REVISTA TIA

Tecnología, Investigación y Academia -Red Avanzada – RITA
Publicación Facultad de Ingeniería y Red de Investigaciones de Tecnología

Identificación Biométrica en empresas de Bogotá Beneficios y riesgos

Biometric identification in companies in Bogota Benefits and risks

Celis-Baracaldo, Maritza [1]. Castellanos-Rodríguez, John Fredy [2].

Citar este documento:

Celis-Baracaldo, Maritza. Castellanos-Rodríguez, John Fredy. Identificación Biométrica en empresas de Bogotá Beneficios y riesgos. Revista Tecnol.Investig.Academia TIA, ISSN: 2344-8288, 8 (2), pp. 74-89. Bogotá-Colombia.

[1] Ingeniero de Sistemas, maritzabaracaldo14@gmail.com, Bogotá-Colombia.

[2] Ingeniero de Telemática, yofreca@gmail.com, Bogotá-Colombia

Vol. 8 No. 2
Fecha de aceptación: abril 2021
ISSN: 2344 8288
Artículo de revisión
Fecha de recepción: julio 2020

Resumen

Hoy en día con las nuevas tecnologías, las empresas se han interesado en herramientas que les permitan mantener y acceder de forma segura a la información, esto debido a los nuevos modelos de negocio y modalidades de trabajo que requieren la comodidad y facilidad para el manejo de estos datos. En este artículo nos centraremos en la descripción de los diferentes métodos de implementación biométrica, sus beneficios y riesgos y la aceptación que ha tenido en las organizaciones como estrategia de seguridad.

Palabras Clave: Reconocimiento Biométrico, Sistema Biométrico, Reconocimiento facial, Huella Dactilar.

Abstract

Nowadays with new technologies, companies have been interested in tools that allow them to maintain and access information securely, due to the new business models and work modalities that require the comfort and ease of handling these dates. In this article, we will focus on the description of the different methods of biometric implementation, their benefits and risks and the acceptance that they have had in organizations as a security strategy.

Key Words: Biometric Recognition, Biometric system, Face Recognition, Fingerprint

I. Introducción

Desde siempre los seres humanos se han identificado con sus semejantes a través de sus rasgos físicos y biológicos. Hoy en día la tecnología nos permite adquirir, almacenar y contrastar la información biométrica de los individuos y usarla para la identificación y autenticación de estos. En el mundo actual donde la presencia virtual y la huella digital cada vez