Tipo de instrumento:	Ficha de Observación.
Objetivo:	Medir el Grado de Eficiencia en la Seguridad de la Información.
Historial:	Propuesto por el autor
Número de datos a recolectar:	10
Aplicación:	Directa

Validez

El especialista mencionado a continuación en la Tabla 6, en base a la ejecución del llamado "juicio de experto" fue el que estableció para el instrumento: observación, su validez, en base a los criterios de claridad, pertinencia y relevancia.

Tabla 6

Experto que dio fe de la validez del contenido del instrumento que mide conocimientos sobre: Seguridad de la Información (Pre Test y Post Test).

DNI	Grado Académico, Apellidos y Nombres	Institución donde Labora	Calificación
10192315	Magister. Joel Martín Visurraga	Universidad Cesar Vallejo	Aplicable

Tomando como elementos de evaluación de cada dimensión de las variables de la tesis, los conceptos de: claridad, pertinencia y relevancia se validó el cuestionario, y a juicio de los expertos coincidieron en darle como resultado de su apreciación de aplicabilidad, el grado de: “Aplicable”.

Confiabilidad

El coeficiente estadístico Alfa de Cronbach fue el estadístico usado para verificar la fiabilidad de la ficha de observación de recolección de datos en esta tesis. Por lo tanto desde el punto de vista cuantitativo el instrumento de evaluación resultó ser medible y como tal me proporcionó el siguiente resultado de la Tabla 7.

Tabla 7

Estadísticos de fiabilidad – (10 observaciones)

Alfa de Cronbach	N de elementos
0.935	10

Adaptado del Software IBM SPSS versión 22.

2.5. Métodos de análisis de datos:

El uso de la Tablas y Gráficos nos permite manejar los datos cuantitativos con comodidad, haciendo uso del software IBM SPS Statistics v22. Redondeando nuestros resultados con el auxilio de Diagramas de Barras y Tablas lo que se lleva a cabo en la realización del análisis descriptivo.

Posteriormente para el análisis inferencial se contrastan las hipótesis, haciendo uso de la Distribución t de Student y para ello se hará nuevamente uso del software IBM anteriormente mencionado.

2.6. Aspectos éticos:

Es necesario dejar en claro que los Derechos de Autor así como la Protección de Datos se encuentran protegidas y respetadas en esta investigación, citando y referenciando las informaciones vertidas.

Los autores mencionados, así como sus trabajos de investigación se evidencian en el capítulo de referencias. Notándose de esta forma que la investigación realizada contribuye a fomentar el buen uso que siempre debe hacerse con información que no es de la propiedad intelectual de uno.

III. Resultados

3.1. Análisis Descriptivo

En virtud de haber definido la investigación presente como del tipo pre experimental, se procedió a realizar el análisis descriptivo de las variables, dimensiones e indicadores que corresponden a los tipos de datos recopilados. En base a estos datos, se detallan los resultados descriptivos obtenidos.

La aplicación de la Biometría de Voz en el proceso de Seguridad de la Información, nos permite evaluar la mejora que se produce en el proceso, en base a dos indicadores: Grado de Fiabilidad y Grado de Eficiencia. Los mismos que son evaluados a partir de Fichas de Observación aplicadas en un antes (Pre Test) y en un después (Post Test) de la implementación de la Biometría de Voz.

Análisis Descriptivo del indicador Grado de Fiabilidad

Tabla 8

Estadísticos descriptivos del Grado de Fiabilidad antes (Pre Test) y después (Post Test) de implementar la Biometría de Voz.

	N	Mínimo	Máximo	Media	Desviación estándar
Grado de Fiabilidad - Pre Test	40	60,00	82,00	72,6000	7,57481
Grado de Fiabilidad - Post Test	40	92,00	100,00	96,2000	2,57337
N válido (según lista)	40				

Elaborado con la ayuda del Software SPSS versión 22.

Nótese una gran diferencia entre la media del grado de fiabilidad en el caso Pre Test 72,60 con el caso Post Test que indica 96,20. De igual forma obsérvese que el momento Post Test toma como valor máximo: 100.00, que indica que para ese registro, todos los trámites realizados han sido validados, es decir que ninguno presenta un error de identificación.

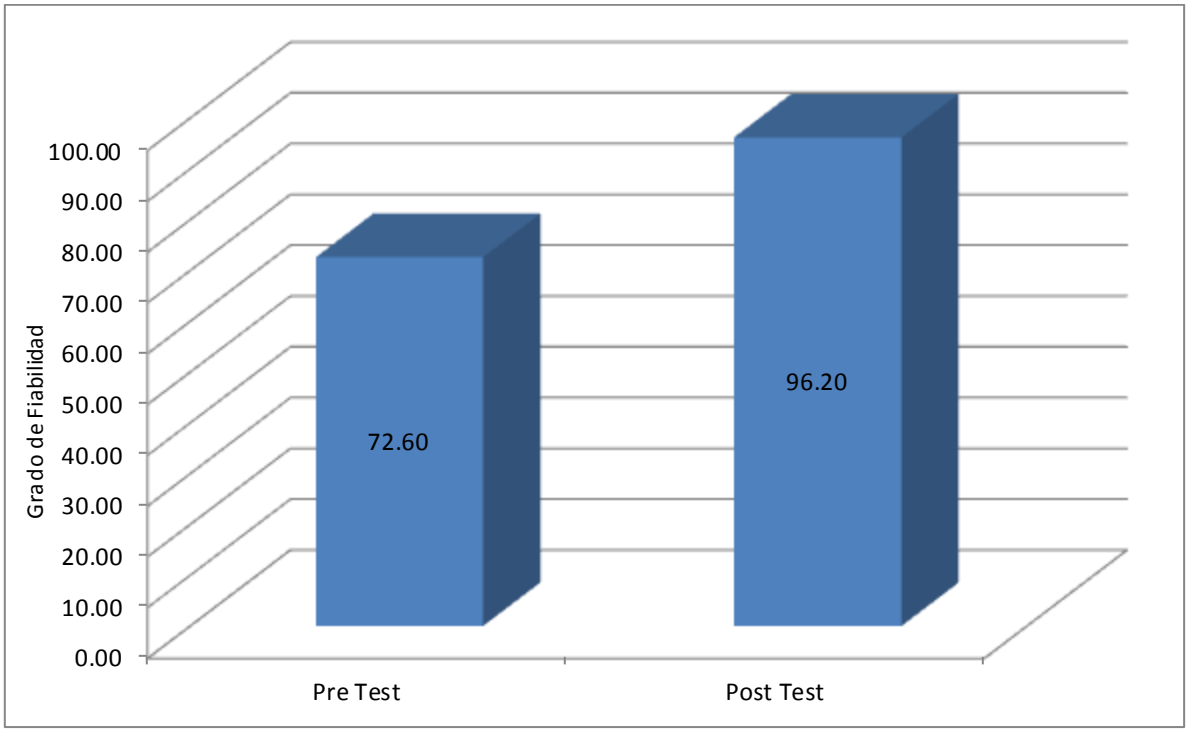


Figura 24. Indicador del Grado de Fiabilidad antes (Pre Test) y después (Post Test) de implementar la Biometría de Voz.
Elaborado con la ayuda del Software SPSS versión 22.

Análisis Descriptivo del indicador Grado de Eficiencia

Tabla 9

Estadísticos descriptivos del Grado de Eficiencia antes (Pre Test) y después (Post Test) de implementar la Biometría de Voz.

	N	Mínimo	Máximo	Media	Desviación típica
Grado de Eficiencia - Pre Test	10	60,00	76,00	66,3000	5,49848
Grado de Eficiencia - Post Test	10	90,00	98,00	94,1000	2,60128
N válido (según lista)	10				

Elaborado con la ayuda del Software SPSS versión 22.

Nótese una gran diferencia entre la media del grado de fiabilidad en el caso Pre Test 66,30 con el caso Post Test que indica 94,10. De igual forma obsérvese que el momento Post Test toma como valor máximo: 100.00, que indica que para ese registro, todos los trámites realizados no han necesitado de consulta externa.

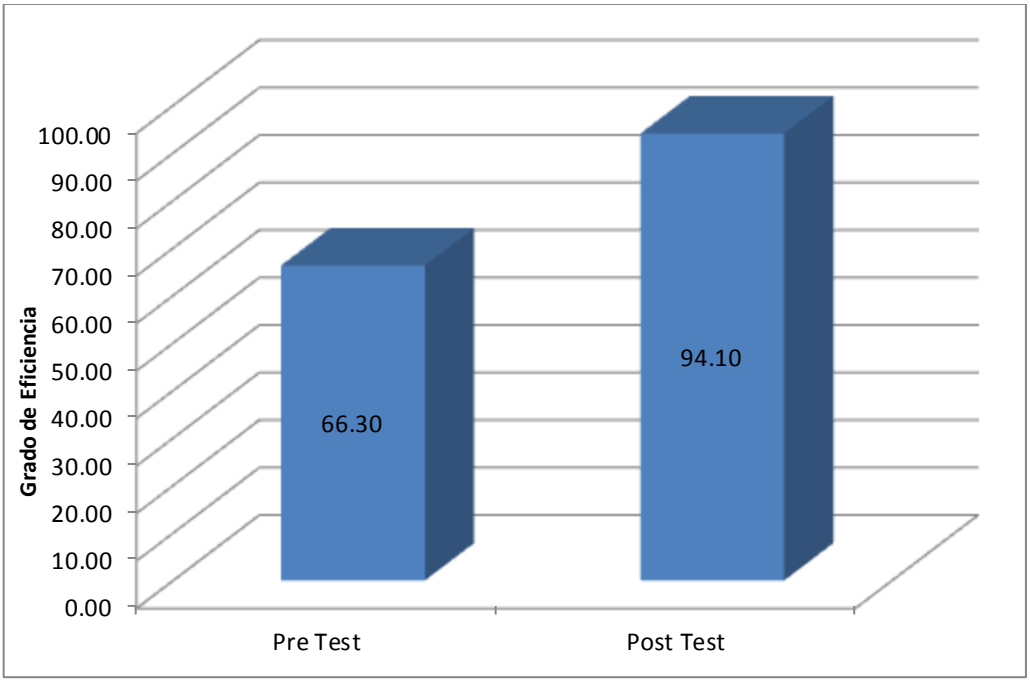


Figura 25. Indicador del Grado de Eficiencia antes (Pre Test) y después (Post Test) de implementar la Biometría de Voz.
Elaborado con la ayuda del Software SPSS versión 22.

3.2. Análisis Inferencial

Análisis Inferencial de la Hipótesis Específica 1, correspondiente al indicador Grado de Fiabilidad

Prueba de Normalidad

Como el número de Observaciones o Registros realizados fueron 40 que es un número menor a 50, se pudó usar el método Shapiro-Wilk para realizar la Prueba de normalidad con un nivel de confiabilidad del 95%

Formulación de la hipótesis estadística:

H_0: Los datos del indicador Grado de Fiabilidad tienen un comportamiento normal.

H_1: Los datos del indicador Grado de Fiabilidad no tienen un comportamiento normal.

Tabla 10

Prueba de Normalidad de Shapiro-Wilk para el Grado de Fiabilidad antes (Pre Test) y después (Post Test) de implementar la Biometría de Voz.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Grado de Fiabilidad - Pre Test	,884	40	,146
Grado de Fiabilidad - Post Test	,924	40	,392

Elaborado con la ayuda del Software SPSS versión 22.

En la Tabla 10 se observan que los resultados de la prueba indicaron que el Sig.: P-valor o nivel crítico del contraste de la muestra referente al grado de fiabilidad antes y después de la implementación de la biometría de voz tuvieron valores mayores a 0.05. Obteniéndose para antes (Pre Test) 0.146 y para después (Pro Test) 0.392, valores que permite rechazar la hipótesis alternativa (H_1) y aceptar la hipótesis nula (H_0), indicando de esta manera que los datos del grado de fiabilidad se distribuyen normalmente.

Se confirmó que la distribución de los datos de la muestra es normal al obtenerse las Figuras 26 y 27 siguientes

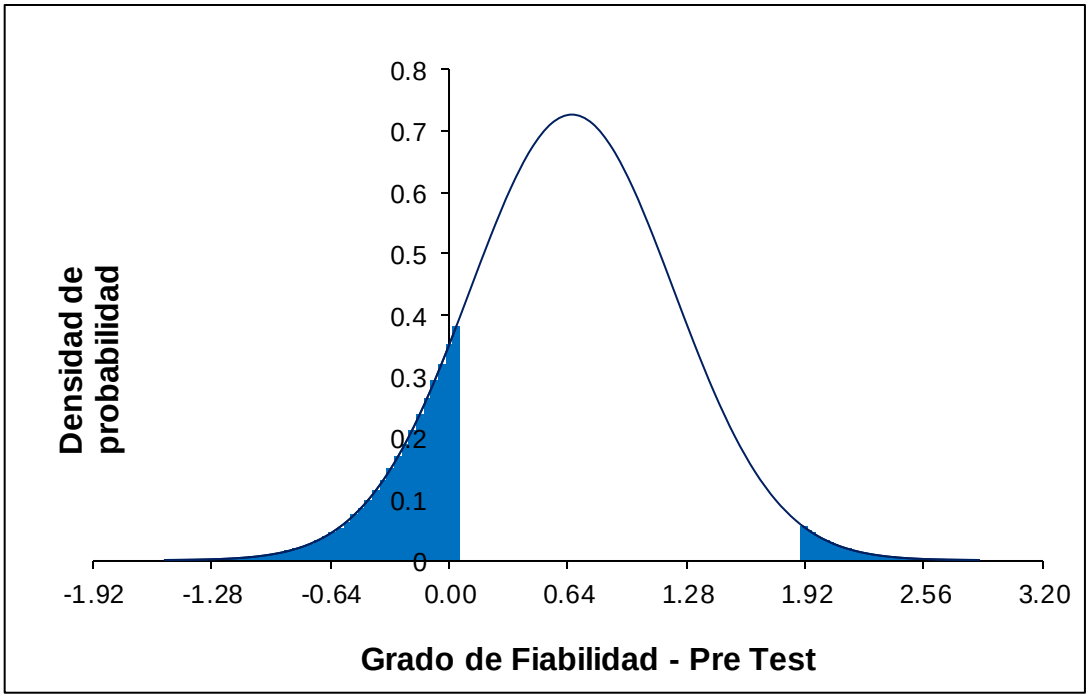


Figura 26. Distribución normal (Gauss) Pre Test del Grado de Fiabilidad. Elaborado con la ayuda del Software SPSS versión 22.

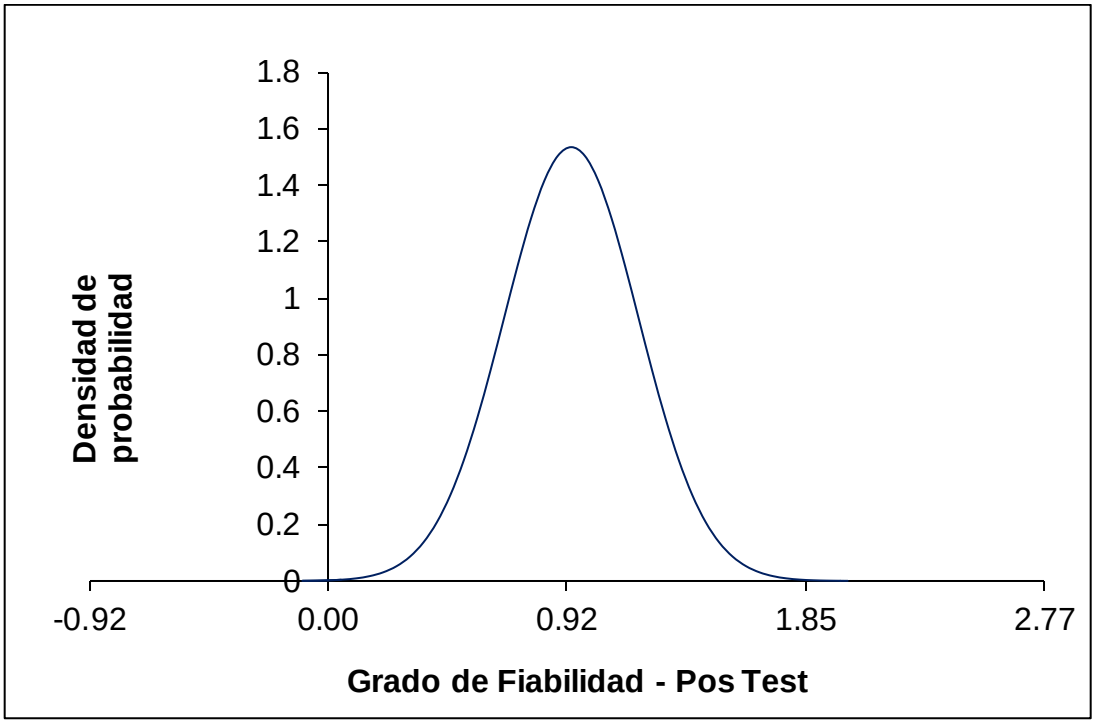


Figura 27. Distribución normal (Gauss) Post Test del Grado de Fiabilidad. Elaborado con la ayuda del Software SPSS versión 22.

Contrastación de la Hipótesis Específica 1: HE1

HE1: La biometría de voz mejora significativamente el grado de fiabilidad en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

Para ello se realizó la Formulación de la hipótesis estadística para el Indicador: Grado de Fiabilidad.

Definición de variables:

GFa = Grado de Fiabilidad sin biometría de voz.

GFp = Grado de Fiabilidad con biometría de voz.

H_0: La biometría de voz no mejora significativamente el grado de fiabilidad en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

$$H_0 = GFa - GFp > 0$$

De aceptarse la Hipótesis Nula H_0 anteriormente mostrada, se podrá afirmar que el indicador Grado de Fiabilidad sin biometría de voz (Sistema actual) es mejor que el indicador Grado de Fiabilidad con biometría de voz (Sistema propuesto).

H_1: La biometría de voz mejora significativamente el grado de fiabilidad en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

$$H_1 = GFa - GFp <= 0$$

De rechazarse la Hipótesis Nula H_0, es decir de aceptarse la Hipótesis Alterna H_1 anteriormente mostrada, se podrá afirmar que el indicador Grado de Fiabilidad con biometría de voz (Sistema propuesto) es mejor que el indicador Grado de Fiabilidad sin biometría de voz (Sistema actual).

Tabla 11

Prueba de t de Student para el Grado de Fiabilidad antes (Pre Test) y después (Post Test) de implementar la Biometría de Voz.

	Prueba t de Student			
	Media	t	gl	Sig. (Bilateral)
Grado de Fiabilidad antes (Pre Test) Grado de Fiabilidad después (Post Test)	-14.500	-7.245	39	.000

Elaborado con la ayuda del Software SPSS versión 22.

Para contrastar la hipótesis específica 1, correspondiente al indicador Grado de Fiabilidad, se aplicó la Prueba t de Student, en virtud a que los datos obtenidos durante la investigación (Pre Test y Post Test) se distribuyen normalmente.

El valor de t contraste obtenido fue de -7.245, y debido a que es bastante menor que el valor T-Teórico de -1.895, se procedió entonces a rechazar la hipótesis nula aceptando la hipótesis alterna con un 95% de confianza.

Si a esto le sumamos el hecho de haberse obtenido una diferencia de medias: Pre test – Post Test de -14.50, las cuales se hacen significativas estadísticamente al haberse obtenido un valor de la probabilidad asociada al estadístico T, que en la Tabla 11 aparece como Sig. (Bilateral), inferior al nivel de error (0,05) es decir 0,000, se permitió concluir que la ubicación de la t sea la de la zona de rechazo de la hipótesis nula.

Por consiguiente se rechazó la hipótesis nula y se aceptó la hipótesis alterna, es decir al implementar la biometría de voz mejora significativamente el grado de fiabilidad en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

La figura 28 que se muestra a continuación da una explicación de los valores característicos de una Distribución de t de Student. En dicho gráfico se observa el valor de 0.95 que corresponde a un nivel de confianza del 95%, es decir un margen de riesgo o de error $\alpha = 0.05$. Así mismo se aprecia, que donde aparece el 0.05 se denomina Región de Rechazo y donde aparece 0.95 se denomina Región de Aceptación. Ambos conceptos haciendo alusión a la Hipótesis nula a la cual se le está haciendo el Análisis Inferencial.

De igual forma nótese que el T = -1.6604 mostrado corresponde al valor de T-Teórico que da el límite o frontera entre la Región de Rechazo y la Región de Aceptación. Su cálculo se obtiene de cruzar dos valores: el nivel de confianza 0.95 y los grados de libertad del estadístico a compararse. Generalmente el estadístico a compararse es la media. Finalmente el t = -11.63 corresponde al valor t obtenido con la prueba de t de Student para el ejemplo mostrado, que me está indicando que al ser mucho menor que -1.6604 ubica a la Hipótesis Nula propuesta en la Región de Rechazo, aceptándose la Hipótesis alterna. Esto debe confirmarse con el valor de la probabilidad asociada al estadístico T o Sig.

(Bilateral), que no aparece en el gráfico, el cual debe ser de un valor menor a 0.05, generalmente 0.000.

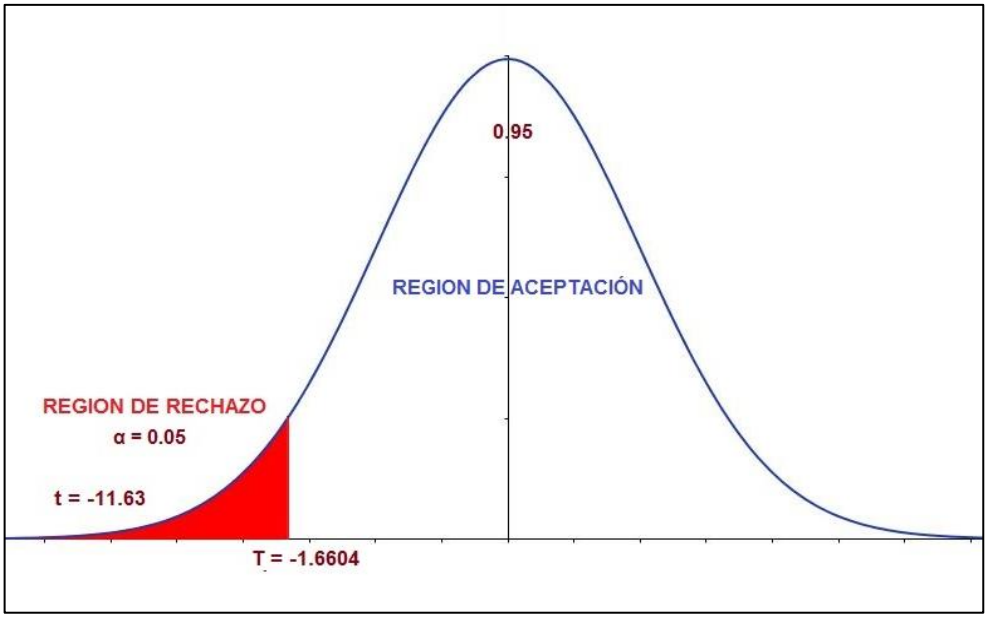


Figura 28. Ejemplo de una Distribución de t de Student donde se muestran sus valores representativos.
Tomado del software GeoGebra 5.0.

Análisis Inferencial de la Hipótesis Específica 2, correspondiente al indicador Grado de Eficiencia

Prueba de Normalidad

Como el número de Observaciones o Registros realizados fueron 40 que es un número menor a 50, se pudó usar el método Shapiro-Wilk para realizar la Prueba de normalidad con un nivel de confiabilidad del 95%.

Formulación de hipótesis estadística:

H_0: Los datos del indicador Grado de Eficiencia tienen un comportamiento normal.

H_1: Los datos del indicador Grado de Eficiencia no tienen un comportamiento normal.

Tabla 12

Prueba de Normalidad de Shapiro-Wilk para el Grado de Eficiencia antes (Pre Test) y después (Post Test) de implementar la Biometría de Voz.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Grado de Eficiencia - Pre Test	,911	40	,290
Grado de Eficiencia - Post Test	,934	40	,493

Elaborado con la ayuda del Software SPSS versión 22.

En la Tabla 12 se observan que los resultados de la prueba indicaron que el Sig.: P-valor o nivel crítico del contraste de la muestra referente al grado de fiabilidad antes y después de la implementación de la biometría de voz tuvieron valores mayores a 0.05. Obteniéndose para antes (Pre Test) 0.290 y para después (Pro Test) 0.493, valores que permite rechazar la hipótesis alternativa (H_1) y aceptar la hipótesis nula (H_0), indicando de esta manera que los datos del grado de fiabilidad se distribuyen normalmente.

Se confirmó que la distribución de los datos de la muestra es normal al obtenerse las Figuras 29 y 30 siguientes.

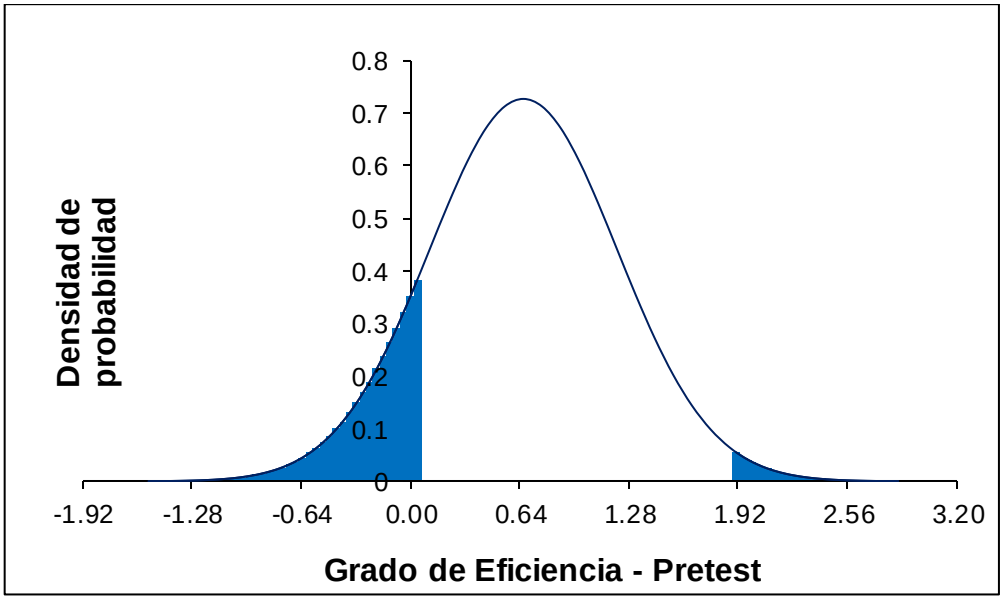


Figura 29. Distribución normal (Gauss) Pre Test del Grado de Eficiencia. Elaborado con la ayuda del Software SPSS versión 22.

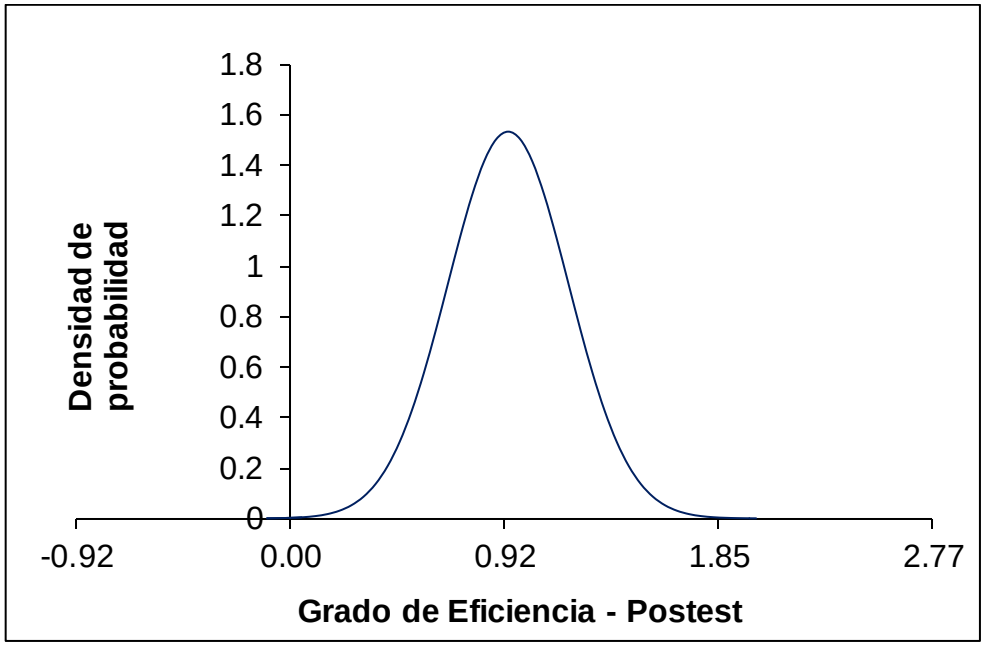


Figura 30. Distribución normal (Gauss) Post Test del Grado de Eficiencia. Elaborado con la ayuda del Software SPSS versión 22.

Contrastación de la Hipótesis Específica 2: HE2

HE2: La biometría de voz mejora significativamente el grado de eficiencia en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

Para ello se realiza la Formulación de la hipótesis estadística para el Indicador: Grado de Eficiencia.

Definición de variables:

GEa = Grado de Eficiencia sin biometría de voz.

GEp = Grado de Eficiencia con biometría de voz.

H_0: La biometría de voz no mejora significativamente el grado de eficiencia en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

$$H_0 = GEa - GEp > 0$$

De aceptarse la Hipótesis Nula H_0 anteriormente mostrada, se podrá afirmar que el indicador Grado de Eficiencia sin biometría de voz (Sistema actual) es mejor que el indicador Grado de Eficiencia con biometría de voz (Sistema propuesto).

H_1: La biometría de voz mejora significativamente el grado de eficiencia en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

$$H_1 = GEa - GEp <= 0$$

De rechazarse la Hipótesis Nula H_0, es decir de aceptarse la Hipótesis Alterna H_1 anteriormente mostrada, se podrá afirmar que el indicador Grado de Eficiencia con biometría de voz (Sistema propuesto) es mejor que el indicador Grado de Eficiencia sin biometría de voz (Sistema actual).

Tabla 13

Prueba de t de Student para el Grado de Eficiencia antes (Pre Test) y después (Post Test) de implementar la Biometría de Voz.

	Prueba t de Student			
	Media	t	gl	Sig. (Bilateral)
Grado de Eficiencia antes (Pre Test) Grado de Eficiencia después (Post Test)	-14.600	-6.155	39	.000

Elaborado con la ayuda del Software SPSS versión 22.

Para contrastar la hipótesis específica 2, correspondiente al indicador Grado de Eficiencia, se aplicó la Prueba t de Student, en virtud a que los datos obtenidos durante la investigación (Pre Test y Post Test) se distribuyen normalmente.

El valor de t contraste obtenido fue de -6.155, y debido a que es bastante menor que el valor T-Teórico de -1.895, se procedió entonces a rechazar la hipótesis nula aceptando la hipótesis alterna con un 95% de confianza.

Si a esto le sumamos el hecho de haberse obtenido una diferencia de medias: Pre test – Post Test de -14.60, las cuales se hacen significativas estadísticamente al haberse obtenido un valor de la probabilidad asociada al estadístico T, que en la Tabla 13 aparece como Sig. (Bilateral), inferior al nivel de error (0,05) es decir 0,000, se permitió concluir que la ubicación de la t sea la de la zona de rechazo de la hipótesis nula.

Por consiguiente se rechazó la hipótesis nula y se aceptó la hipótesis alterna, es decir al implementar la biometría de voz mejora significativamente el grado de eficiencia en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

IV. Discusión

La realización de un análisis comparativo de los indicadores grado de fiabilidad y grado de eficiencia en el proceso seguridad de la información en las notarías públicas peruanas se puede lograr en base a los resultados obtenidos en la presente tesis de investigación y los Trabajos Previos, tanto Internacionales como Nacionales expuestos en el capítulo uno. Y bajo este planteamiento de análisis es que se desarrollará este capítulo de discusión.

1. El grado de fiabilidad para el proceso seguridad de la información, en la evaluación Pre-Test nos proporcionó un 72.60 y con la aplicación de biometría de voz se elevó a 96.20; indicándome con estos resultados un incremento de 23.60, que me permite asegurar que con la aplicación de la biometría de voz se obtuvo un aumento de 32.50% en el grado de fiabilidad en el proceso seguridad de la información.

Los resultados anteriormente obtenidos son inobjetables. Y así lo entiende también Aguirrezabala (2015), en su investigación "Estudio de Verificación Biométrica de Voz" al hacer notar que el grado de fiabilidad de un tipo de biometría dinámica como es la biometría de voz, supera a las biometrías estáticas como la que actualmente se tiene en las notarías públicas peruanas, como máximo sistema de seguridad en la información, es decir la biometría dactilar. Pero no todo lo que brilla es oro, los resultados anteriormente obtenidos deben engranarse convenientemente con la función que tiene un notario en el Perú, para que de esta manera la aplicación de la biometría de voz en la seguridad de la información en las notarías públicas peruanas tenga el máximo provecho posible. Si consideramos el estudio efectuado por Peralta (2015), en su investigación "Nueve años de biometría en el Perú: La fe de identificación en la encrucijada", se aprecia claramente que en el análisis que realizó el autor sobre los sistemas de identificación biométrica y su papel en la identificación de las personas aceptó los principios y origen científico que tienen estos sistemas, por ende entendió las cualidades que se aprovechan de su aplicación en las notarías. Pero con la misma contundencia argumental de las cualidades, lo hizo de igual forma con las limitaciones que traen consigo, tomando como eje de sustento el hecho de que la obligatoriedad bajo sanción de la consulta biométrica por los notarios genera una

preferencia por el resultado de un test automatizado en lugar de la fe de identificación notarial. Y esto al parecer del autor no debe ser así, llegando incluso a advertir del peligro que trae consigo la atribución de infalibilidad a los sistemas de identificación automatizados.

Obviamente esta investigación no comparte esta opinión, muy respetable por cierto, pero inexacta con el objetivo principal que se está manejando, que como se dijo en capítulos anteriores es demostrar la forma en que la biometría de voz mejora el proceso de seguridad de la información en las notarías públicas peruanas mas no la de demostrar su infalibilidad en los resultados obtenidos cuando se realice su aplicación.

2. El grado de eficiencia para el proceso seguridad de la información, en la medición Pre-Test resulto ser 66.30 y en la medición pos-test 94.10 indicándome con estos resultados que existe nuevamente un aumento, pero que en este caso es de 27.80, de manera que se puede asegurar que con la aplicación de biometría de voz se obtuvo un aumento de 32.50% en el grado de eficiencia en el proceso seguridad de la información. Con lo cual se puede afirmar que con la implementación de la biometría de voz a través del hardware y software que se explicará en el capítulo de la propuesta se logró nuevamente una mejora en el proceso de seguridad de la información. Sin embargo es conveniente recoger otros ángulos experimentales de estudios de investigación realizados, en donde se pueda apreciar factores que limiten los alcances del uso de estas tecnologías. En tal sentido Cárdenas (2015), en su investigación “Diseño de la Estrategia de Implementación de un Sistema de Prevención del Fraude en el Sector Financiero, mediante el uso de Biometría Facial y por Voz” demostró que si bien es cierto el uso de estas nuevas tecnologías generan un gran aporte en la prevención del fraude en el sistema bancario chileno, de igual manera la utilización de los software existentes al marco legal nacional es quien le pone un límite a las bondades que se puedan obtener cuando se implementan estas nuevas tecnologías.

Aunque las realidades o los entornos donde se plantean las actuaciones de las variables tanto dependiente como la independiente son diferentes, mientras Cárdenas hace referencia a Chile, la presente investigación se circunscribe a las notarías públicas peruanas. Sus conclusiones sin embargo no dejan de tener una gran aproximación a lo que sucede en la realidad mundial. Es bastante atinado en pensar que el marco legal que establece una determinada nación es uno de los límites que se establece como tope para las ventajas que se puedan obtener con la implementación de nuevas tecnologías, como la biometría de voz, a pesar de demostrarse que su grado de eficiencia mejora significativamente la seguridad de la información.

3. El objetivo principal de la presente investigación, como se mencionó en el capítulo uno, es la de demostrar la forma en que la biometría de voz mejora el proceso de seguridad de la información en las notarías públicas peruanas. El cual ha sido realizado, dado que la investigación expone resultados que permiten garantizar que la biometría de voz sirve como instrumento adicional a los ya existentes de mejora en el tratamiento y seguridad en la información en las notarías públicas peruanas, ya que proporciona un aumento en la eficiencia a la hora de manipular datos, mostrando a su vez un grado de fiabilidad mejorado al momento de usarse, confirmando así que la biometría de voz para el proceso seguridad de la información incrementa el grado de fiabilidad en un 32.50%, así mismo se observa que el grado de eficiencia logra incrementarse en un 41.93%.

A pesar de ello, Escajedo (2015), en su Tésis Doctoral “Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas”, resalta un elemento no considerado hasta ahora en esta investigación: el exceso de seguridad. Pudiera parecer hasta increíble, pero en otras latitudes el uso de otros tipos de biometría diferentes a la biometría dactilar, que es la que hasta el momento marca el nivel máximo de seguridad en las instituciones públicas peruanas y dentro de ellas las notarías públicas, tienen un uso tan extendido que como bien lo remarca Escajedo sobrepasa el nivel de privacidad que todo individuo posee en cuanto al acopio de información de su identidad. Es decir mientras acá ni siquiera se aplica en forma masiva la biometría de voz, en otros

sitios se aplica demasiado dicha biometría. Y como tal es importante hacer notar, como lo describe Escajedo, el riesgo de la vigilancia excesiva. En esa dirección es rescatable lo de Bouihrouzan (2016), en su investigación “Seguridad e Inseguridad en los Sistemas Biométricos:Seguridad Vs Privacidad”, donde intenta establecer el límite entre la seguridad y la privacidad.

V. Conclusiones

Primera: Se concluye que el grado de fiabilidad sin la implementación de la herramienta tecnológica de biometría de voz, nos lleva a la realidad actual de funcionamiento del proceso de seguridad de la información en las notarías públicas peruanas; es decir un valor de representación de 72.60. Al incrementarse este valor a 96.20, valor muy cercano al máximo posible de obtener que es 100.00, cuando se implementa la herramienta tecnológica, nos está diciendo en cifras su alto grado de confianza en la biometría de voz.

Segunda: Se concluye que el grado de eficiencia sin la implementación de la herramienta tecnológica de biometría de voz, nos lleva a la realidad actual de funcionamiento del proceso de seguridad de la información en las notarías públicas peruanas; es decir un valor de representación de 66.30. Al incrementarse este valor a 94.10, valor muy cercano al máximo posible de obtener que es 100.00, cuando se implementa la herramienta tecnológica, nos está diciendo en cifras su alto grado de rentabilidad en la biometría de voz.

Tercera: Finalmente, después de haber obtenidos valores tan favorables en el aspecto de fiabilidad y eficiencia al implementar la biometría de voz, se puede concluir que su uso no se lleva a cabo aun casualmente por dos factores que se agudizan ante la falta de divulgación de los mismos. Estos son: la falta de interés por la poca confianza que se le brinda a la herramienta tecnológica, situación que se desploma con la medición Post Test del grado de fiabilidad obtenido y la creencia del alto tiempo de retorno de la inversión que llevaría el implementar la herramienta Biometría de voz, situación que igualmente pierde sustento cuando se observa el valor obtenido como Post Test en el grado de eficiencia.

VI. Recomendacion

Primera: Se sugiere promover entre las Notarías Públicas el hecho de que la evolución de las herramientas de seguridad para el manejo de sus informaciones pasa por observar el grado de fiabilidad que va cediendo paso ante los avances que se dan mundialmente en los nuevos sistemas de medición biométricos como lo es la Biometría de Voz.

Segunda: Se recomienda examinar la seguridad de la información en las Notarías Públicas, y revisar el costo que significa la verificación de sus resultados de autenticidad de los usuarios que así lo requieran con la recurrencia de sitios exteriores a las Notarías, en otras palabras obtener información del ahorro que significaría tener su propia base de datos para la disminución del tiempo de verificación, situación que se logra con la implementación de la biometría de voz

Tercera: Se sugiere realizar una combinación de verificación de rasgos biométricos, usando el actual patrón biométrico dactilográfico con el patrón biométrico de voz, lo que le da una mayor potencia al proceso de seguridad de la información y así no se estaría cambiando un mecanismo de seguridad por otro, sino más bien se estaría repotenciando el proceso de seguridad de la información con la implementación de la biometría de voz.

.

VII. Propuesta

7.1. Organización Empresarial

La organización empresarial que en este esta investigación de tesis corresponde a una institución pública, como lo es una notaría pública peruana está formada por las siguientes áreas de trabajo: el Área Usuaria y el Área Técnica. Se debe entender por Área Usuaria como aquella ubicación donde se encuentran las personas que de alguna u otra manera harán uso de la tecnología de información propuesta Biometría de Voz, vale decir: el usuario propiamente dicho, el empleado y el notario.

Por esta razón, esta área de trabajo se encuentra en la ubicación organizacional de una notaría cumpliendo las funciones de Actividades Primarias. Encontrándose dentro de este grupo de actividades, las que corresponden a: Servicio al Ciudadano, Gestión de Trámites de Identificación y Gestión Servicio Registral, como las más importantes.

Por otro lado el Área Técnica se encuentra en la ubicación organizacional de una notaría cumpliendo las funciones de Actividades de Soporte. Encontrándose dentro de este grupo de actividades, las que corresponden a: Gestión Humana, Gestión Tecnológica, Gestión Logística, Gestión Jurídica y Gestión Financiera. Las actividades mencionadas son las que mejor caracterizan a la organización de una Notaría Pública Peruana.

El proceso de estudio en la propuesta es la Seguridad de la Información, el cual si es analizado en una Notaría Pública Peruana bajo la perspectiva de encontrar los puntos en la organización donde las personas allí ubicadas tengan que ver algo con el proceso, tendríamos que concluir que realmente todas las áreas y puntos organizacionales de la notaría se encuentran involucradas, ya que

todos de alguna u otra manera buscan preservar la mayor Seguridad de la Información que manejan, es algo inherente a cualquier notaría.

Sin embargo es fácil notar en el Diagrama de la Cadena de Valor de una Notaría Pública Peruana, que es el grupo de personas que cumplen el rol de Actividades Primarias en la organización de una notaría las que se encuentran involucradas en los subprocesos Gestión Servicio Registral y Gestión de Trámites de Identificación, que son los subprocesos definidos donde se aplicará la propuesta de tecnología de información Biometría de Voz que con más detalle se verá en la siguiente sección 7.2 Procesos.

Las personas que cumplen las Actividades de Soporte, sobre todo en las secciones concernientes a Gestión Tecnológica y Gestión Logística, serán cruciales a la hora de realizar la implementación de la Biometría de Voz. Ya que la tecnología de información propuesta supone un cambio en el funcionamiento habitual que tiene una notaría al cual se le implementa esta nueva tecnología de información.

Las personas por lo general son renuentes a los cambios y desde el punto de vista organizacional es hasta comprensible dicha actitud. En una notaría cualquiera, cada persona tiene una labor asignada que cumplir. El cambio que suscita la implementación de la Biometría de Voz en el proceso de Seguridad de la Información con lleva a una variación de la forma que se tiene de realizar la verificación e identificación de alguien, que de alguna manera ejercerá un cambio en la organización de la notaría. Lo que se propone es que es que el cambio se dé, pero como una mejora del proceso Seguridad de la Información, evidenciado en mejoras en las realizaciones de los subprocesos Gestión Servicio Registral y Gestión de Trámites de Identificación.

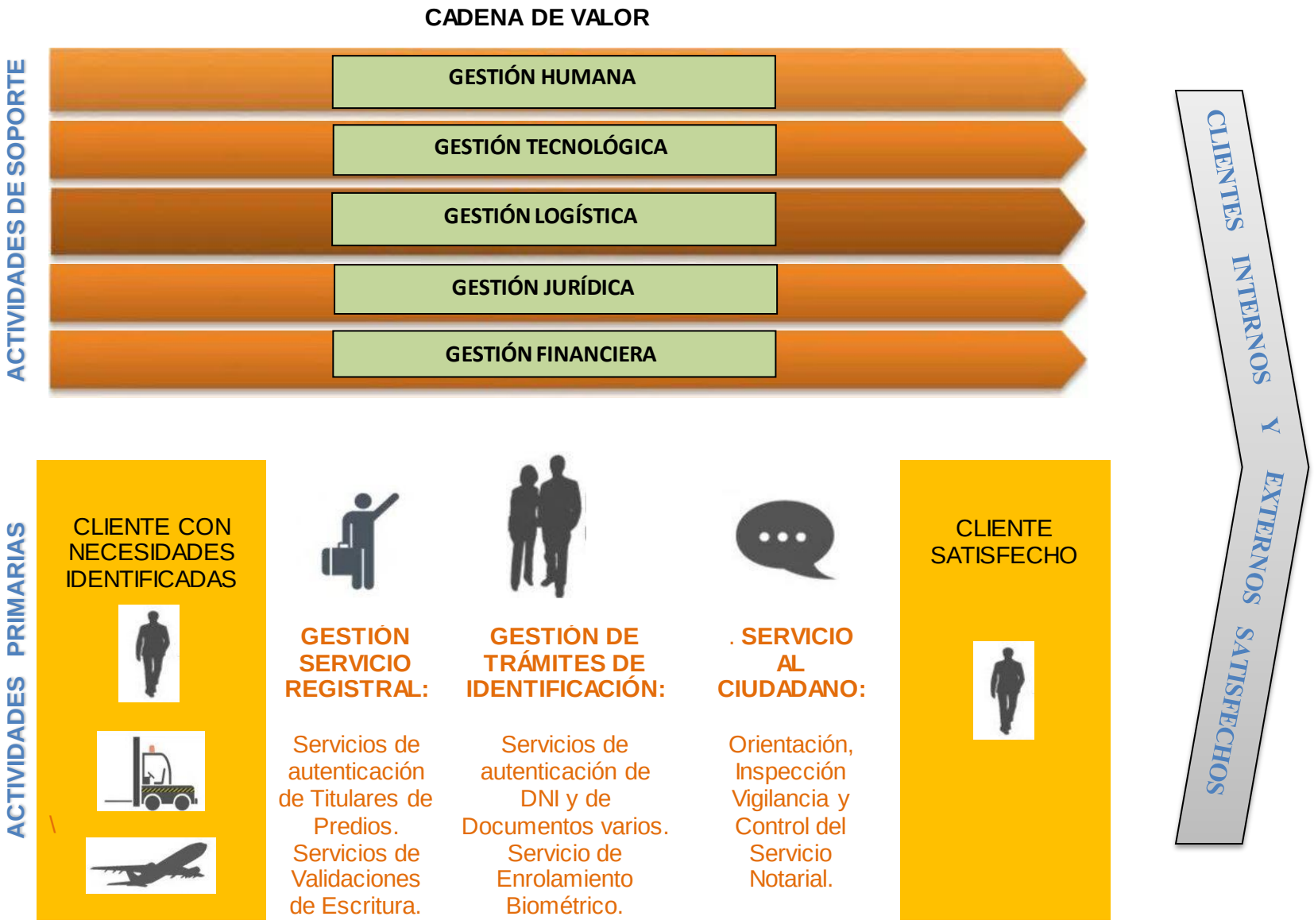


Figura 29. Cadena de Valor de una Notaría Pública Peruana.

7.2. Procesos

El proceso en estudio propuesto es el proceso de la Seguridad de la Información el cual tiene los subprocesos definidos: Gestión de Trámites de Identificación y Gestión de Servicio Registral a realizarse en una Notaría Pública Peruana. Estos Subprocesos llevan una secuencia de ejecución que comienza con la solicitud de un cliente en el Área de Actividades Primarias de la notaría, de alguna de las dos Gestiones mencionadas.

El inicio de cualquiera de los Subprocesos, supone haber realizado previamente la función de Enrolamiento del patrón de voz en la notaría sujeta a estudio de la implementación de la tecnología de información Biometría de Voz. Vale decir, que la persona que solicita la ejecución de la Biometría de Voz como herramienta de verificación y/o autenticación de alguna de las dos Gestiones mencionadas como Subprocesos en la notaría, deberá previamente Registrar su Voz, es decir enrolar esa información en la notaría respectiva.

Los Diagramas de Procesos Pre Test, hacen referencia a la realización de cualquiera de las dos Gestiones: Gestión de Trámite de Identificación y Gestión de Servicio Registral sin la implementación de la tecnología de información Biometría de Voz. De igual forma los Diagramas de Procesos Post Test son las Gestiones realizadas con la Implementación ya realizada de la Biometría de Voz.

Tanto para el caso Pre Test y Post Test, siempre se hará uso previamente como elemento de identificación inicial el Documento Nacional de identidad del individuo solicitante del servicio notarial. Esto en virtud de que en todo momento se ha mencionado a lo largo del trabajo de investigación, que la tecnología de información propuesta no va a ser un reemplazo de las actuales formas de verificación y/o autenticidad de identidad de alguien, sino que debe considerarse

un complemento o segundo filtro de identificación. De esta manera se está cumpliendo lo que el mercado exige, que es la forma multimodal de verificación y/o identificación de la identidad de alguna persona.

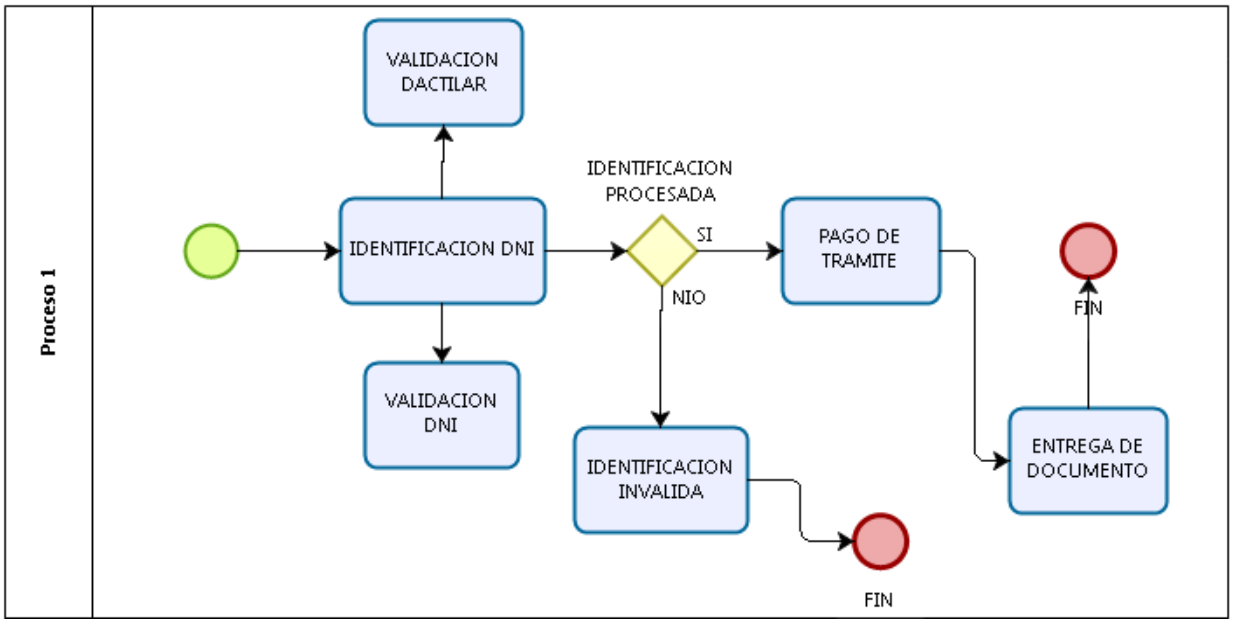
Por otro lado, es consecuente la exigencia previa del Documento Nacional de Identidad antes del enrolamiento del patrón de voz en la notaría, ya que se tiene que tener la certeza de que la persona a la cual se le va adjudicar mayor información de identificación es quien dice ser.

Lo anterior implica la presencia del Registro Nacional de Identificación y Estado Civil (RENIEC), como parte de la ruta del proceso mostrado antes y después de implementado la tecnología de información. Además la tendencia es que no solamente la notaría que realiza el enrolamiento tenga dicha información sino también la RENIEC. De esta manera no se crea cuellos de botella en el aspecto de acceso a la información.

Los indicadores de Grado de Fiabilidad y Grado de Eficiencia explicados extensamente en el estudio de investigación presente se ponen de manifiesto en el Diagrama de Procesos que se presenta a continuación, en la medida que se consulta luego de la comparación con la base de datos enrolados de los clientes de la notaría. El Grado de Fiabilidad se observa al obtenerse menos casos de error en la identificación de alguien casualmente por la doble verificación que se le realiza al individuo. Por otro lado, el Grado de Eficiencia se observa en el Diagrama de Procesos al no necesitarse la consulta externa con alguna otra notaría, ya que con la base datos que se forma y que lo guarda la notaría, se minimiza este procedimiento adicional.

Todo lo anteriormente expuesto queda aclarado en el Diagrama de Procesos mostrado a continuación:

- **GESTION DE TRÁMITES DE IDENTIFICACIÓN - ANTES**
  - SIN BIOMETRIA DE VOZ



- **GESTION DE TRÁMITES DE IDENTIFICACIÓN - DESPUÉS**
  - CON BIOMETRIA DE VOZ

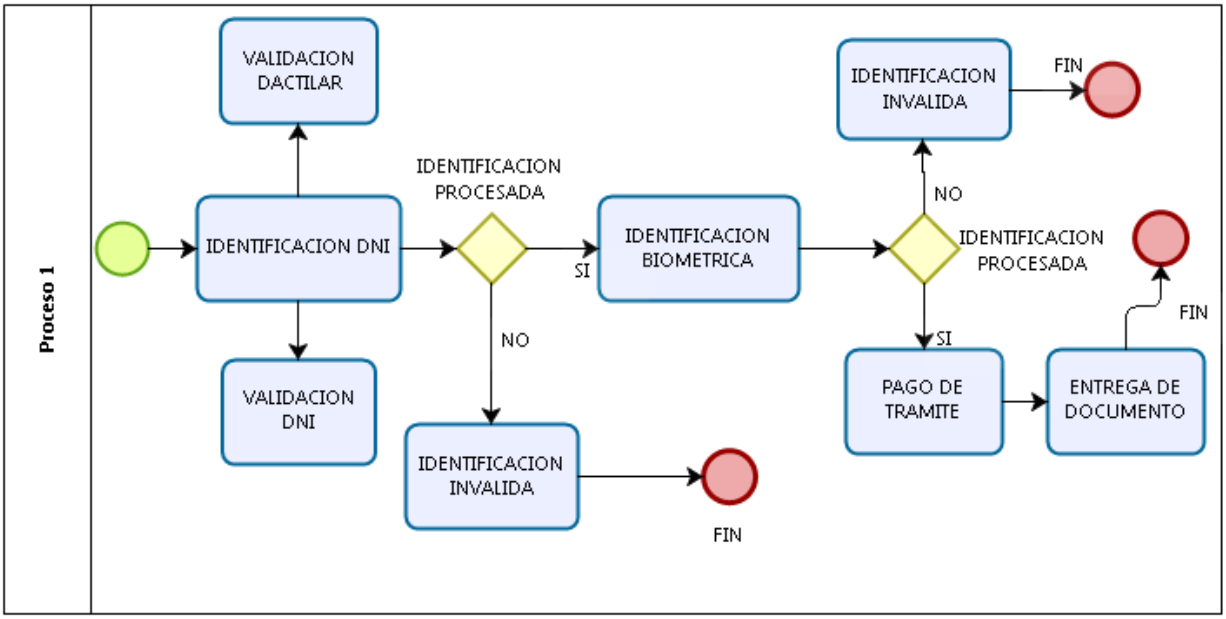
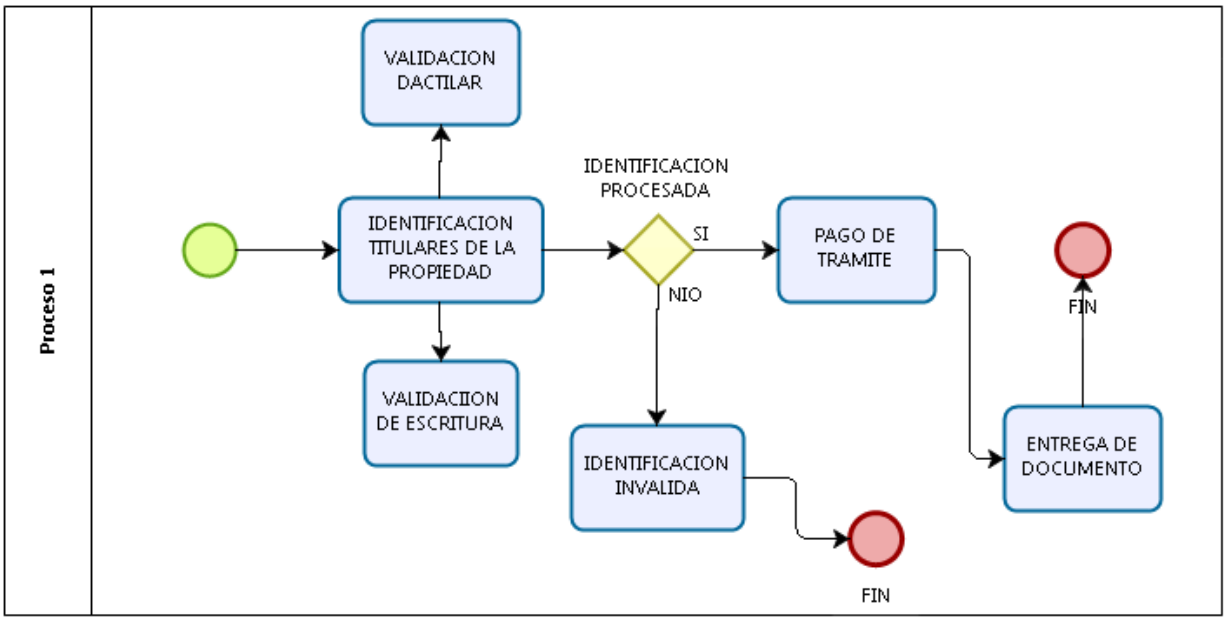


Figura 30. Diagrama de Procesos del Subproceso Gestión de Trámites de Identificación.

- **GESTIÓN DE SERVICIO REGISTRAL - ANTES**
  - SIN BIOMETRIA DE VOZ



- **GESTIÓN DE SERVICIO REGISTRAL - DESPUÉS**
  - CON BIOMETRIA DE VOZ

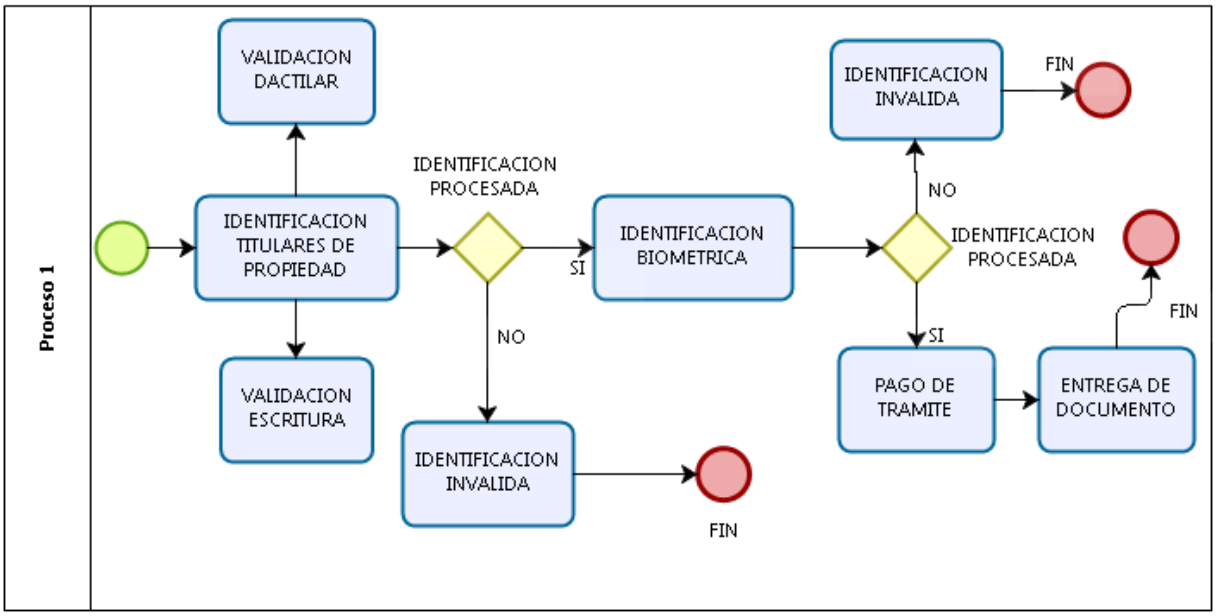


Figura 31. Diagrama de Procesos del Subproceso Gestión de Servicio Registral.

7.3. Arquitectura de Tecnología de Información

La tecnología de información biometría de voz propuesta en esta investigación requiere del procedimiento de enrolamiento o registro del Patrón de Voz. Proceso que como se muestra en el Diagrama Arquitectónico de la Biometría de voz, consistirá en contestar 3 preguntas que se le formulará en la oficina de registro de la Notaría al cliente que así lo desee.

Previo a ello como lo indica el Diagrama Arquitectónico, la persona tendrá que identificarse con su DNI en primer lugar, para posteriormente hacerlo a través del reconocedor biométrico dactilar y de esta manera tener la certeza que a la persona que se la va a registrar su Patrón de Voz es quien dice ser.

Este procedimiento se realiza en la oficina de registro, participando activamente el Administrador de la Notaría, al cual se le ha entrenado para este procedimiento inicial o de Enrolamiento de un cliente nuevo.

Se hace notar que para el procedimiento de enrolamiento el cliente nuevo tiene que apersonarse a la notaría, no necesitándose posteriormente acercarse personalmente para su identificación, la cual la podrá realizar en forma remota vía teléfono fijo simple o teléfono móvil o celular.

Nótese también que la herramienta de Biometría de Voz es la única herramienta biométrica que permite comprobar la identidad de una persona vía remota, utilizando convenientemente la red de telefonía pública o PSTN con el Internet. Además de acondicionar una Central Telefónica Privada o PBX. A continuación se muestra el Diagrama Arquitectónico de la Biometría de Voz, nótese que sin la implementación de la herramienta propuesta, no se tienen clientes remotos.

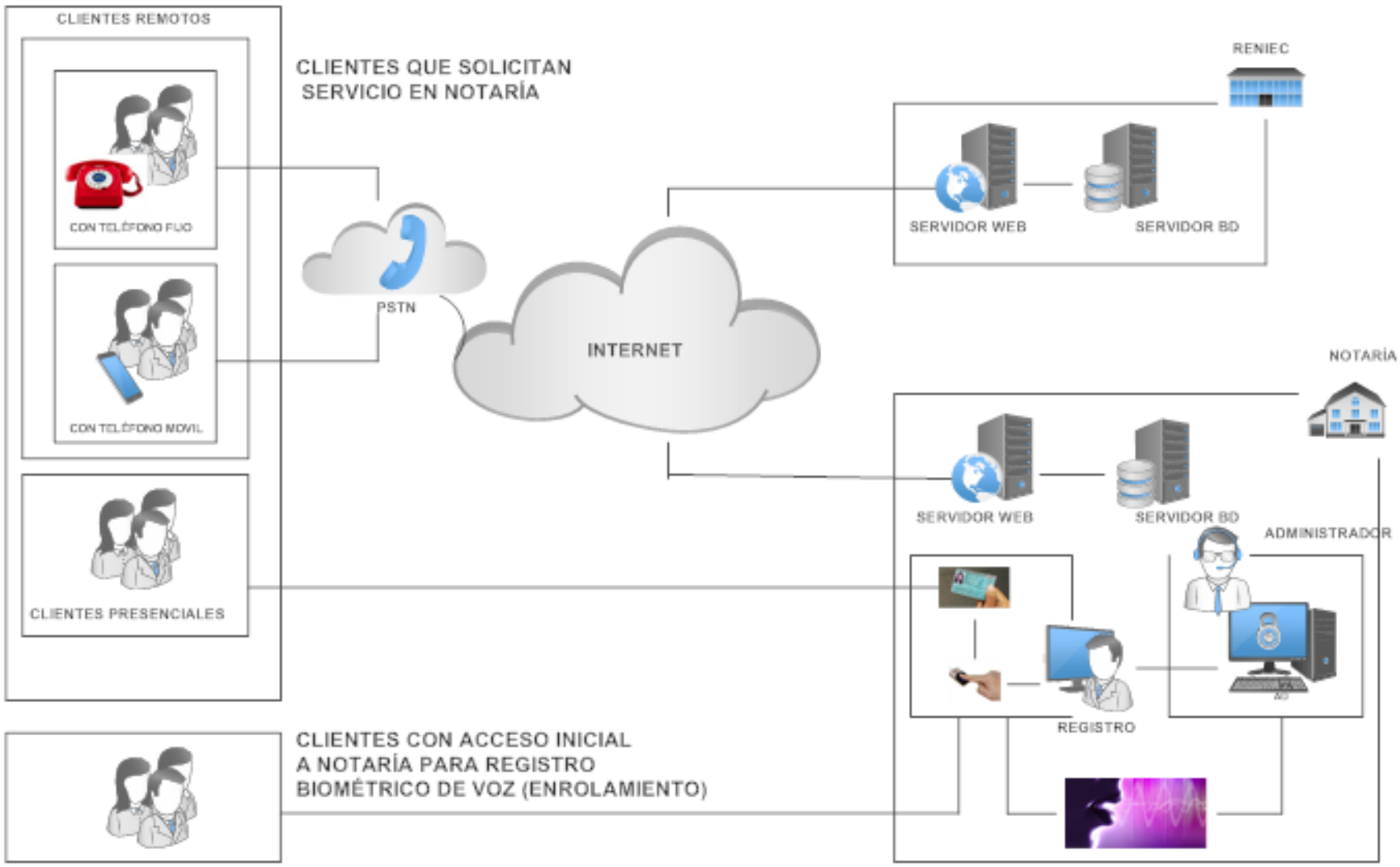


Figura 32. Arquitectura de la Biometría de Voz.

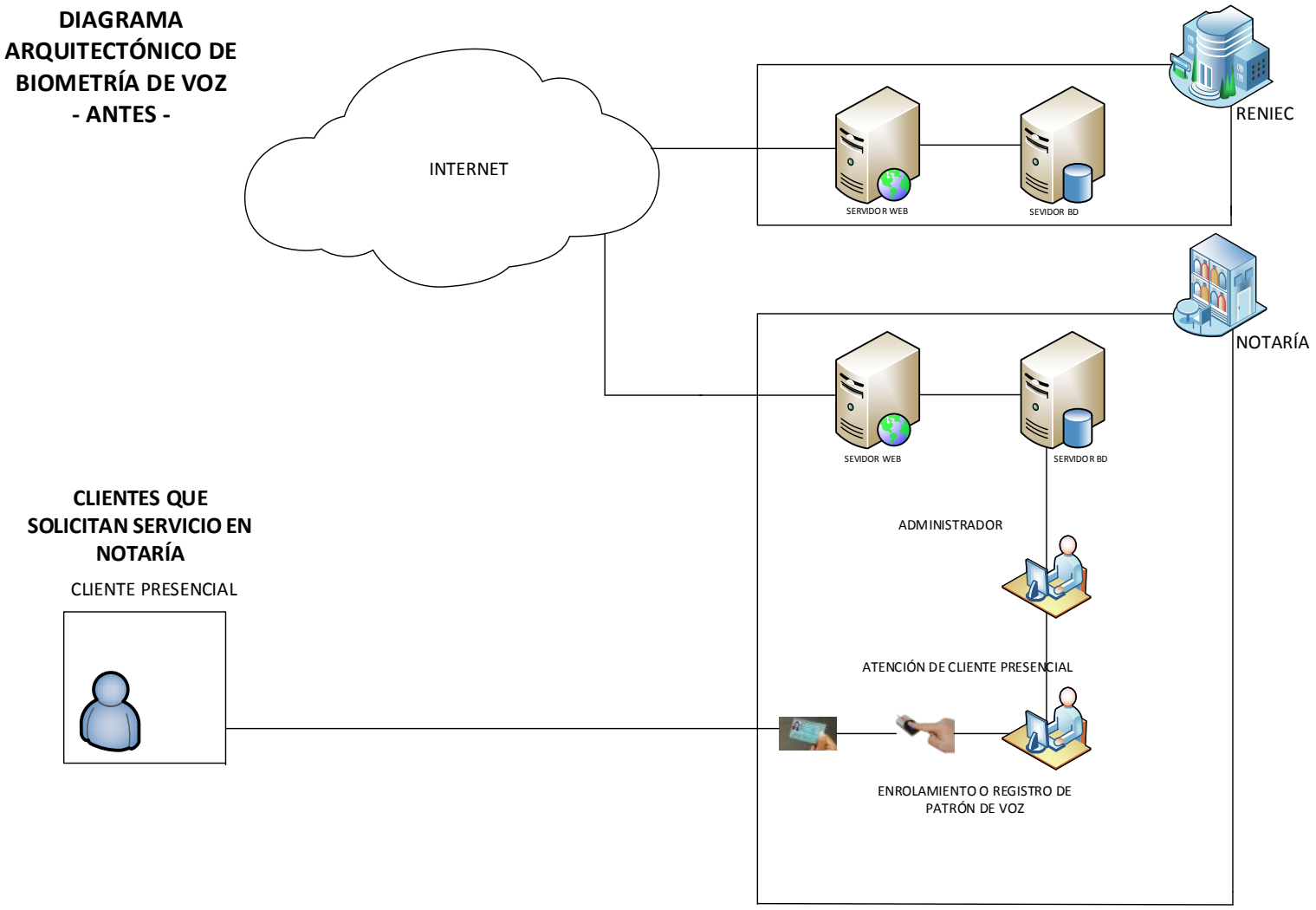


Figura 33. Diagrama Arquitectónico de Biometría De Voz antes de implementación de Propuesta.

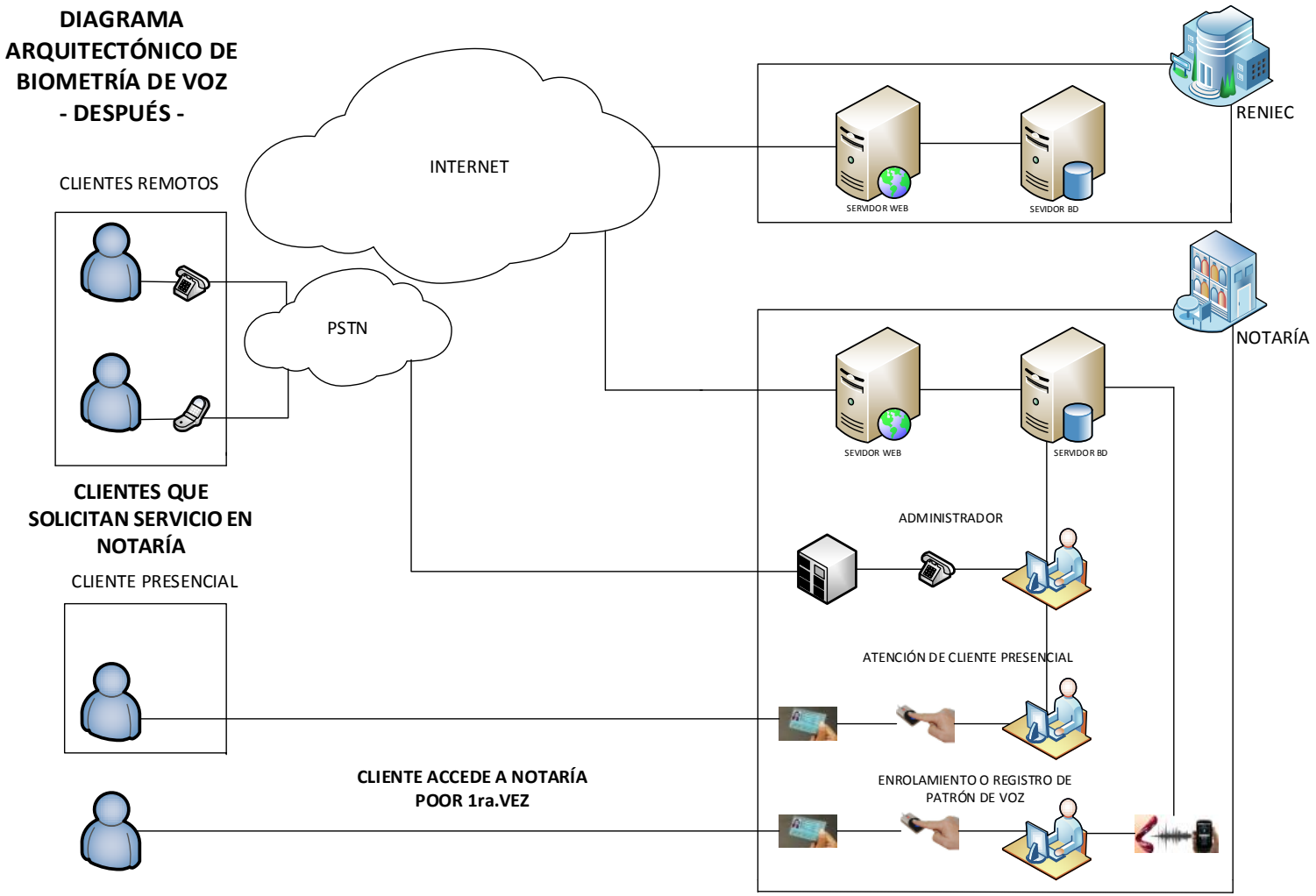


Figura 34. Diagrama Arquitectónico de Biometría De Voz después de implementación de Propuesta.

7.4. Prototipeo

La tecnología de información propuesta en el estudio es biometría de voz el cual va a ser implementado a través de un software, el cual debe contener las siguientes vistas.

VISTA 1: LOGGIN Y REGISTRO DE DNI

En esta primera vista lo que se le pedirá al cliente que accede a los Servicios de una Notaría implementada con Biometría de Voz es que tenga que identificarse con su DNI, que es el primer paso del Enrolamiento.

VISTA 2: REGISTRO BIOMÉTRICO DACTILAR

Seguidamente, el cliente deberá realizar una Verificación de Identidad haciendo uso del Registro Biométrico Dactilar con que debe de contar la Notaría que desea implementar la Biometría de Voz.

VISTA 3: INFORMACIÓN DE DNI Y HUELLA DACTILAR EMITIDA POR RENIEC

Seguidamente la Notaría se enlazará con las oficinas de la RENIEC, vía Internet, a través de su Servidor Web, con el objeto de tener la mayor certeza de que la persona a la cual se va a someter a la grabación de su Patrón de Voz es quien dice ser.

VISTA 4: ENROLAMIENTO O REGISTRO DE PATRÓN DE VOZ

De ser positiva la verificación biométrica dactilar el cliente procederá a Registrar su Patrón de Voz, para lo cual tendrá que contestar 3 preguntas que la persona encargada de Registro en la Notaría le efectuará. Esto lo hará en un teléfono simple no propietario que está conectado a una Central Telefónica Privada (PBX) acondicionada para ello.

VISTA 5: ALMACENAJE DE PATRÓN DE VOZ EN SERVIDOR DE BASE DE DATOS DE NOTARÍA

El software implementado en la PBX, guardará las respuestas a las 3 preguntas en su Servidor BD o Servidor de Base de Datos de la Notaría, como un Archivo Digital. Trabajo realizado por el Administrador de la Notaría, identificando convenientemente al cliente en mención.

VISTA 6: ASIGNACIÓN DE REGISTRO NUMÉRICO AL PATRÓN DE VOZ DE CLIENTE

El cliente se retirará con un número de registro que corresponderá al Patrón de Voz registrado en la Notaría, culminando de esta manera el Proceso de Enrolamiento o registro del Patrón de Voz.

VISTA 7: CLIENTE ACCEDE A SERVICIO NOTARIAL CON PATRÓN DE VOZ

El cliente cuando posteriormente desee realizar un Servicio en la Notaría al cual se ha enrolado, podrá demostrar su identificación, por 3 medios: vía teléfono fijo simple, vía teléfono móvil o celular o acercándose personalmente a la Notaría.

VISTA 8: RECEPCIÓN DE VOZ DEL LLAMANTE O CLIENTE

De la forma remota, es decir vía teléfono fijo o móvil, el cliente sólo llamará a la Notaría, haciendo uso de la red de telefonía pública o PSTN, la cual estará convenientemente enlazada con el Internet

VISTA 9: COMPARACIÓN DE PATRÓN DE VOZ EN NOTARÍA Y VOZ DEL LLAMANTE O CLIENTE

Lo que se comprobará con la llamada a la Notaría es el resultado de la comparación del Patrón de Voz guardado en la Notaría con la voz del llamante o cliente. La persona que recepciona la llamada en la Notaría hará las preguntas convenientes a la persona que solicita comprobación de identificación.

VISTA 10: ANÁLISIS DE REGISTRO DE VOZ DEL LLAMANTE

El Registro de Voz del llamante es lo que se va a comparar, haciendo pasar por 2 canales de voz la llamada efectuada. Uno de los canales de voz tiene el Patrón de Voz guardado en Notaría.

VISTA 11: RESULTADO NUMÉRICO OBTENIDO DE ANÁLISIS DE REGISTRO DE VOZ

La comparación del Registro de Voz se manifestará con un resultado numérico que indicará si el Registro de voz se encuentra dentro del rango permitido como aceptación de identidad de la persona que dice ser.

<u>VISTA 12</u>: VERIFICACIÓN SI SE ENCUENTRA DENTRO DEL MARGEN DE ERROR PERMITIDO

De ser satisfactoria la comparación de registro o estar dentro del margen de error permitido se procederá a continuar con el trámite notarial que en este caso el cliente lo quiere realizar de forma remota.

VIII. Referencias

Aguilar, G. (2016). *Implementación de un modelo simplificado de firma digital basado en la tecnología PKI y la innovación por protocolos caso de estudio: Municipalidad de Miraflores.* Facultad de Ingeniería de Sistemas e Informática. E.A.P. Ingeniería de Sistemas. UNMSM. Lima. Perú. Recuperado el 9 de diciembre de 2016 de: http://cybertesis.unmsm.edu.pe /bitstream/cybertesis/4993/1/Aguilar_ag.pdf.

Aguirrezabala, M. (2015). *Estudio de Verificación Biométrica de Voz.* Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicación. Madrid. España. Recuperado el 9 de diciembre de 2016 de: http://oa.upm.es/38115/1/TESIS_MASTER_MARTA_AGUIRRE ZABALA_AGUSTIN.pdf.

Aliaga, T. (2014). *Retos sociales.* RENIEC. Lima. Perú. Recuperado el 12 de marzo de 2017 de: http://dspace.concytec.gob.pe/bitstream/concytec/106 /1/Retos-Sociales-RENIEC.pdf.

Alvez, C.; Benedetto, M.; Etchart, G.; Luna, L.; Leal, C.; Fernández, M.…Loggio, S. (2015). *Identificación de personas mediante Sistemas Biométricos. Estudio de factibilidad y su implementación en organismos estatales.* Ciencia, Docencia y Tecnología Suplemento. Universidad Nacional de Entre Ríos. Concepción del Uruguay. Entre Ríos. Argentina. Recuperado el 9 de enero de 2017 de: file:///C:/Users/TOSHIBA/Downloads/7-91-1-PB%20(6). pdf.

Anguiano, A.; Chávez, H. y Vásquez, J. (2011). *Sistema de Seguridad activado por medio de la Voz Humana.* Instituto Politécnico Nacional. Escuela Superior de Ingeniería Mecánica y Eléctrica. Unidad Zacatenco. México D.F. Recuperado el 6 de diciembre de 2016 de: http://tesis.ipn.mx/bitstream/ 123456789/1146 4/23.pdf?sequ ence=1.

Asato, J. y Rosales, E. (2011). *La biometría dactilar como una opción para la seguridad informática.* Instituto Tecnológico de Celaya. Celaya. México D.F.

Recuperado el 29 de marzo de 2017 de: http://pistaseducativas.itc.mx/wp-content/uploads/2012/02/3-ASATO-PE-97-44-58.pdf.

Aucanshala, C. y Senteno, S. (2016). *Desarrollo e Implementación de un Sistema de Control Biométrico para la Unidad Educativa Intercultural Bilingüe "Santiago de Guayaquil" de la Ciudad de Guayaquil.* Facultad de Ciencias Matemáticas y Físicas. Universidad de Guayaquil. Guayaquil. Ecuador. Recuperado el 20 de enero de 2017 de: http://repositorio.ug.edu.ec/ bitstream/redug/11638/1/PTGCISC%20993%20%20Aucanshala%20Guashpa% 20Cristian%20Rodolfo.pdf.

Ayala, N. (2015). *Monografía de estudio sobre la aplicación de seguridad biométrica para la identificación de usuarios en entornos web.* Escuela de Ciencias Básicas, Tecnología e Ingeniería. Universidad Nacional Abierta y a Distancia. Tunja. Colombia. Recuperado el 12 de marzo de 2017 de: http://repository.unad.edu.co/bitstream/10596/3743/3/7161218.pdf.

Bouihrouzan, O. (2016). *Seguridad e Inseguridad en los Sistemas Biométricos:Seguridad Vs Privacidad*. Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicaciones. Universidad Politécnica de Madrid. Madrid. España. Recuperado el 31 de diciembre de 2016 de: http://oa.upm.es/43786/1/PFC_OMAR_BOUIHROUZAN_BELHAJ.pdf.

Briceño, C. (2012). *Diseño e Implementación de un Sistema de Reconocimiento de Palabras en un FPGA basado en el algoritmo de LPC*. Facultad de Ingeniería Eléctrica y Electrónica. Universidad Nacional de Ingeniería. Lima. Perú. Recuperado el 10 de diciembre de 2016 de: http://cybertesis.uni.edu. pe/bitstream/uni/2228/1/briceno_ac.pdf.

Cárdenas, J. (2015). *Diseño de la Estrategia de Implementación de un Sistema de Prevención del Fraude en el Sector Financiero, mediante el uso de Biometría Facial y por Voz.* Universidad de Chile. Chile. Recuperado el 6 de

diciembre de 2016 de: http://repositorio.uchile.cl/bitstream/handle/2250/137107/Diseno-de-laestrategia=de-implementacion-de-un-sistema-de-preve ncion-del-fraude.pdf?sequence=1.

Cerame, P. (2014). *Detección automática de voz degradada usando medidas de calidad.* Escuela Politécnica Superior. Universidad Autónoma de Madrid. Madrid. España. Recuperado el 18 de enero de 2017 de: https://repositorio.uam.es/bitstream/handle/10486/661685/ceramelardiespedropfcpdf?sequence=1.

El Comercio. (19 de abril de 2014). Lo suplantaron en el banco y le robaron US $46.500. *El Comercio*. Recuperado el 16 de diciembre de 2016 de: http://elcomercio.pe/sociedad/lima/suplantaron-banco-y-le-robaron-46500-dolares-noticia-1723862.

Escajedo, L. (2015). *Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas.* Departamento de Biotecnología. Facultad de Ciencias. Universidad de Alicante. Alicante. España. Recuperado el 6 de enero de 2017 de: file:///C:/Users/TOSHIBA/Downloads/tesis_escajedo_sanepifanio.pdf.

Gartner. (2016). *Technology Insight for Biometric Authentication.* Analista: Ant Allan. 2016 Gartner, Inc. y/o sus Afiliados. USA. Recuperado el 20 de enero de 2017 de: https://www.gartner.com/doc/3392820/technologyinsight biometricauthentication.

Gómez, L. y Andrés, A. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.2da.edición.* AENOR (Asociación Española de Normalización y Certificación). Madrid. España. Recuperado el 7 de enero de 2017 de: http://s3.amazonaws.com/academia.edu.documents/36974512/NOV_DOC_Tabla_AEN_22994_1.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTPEA&

Expires=1483785586&Signature=ObOUztZJewUesDnysvPkhpeOhBg%3D&responsecontentdisposition=inline%3B%20filename%3DNOV_DOC_Tabla_AEN_22994_1.pdf.

Gonzales, J. (2013). *Sistema de Identificación Biométrica basado en Huella Dactilar mediante Binarización sobre Plataformas Android.* Universidad Carlos III de Madrid www.uc3m.es. España. Recuperado el 6 de diciembre de 2016 de: http://e-archivo.uc3m.es/bitstream/handle/10016/19246/TFG_GONZALEZ_ISABEL_JOSE_%20RAMON.pdf?sequence=1.

Llatas, O. (2015). *El registro biométrico dactilar con el sistema AFIS y el control del delito.* Escuela de posgrado. PUCP. Lima. Perú. Recuperado el 9 de diciembre de 2016 de: file:///C:/Users/TOSHIBA/Downloads/LLATAS_SORALUZ_OSCAR_MABEL_REITRO.pdf.

Loyola, L. (2015). *La Espectrografía de Voces en el Peritaje de Identificación del Hablante.* Facultad de Derecho y Ciencias Políticas. Universidad de Huánuco. Huánuco. Perú. Recuperado el 20 de enero de 2017 de: http://repositorio.udh.edu.pe/bitstream/handle/123456789/217/LOYOLA%20MANTILLA%2c%20LUIS %20TITO.pdf?sequence=1&isAllowed=y.

Masana de Bouffard, J. (2016). *Integración de biometría de voz en un sistema de pago por teléfono: verificación del locutor dependiente del texto.* Escuela Técnica Superior de Ingeniería de Telecomunicaciones de Barcelona. Universidad Politécnica de Cataluña. Cataluña. España. Recuperado el 9 de diciembre de 2016 de: https://upcommons.upc.edu/bitstream/handle/2117/97429/Degree%20thesis%20Judit%20Masana.pdf?sequence=1&isAllowed=.

Mallqui, M. (2015). Consideraciones Generales sobre la Importancia del Derecho Notarial en el Perú, *IUS Revista de Investigación Jurídica, 1*(9).

Recuperado el 20 de enero de 2017 de: file:///C:/Users/TOSHIBA/Downloads/294-482-1-PB.pdf.

Marcos, R. (2015). *Estudio de las normas españolas y estadounidenses de seguridad de la información*. Universidad de Valladolid. Escuela de Ingenierías Industriales. Valladolid. España. Recuperado el 12 de enero de 2017 de: http://uvadoc.uva.es/bitstream/10324/13335/1/TFG-I-244.pdf.

Mejía, J. (2015). *Plan de seguridad informática del departamento de tecnologías de la información y comunicación de la universidad técnica de Babahoyo para mejorar la gestión en la confidencialidad e integridad de la información y disponibilidad de los servicios.* Facultad de Sistemas Mercantiles. Universidad Regional Autónoma de los Andes. Babahoyo. Ecuador. Recuperado el 29 de marzo de 2017 de: http://dspace.uniandes.edu.ec/ bitstream/123456789/732/1/TU AM EIE012-2015.pdf.

Mendoza, G. (2016). *Publicidad Registral y los Datos Personales de los Candidatos Presidenciales.* From the Select Works of Gilberto Mendoza del Maestro. Pontificia Universidad Católica del Perú. Lima. Perú. Recuperado el 20 de enero de 2017 de: file:///C:/Users/TOSHIBA/Downloads/Parthenon %20Publicidad%20Formal_stamped.pdf.

Montenegro, C.; Gaona, E. y Gaona, P. (2012). *Plataforma de seguridad basado en autenticidad de contenidos sobre conjunto de especificaciones SCORM.* Biblioteca Digital Universidad del Valle. Bogotá. Colombia. Recuperado el 29 de marzo de 2017 de: http://hdl.handle.net/10893/3440.

Morán, P. (2016). *Plan de Seguridad Informática en base a parámetros de la norma ISO/IEC 27002 para mejorar la Seguridad de la Información en el Departamento de Tecnologías de Información y Comunicación del Gobierno Autónomo Descentralizado Provincial De Santo Domingo de los Tsáchilas.* UNIANDES. Facultad Sistemas Mercantiles. Carrera de Sistemas. Ecuador. Recuperado el 6 de diciembre de 2016 de:

http://dspace.uniandes.edu.ec/ bitstream/123456789/4222/1/TUSDSIS030-2016.pdf.

Navarro, F. (2014). *El Mundo de los Controles de Acceso.* Universitat Oberta de Cataluya. Cataluya. España. Recuperado el 31 de diciembre de 2016 de: file:///C:/Users/TOSHIBA/Downloads/fnavamaTFG0614memoria.pdf.

Peralta, J. (2015). Nueve años de biometría en el Perú: La fe de identificación en la encrucijada. *IUS Revista del Instituto de Ciencias Jurídicas de Puebla A.C., IX*(36), 275-301. Recuperado el 16 de diciembre de 2016 de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472015 000200275.

Poblete, V. (2014). *Reconocimiento robusto de patrones acústicos basados en el sistema auditivo periférico.* Facultad de Ciencias Físicas y Matemáticas. Departamento de Ingeniería Eléctrica. Universidad de Chile. Chile. Recuperado el 16 de diciembre de 2016 de: file:///C:/Users/TOSHIBA/ Downloads/cf-poblete_vr.pdf.

Ramírez, S. (1999). *Teoría General de Sistemas de Ludwig Von Bertalanffy.* Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades. Universidad Autónoma de México. México D.F. Recuperado el 12 de junio de 2017 de: https://books.google.es/books?hl=es&lr=&id=siofrhfXsOwC&oi=fnd&pg=PA9&dq=Teor%C3%ADa+General+de+Sistemas+de+Karl+Ludwg+von+Bertalanffy,+&ots=urrhwBkyyC&sig=0Sn1fmd2zqYluZuJGKj5pOYy4v=onepage&q=Teor%C3%ADa%20General%20de%20Sistemas%20de%20Karl%20Ludwig%20von%20Bertalanffy%2C&f=false.

RENIEC-DH (2014). La Fiesta de la Biometría. *Dejando Huella. Julio–Agosto 2014*, 8-10. Recuperado el 20 de enero de 2017 de: https://issuu.com/sgrp-gii/docs/dejando_huella_jul_ago_2014_issuu.

Rodrigo, M. y Muñante, W. (2015). *Sistema de Identificación y Clasificación de Inculpados.* UPC. División de Estudios Profesionales para Ejecutivos. Carrera de Ingeniería de Sistemas. Facultad de Ingeniería. Universidad Peruana de Ciencias Aplicadas. Lima. Perú. Recuperado el 9 de diciembre de 2016 de: file:///C:/Users/TOSHIBA/Desktop/T%C3%89SIS%20DE%20BIOMETR%C3%8DA/SISTEMA%20DE%20IDENTIFICACI%C3%93N%20Y%20CLASIFICACI%C3%93N%20DE%20INCULPADOS.pdf.

Rueda, L. (2011). *Mejoras en reconocimiento del habla basadas en mejoras en la parametrización de la voz.* Escuela Politécnica Superior. Universidad Autónoma de Madrid. Madrid. España. Recuperado el 20 de enero de 2017 de: https://repositorio.uam.es/bitstream/handle/10486/6734/39702_20110603LeticiaRueda.pdf?sequence=1.

Ruiz, S. et al. (2016). *Arquitectura Genérica para el Almacenamiento de Datos Biométricos.* Facultad de Ciencias de la Administración. Universidad Nacional de Entre Ríos. Concepción del Uruguay. Entre Ríos. Argentina. Recuperado el 20 de enero de 2017 de: http://sedici.unlp.edu.ar/bitstream/handle/10915/52887/Documento_completo.pdf -PDFA.pdf?sequence=1.

Sánchez, C. (2012). *Aplicaciones de la Biometría a la Seguridad.* Centro de Domótica Integral (CEDINT). Universidad Politécnica de Madrid. Madrid. España. Recuperado el 12 de marzo de 2017 de: http://oa.upm.es/20071/1/INVE_MEM_2012_14306 1.pdf.

Villavicencio, F. (2014). Delitos Informáticos. *IUS ET VERITAS*, *24*(49), 284-304. Recuperado el 28 de enero de 2017 de: file:///C:/Users/TOSHIBA/Downloads/13630-54269-1-PB.pdf.

Anexos

Anexo A
Matriz de Consistencia

TÍTULO: Biometría de voz en la seguridad de la información en las notarías públicas peruanas, 2017.

AUTOR: JORGE LUIS CIENFUEGOS SOLÍS

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES E INDICADORES
PROBLEMA GENERAL: ¿Cómo la biometría de voz mejora el proceso de la seguridad de la información en las notarías públicas peruanas, 2017? **PROBLEMAS ESPECÍFICOS** ¿De qué forma la biometría de voz mejora el grado de fiabilidad en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017? ¿De qué forma la biometría de voz mejora el grado de eficiencia en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017?	**OBJETIVO GENERAL:** Demostrar la forma en que la Biometría de voz mejora el proceso de la seguridad de la información en las notarías públicas peruanas, 2017 **OBJETIVOS ESPECÍFICOS:** Determinar la forma en que la biometría de voz mejora el grado de fiabilidad en el proceso de seguridad de la información en las notarías públicas peruanas, 2017. Determinar la forma en que la biometría de voz mejora el grado de eficiencia en el proceso de seguridad de la información en las notarías públicas peruanas, 2017.	**HIPÓTESIS GENERAL:** Existe una mejora significativa al aplicar la biometría de voz en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017 **HIPÓTESIS ESPECÍFICAS:** La biometría de voz mejora significativamente el grado de fiabilidad en el proceso de seguridad de la información en las notarías públicas peruanas, 2017. La biometría de voz mejora significativamente el grado de eficiencia en el proceso de seguridad de la información en las notarías públicas peruanas, 2017.	**Variable 1: Biometría de Voz** **Dimensiones** / **Indicadores** Reconocimiento: Accesibilidad; Conocimiento Verificación: Usabilidad; Tiempo de respuesta Identificación: Seguridad; Asertividad **Variable 2: Proceso de Seguridad de la Información** **Dimensiones** / **Indicadores** Confidencialidad: Accesibilidad; Conocimiento Integridad: Grado de Fiabilidad; Grado de Eficiencia Disponibilidad: Accesibilidad; Tiempo de respuesta
TIPO Y DISEÑO DE INVESTIGACIÓN	**POBLACIÓN Y MUESTRA**	**TÉCNICAS E INSTRUMENTOS**	**ESTADÍSTICA DESCRIPTIVA E INFERENCIAL**
TIPO: APLICADA Hernández (2014), determina causalidad y sus implicaciones, características que se ajustan a las acciones que se pueden realizar con los planteamientos cuantitativos que se manejan en esta investigación (p.42). **DISEÑO: PRE EXPERIMENTAL** Se utilizará la Distribución t de Student para el análisis inferencial de la variable cuantitativa, discreta y dependiente: Seguridad de la Información.	**POBLACIÓN:** Constituido por los trámites notariales realizados y validados. **POBLACIÓN** / **TRÁMITES** Área Usuaria y Área Técnica de Notarías: 40 **TAMAÑO DE MUESTRA: 40** La muestra se considera del tipo Censal	**Variable 1:Biometría de Voz** **Variable 2:Seguridad de la Información.** Técnica: Observación. Instrumento: Ficha de Observación. Año: 2017 Monitoreo Pre: Abril 2017. Monitoreo Pos: Julio 2017. Ámbito de Aplicación: Lima – Perú. Forma de Administración: Directa	**DESCRIPTIVA:** Mediante Fichas de Observación se recogen datos cuantitativos y se procesan utilizando el software SPSS, teniéndose como resultado el Análisis Descriptivo, el cual se muestra a través de Tablas y Diagramas de Barras. **INFERENCIAL:** Inicialmente haciendo uso del Test de Shapiro - Wilk, se analiza la Normalidad de los Datos. Posteriormente usando la Distribución t de Student, se realiza la Contrastación de Hipótesis de los dos indicadores usados. Para ello se realiza una medición previa de la variable dependiente a ser utilizada antes de la aplicación de la variable independiente (Pre - Test). Luego se efectúa la aplicación de la variable independiente a los sujetos de la muestra obteniéndose una nueva medición de la variable dependiente después de la aplicación de la variable independiente (Post - Test).

Anexo B
Matriz de Operacionalización de Variables

TÌTULO: “Biometría de Voz en la Seguridad de la Información en las Notarías Públicas peruanas, 2017”					
Variable	**Indicador**	**Descripción**	**Instrumento**	**Unidad de medida**	**Fórmula**
Proceso de Seguridad de la Información	**Grado de Fiabilidad en la Seguridad de la Información**	Evaluación del número de errores de identificación en un trámite notarial	Ficha de observación Contador	Unidades numéricas	$$GE = \left[1 - \frac{Te}{Tr}\right] * 100$$ GE: Grado de Fiabilidad (%). Tr: Nro. de trámites realizados y validados. Te: Nro. de trámites realizados y validados con error de identificación.
	Grado de Eficiencia en la Seguridad de la Información	Evaluación del número de consultas externas que se necesitan para un trámite notarial	Ficha de observación Contador	Unidades numéricas	$$GE = \left[1 - \frac{Tc}{Tr}\right] * 100$$ GE: Grado de Eficiencia (%). Tr: Nro. de trámites realizados y validados. Tc: Nro. de trámites realizados y validados con consulta externa.

Anexo C
Instrumentos de Recolección de Datos

Ficha de Observación 1

Medición del indicador Grado de Fiabilidad en la Seguridad de la Información (Pre test)

Investigador:	Cienfuegos Solís Jorge Luis				
Proceso Observado:	Seguridad de la Información				
Pre test					
Nro. Obs.	Fecha de Inicio	Nro. de Trámites realizados y validados que no usan Biometría de Voz	Nro. de Trámites con error de identificación que no usan Biometría de Voz	Grado de Fiabilidad = (1- Nro. de Trámites con error de identificación / Nro. de Trámites realizados y validados) x 100	Grado de Fiabilidad en la Seguridad de la Información (%)
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Medición del indicador Grado de Fiabilidad en la Seguridad de la Información (Post test)

Investigador:	Cienfuegos Solís Jorge Luis				
Proceso Observado:	Seguridad de la Información				
Post test					
Nro. Obs.	Fecha de Inicio	Nro. de Trámites realizados y validados que usan Biometría de Voz	Nro. de Trámites con error de identificación que usan Biometría de Voz	Grado de Fiabilidad = (1- Nro. de Trámites con error de identificación / Nro. de Trámites realizados y validados) x 100	Grado de Fiabilidad en la Seguridad de la Información (%)
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Ficha de Observación 2

Medición del indicador Grado de Eficiencia en la Seguridad de la Información (Pre test)

Investigador:	Cienfuegos Solís Jorge Luis				
Proceso Observado:	Seguridad de la Información				
Pre test					
Nro. Obs.	Fecha de Inicio	Nro. de Trámites realizados y validados que no usan Biometría de Voz	Nro. de Trámites con consulta externa que no usan Biometría de Voz	Grado de Eficiencia = (1- Nro. de Trámites con consulta externa / Nro. de Trámites realizados y validados) x 100	Grado de Eficiencia en la Seguridad de la Información (%)
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Medición del indicador Grado de Eficiencia en la Seguridad de la Información (Post test)

Investigador:	Cienfuegos Solís Jorge Luis				
Proceso Observado:	Seguridad de la Información				
Post test					
Nro. Obs.	Fecha de Inicio	Nro. de Trámites realizados y validados que usan Biometría de Voz	Nro. de Trámites con consulta externa que usan Biometría de Voz	Grado de Eficiencia = (1- Nro. de Trámites con consulta externa / Nro. de Trámites realizados y validados) x 100	Grado de Eficiencia en la Seguridad de la Información (%)
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Anexo D
Certificados de Validez de Contenido del Instrumento

Validación del Experto

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE CONOCIMIENTOS SOBRE:
"SEGURIDAD DE LA INFORMACIÓN" (Pre test y Post Test)

N°	DIMENSIONES / INDICADORES	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
		Si	No	Si	No	Si	No	
1	**INDICADOR GRADO DE FIABILIDAD EN LA SEGURIDAD DE LA INFORMACIÓN** GF = [1 - (Te / Tr)] * 100 GF = Grado de Fiabilidad (%). Tr = Nro. de trámites realizados y validados. Te = Nro. de trámites realizados y validados con error de identificación.	X		X		X		
2	**INDICADOR GRADO DE EFICIENCIA EN LA SEGURIDAD DE LA INFORMACIÓN** GE = [1 - (Tc / Tr)] * 100 GE = Grado de Eficiencia (%). Tr = Nro. de trámites realizados y validados. Tc = Nro. de trámites realizados y validados con consulta externa.	X		X		X		

Observaciones (precisar si hay suficiencia): SUFICIENTE

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ] 15 de JUNIO del 2017

Apellidos y nombres del juez evaluador: VISURRAGA AGUERO JOEL **DNI:** 10192315

Especialidad del evaluador: INGENIERIA DE SISTEMAS **Firma:**

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

Mag. José Martín Visurraga Agüero
DOCENTE
Escuela de Postgrado - UCV

Anexo E
Constancia de autorización de la Investigación

CONSTANCIA

La Notaría Mendoza Vásquez hace constar que el Bachiller Jorge Luis Cienfuegos Solís, identificado con DNI 09250121, estudiante del programa de Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información de la Universidad César Vallejo, en la sede Lima Norte, promoción 2016, ha realizado la toma de datos necesarios, mediante una encuesta realizada en dicha Notaría, pará poder realizar su investigación " Biometría de voz en la Seguridad de la Información en las Notarías Públicas Peruanas, 2017".

Se expide la presente constancia para los fines pertinentes.

Santiago de Surco, 21 de agosto de 2017

NOTARIA MENDOZA VASQUEZ
Av. Benavides Nº 4982 - Surco
Telefono: 644-0010
21 AGO 2017
RECIBIDO
HORA 15:30 FIRMA

Anexo F

Base de Datos – Observación

Base de Datos - Observación

		Pre Test					Post Test				
		Trámites Notariales									
		Que no usan Biometría de Voz					Que usan Biometría de Voz				
Registro	Fecha	Realizados y validados	Con error de identificación	Grado de Fiabilidad	Con consulta externa	Grado de Eficiencia	Realizados y validados	Con error de identificación	Grado de Fiabilidad	Con consulta externa	Grado de Eficiencia
1	04/04/2017	50	11	0.78	15	0.70	45	2	0.96	3	0.93
2	10/04/2017	45	10	0.78	18	0.60	48	1	0.98	2	0.96
3	11/04/2017	48	19	0.60	18	0.63	50	3	0.94	4	0.92
4	18/04/2017	49	19	0.61	14	0.71	53	3	0.94	4	0.92
5	25/04/2017	53	12	0.77	20	0.62	52	2	0.96	3	0.94
6	26/04/2017	45	8	0.82	18	0.60	49	4	0.92	5	0.90
7	09/05/2017	38	10	0.74	9	0.76	51	0	1.00	1	0.98
8	16/05/2017	49	11	0.78	16	0.67	52	0	1.00	1	0.98
9	23/05/2017	52	16	0.69	15	0.71	49	2	0.96	3	0.94
10	30/05/2017	51	16	0.69	19	0.63	47	2	0.96	3	0.94

Anexo G

Artículo de Investigación

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Biometría de voz y seguridad de la información en Notarías Públicas 2017

Br. Jorge Luis Cienfuegos Solís

Escuela de Posgrado
Universidad César Vallejo Filial Lima

Resumen

El objetivo principal de esta investigación fue demostrar en que forma la Biometría de Voz mejora el proceso de la Seguridad de la Información. Para ello se trabajó como herramienta tecnológica o variable independiente a la Biometría de Voz y al proceso o variable dependiente donde se aplica la herramienta tecnológica, la Seguridad de la Información. Así mismo para medir cuantitativamente la mejora que ofrece la Biometría de Voz, se utilizaron los indicadores de medición: grado de fiabilidad y grado de eficiencia. Además haciendo uso de Tablas y Gráficas provenientes del Software de IBM SPSS, que sirvió de herramienta para el uso de coeficientes estadísticos, permitiendo averiguar la mejora existente que se produce cuando se realiza la aplicación de la Biometría de Voz en el proceso de la Seguridad de la Información. Lo que trajo como conclusión más importante: que la aplicación de la biometría de voz no solo mejore el proceso de la seguridad de la información, si no que además su aplicación permite concientizar en la población peruana lo que se entiende por seguridad de la información y lo que se entiende por fiabilidad y eficiencia en el tratamiento de dicha información.

Palabras clave: *Biometría de Voz, Seguridad de la Información, Proceso.*

Abstract

The main objective of this research was to demonstrate how Voice Biometrics improves the Information Security process. To this end, we worked as a technological tool or variable independent of Voice Biometrics and the dependent process or variable where the technological tool, Information Security, is applied. Likewise, to quantitatively measure the improvement offered by Voice Biometrics, the measurement indicators were used: degree of reliability and degree of efficiency. In addition, using Tables and Graphs from the IBM SPSS Software, which served as a tool for the use of statistical coefficients, allowing to find out the existing improvement that occurs when the application of Voice Biometrics is made in the process of Security of information. What came as the most important conclusion: that the application of voice biometrics not only improves the process of information security, but also that its application allows awareness in the

Peruvian population what is meant by information security and what is meant by reliability and efficiency in the processing of said information.

Keywords: *Voice Biometrics, Information Security, Process.*

Introducción

La investigación persigue demostrar la mejora que se consigue con la Biometría de voz en el proceso de seguridad de la información en las notarías públicas peruanas, 2017. La investigación está presentada en nueve secciones, donde: la primera sección corresponde al resumen de la investigación con su correspondiente traducción al inglés, la segunda sección correspondiente a la introducción, describe el problema en estudio y abarca el primer contacto teórico de la investigación, la tercera sección detalla los antecedentes del problema, donde se ve la realidad problemática, en los ámbitos internacional y nacional. La cuarta sección ve concretamente el problema general y los problemas específicos de la investigación. Los objetivos tanto general como específicos se tratan en la quinta sección. En la sexta sección se trata todo lo relacionado al método utilizado, describe el tipo de investigación, diseño de investigación, la definición conceptual y operacional de las variables a usar, el manejo de la población, muestra y muestreo, las técnicas e instrumentos de recolección de datos (su validez y confiabilidad), los métodos de análisis de datos y los aspectos éticos. Los resultados obtenidos se consideran en la séptima sección. En la octava sección se exponen la discusión de la investigación, además de las conclusiones y las recomendaciones. La novena sección detalla las referencias bibliográficas usadas en la presente investigación.

Antecedentes del problema

Según Escajedo (2015) en su Investigación “Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas” realizado en la Universidad de Alicante de España, cuyo propósito fue estudiar la situación en que se encuentra los sistemas biométricos contemporáneos. Por otro lado Cárdenas (2015) en su Tesis “Diseño de la Estrategia de Implementación de un Sistema de Prevención del Fraude en el Sector Financiero, mediante el uso de

Biometría Facial y por Voz" realizado en el Sistema Nacional de Comunicaciones Financieras de Chile, cuyo propósito fue elegir la mejor tecnología de biometría facial y por voz que se acomoden mejor a las condiciones técnicas, de seguridad, legal y de negocio al sector financiero de Chile. Así mismo, Anguiano, Chávez & Vásquez (2011) en su Investigación "Sistema de Seguridad activado por medio de la Voz Humana" realizado en la Escuela Superior de Ingeniería Mecánica del campus Zacatenco - México D.F., cuyo objetivo fue diseñar un sistema de seguridad basado en el reconocimiento de voz humana, para autenticar a una persona, llegaron a la conclusión que el tono fundamental de una persona es una característica única que se presenta y que en pocos casos, diferentes personas tendrán el mismo tono fundamental, por lo que nos permite identificar la voz de cada individuo a partir de esta característica. De igual forma, Aguilar (2016) en su Investigación "Implementación de un modelo simplificado de firma digital basado en la tecnología PKI y la innovación por protocolos caso de estudio: Municipalidad de Miraflores" realizado en la Municipalidad de Miraflores – Lima, cuyo objetivo principal fue la de implementar un modelo simplificado de firma digital basado en tecnología PKI y la invocación por protocolos dentro de la Municipalidad de Miraflores. desarrolla una tesis que se encuentra involucrada en el ámbito de la seguridad de la información y permite rescatar puntos de vista útiles para lel artículo. Finalmente se puede citar a Loyola (2015) en su Investigación "La Espectrografía de Voces en el Peritaje de Identificación del Hablante" realizado en la Universidad de Huánuco. Perú mediante un estudio descriptivo y explicativo de tipo no experimental con una población de 30 profesionales encargados de delitos de corrupción de funcionarios, cuyo objetivo principal fue el demostrar que el uso de espectrogramas de las voces si influyen en la identificación positiva del locutor y por consiguiente mejoran la calidad y eficacia probatoria de los dictámenes e informes periciales. Todos estos problemas expuestos, diferentes por la locación donde se realizaron, tienen en común el uso de la Biometría como mejora de la Seguridad de la Información.

Problema

El problema se concentra en el hecho de que en nuestra realidad peruana, la forma extendida de evitar la suplantación de identidad de alguien es en primera instancia disminuida con la verificación del Documento Nacional de Identidad. Y

cuando se pretende aumentar el grado de verificación se hace uso de la Biometría Dactilar, habiéndose convertido en la actualidad como el medio más seguro y extendido no solo para evitar la suplantación de la identidad sino para evitar poner en peligro la seguridad de la información de alguien o algo. Sin embargo todos sabemos la forma tan fácil de falsificar un Documento Nacional de Identidad así como el uso del látex como generador de huellas dactilares postizas. Por estas razones es necesario el planteamiento masivo y no sectario de una nueva herramienta tecnológica en el Perú.

Objetivo

Demostrar la forma en que la biometría de voz mejora el proceso de la seguridad de la información en las notarías públicas peruanas, 2017. Específicamente, determinar la forma en que la biometría de voz mejora el grado de fiabilidad en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017. De ifual forma, determinar la forma en que la biometría de voz mejora el grado de eficiencia en el proceso de la seguridad de la información en las notarías públicas peruanas, 2017.

Método

La investigación es del tipo aplicada con un diseño de estudio pre-experimental. La muestra seleccionada presenta las mismas características de la población. Es decir de una población de 40 trámites notariales: ser aleatoria y suficiente ya que cada elemento del conjunto poblacional tiene la misma probabilidad de ser elegidos al azar, a la vez es homogénea y representativa del resto de la población por tener las mismas características que ella. De una población de 40 trámites notariales y con una precisión de porcentaje máximo aceptable de error del 5% se utilizó la técnica de la muestra censal para determinar el tamaño de muestra, resultando el número de 40 trámites para los dos indicadores seleccionados para el análisis estadístico del estudio realizado.

Dentro de las características del instrumento usado, en este caso Ficha de observación, se contempla: el autor, el proceso observado, la fecha de inicio o fecha de observación, el objetivo de la ficha técnica es decir la medición del indicador, el número de datos a recolectar que son 40 observaciones, lo

observado vale decir: el número de trámites notariales realizados y validados, el número de trámites notariales realizados. El modo de aplicación de esta Ficha de Observación corresponde al tipo directa. El contenido del instrumento Ficha de observación fue validado a través de “Juicio de experto”.

El procedimiento seguido con la Ficha de Observación, comienza con la recolección de datos cuantitativos a través de dicha Ficha, para que una vez que son recogidos sean procesados utilizando el Software IBM SPSS, teniéndose como resultado el Análisis Descriptivo, el cual se muestra a través de Tablas y Diagramas de Barras. El Análisis Inferencial comienza con el uso del Test de Shapiro - Wilk, para poder analizar la normalidad de los datos. Luego se usa la Distribución t de Student para el análisis inferencial de la variable cuantitativa, discreta y dependiente: Seguridad de la Información.

Resultados

La investigación expone resultados que permiten garantizar que la biometría de voz sirve como instrumento adicional a los ya existentes de mejora en el tratamiento y seguridad en la información en las notarías públicas peruanas, ya que proporciona un aumento en la eficiencia a la hora de manipular datos, mostrando a su vez un grado de fiabilidad mejorado al momento de usarse, confirmando así que la biometría de voz para el proceso seguridad de la información incrementa el grado de fiabilidad en un 32.50%, así mismo se observa que el grado de eficiencia logra incrementarse en un 41.93%. De los resultados obtenidos se puede concluir que la biometría de voz permitió la mejora del proceso seguridad de la información. Se puede finalmente afirmar que la implementación de la herramienta biometría de voz en el proceso seguridad de la información en las notarías públicas peruanas es algo que debe realizarse.

Discusión

El grado de fiabilidad para el proceso seguridad de la información, en la evaluación Pre-Test nos proporcionó un 72.60 y con la aplicación de biometría de voz se elevó a 96.20; indicándome con estos resultados un incremento de 23.60, que me permite asegurar que con la aplicación de la biometría de voz se obtuvo un aumento de 32.50% en el grado de fiabilidad en el proceso seguridad de la

información. Si se compara este resultado con el obtenido por Llatas (2015) en su inestigación “El registro biométrico dactilar con el sistema AFIS y el control del delito”, se apreciará los grandes niveles de similitud en cuanto a resultados.

Se puede concluir después de haber obtenidos valores tan favorables en el aspecto de fiabilidad y eficiencia al implementar la biometría de voz, se puede concluir que su uso no se lleva a cabo aun casualmente por 2 factores que se agudizan ante la falta de divulgación de los mismos. Estos son: la falta de interés por la poca confianza que se le brinda a la herramienta tecnológica, situación que se desploma con la medición Post Test del grado de fiabilidad obtenido y la creencia del alto tiempo de retorno de la inversión que llevaría el implementar la herramienta Biometría de voz, situación que igualmente pierde sustento cuando se observa el valor obtenido como Post Test en el grado de eficiencia.

Se recomienda realizar una combinación de verificación de rasgos biométricos, usando el actual patrón biométrico dactilográfico con el patrón biométrico de voz, lo que le da una mayor potencia al proceso de seguridad de la información y así no se estaría cambiando un mecanismo de seguridad por otro, sino más bien se estaría repotenciando el proceso de seguridad de la información con la implementación de la biometría de voz.

Referencias

Aguilar, G. (2016). *Implementación de un modelo simplificado de firma digital basado en la tecnología PKI y la innovación por protocolos caso de estudio: Municipalidad de Miraflores.* Facultad de Ingeniería de Sistemas e Informática. E.A.P. Ingeniería de Sistemas. UNMSM. Lima. Perú. Recuperado el 9 de diciembre de 2016 de: http://cybertesis.unmsm.edu.pe /bitstream/cybertesis/4993/1/Aguilar_ag.pdf.

Aliaga, T. (2014). *Retos sociales.* RENIEC. Lima. Perú. Recuperado el 12 de marzo de 2017 de: http://dspace.concytec.gob.pe/bitstream/concytec/106 /1/Retos-Sociales-RENIEC.pdf.

Anguiano, A.; Chávez, H. y Vásquez, J. (2011). *Sistema de Seguridad activado por medio de la Voz Humana.* Instituto Politécnico Nacional. Escuela Superior de Ingeniería Mecánica y Eléctrica. Unidad Zacatenco. México

D.F. Recuperado el 6 de diciembre de 2016 de: http://tesis.ipn.mx/bitstream/ 123456789/1146 4/23.pdf?sequ ence=1.

Briceño, C. (2012). *Diseño e Implementación de un Sistema de Reconocimiento de Palabras en un FPGA basado en el algoritmo de LPC*. Facultad de Ingeniería Eléctrica y Electrónica. Universidad Nacional de Ingeniería. Lima. Perú. Recuperado el 10 de diciembre de 2016 de: http://cybertesis.uni.edu. pe/bitstream/uni/2228/1/briceno_ac.pdf.

Cerame, P. (2014). *Detección automática de voz degradada usando medidas de calidad.* Escuela Politécnica Superior. Universidad Autónoma de Madrid. Madrid. España. Recuperado el 18 de enero de 2017 de: https://repositorio.uam.es/bitstream/handle/10486/661685/ceramelardiespe dropfcpdf?sequence=1.

Escajedo, L. (2015). *Reconocimiento e Identificación de las personas mediante Biometrías estáticas y dinámicas.* Departamento de Biotecnología. Facultad de Ciencias. Universidad de Alicante. Alicante. España. Recuperado el 6 de enero de 2017 de: file:///C:/Users/TOSHIBA/Downloads/tesis_escajedo_ sanepifanio.pdf.

Loyola, L. (2015). *La Espectrografía de Voces en el Peritaje de Identificación del Hablante.* Facultad de Derecho y Ciencias Políticas. Universidad de Huánuco. Huánuco. Perú. Recuperado el 20 de enero de 2017 de: http://repositorio.udh.edu.pe/bitstream/handle/123456789/217/LOYOLA%20 MANTILLA%2c%20LUIS %20TITO.pdf?sequence=1&isAllowed=y.

Mallqui, M. (2015). Consideraciones Generales sobre la Importancia del Derecho Notarial en el Perú, *IUS Revista de Investigación Jurídica, 1*(9). Recuperado el 20 de enero de 2017 de: file:///C:/Users/TOSHIBA/Downloads/294-482-1-PB.pdf.

Navarro F. J. (2014). *El Mundo de los Controles de Acceso.* Universitat Oberta de Cataluya. Cataluya. España. Recuperado el 31 de diciembre de 2016 de: file:///C:/Users/TOSHIBA/Downloads/fnavamaTFG0614memoria.pdf.

Villavicencio, F. (2014). Delitos Informáticos. *IUS ET VERITAS*, *24*(49), 284-304. Recuperado el 28 de enero de 2017 de: file:///C:/Users/TOSHIBA/ Downloads /13630-54269-1-PB.pdf.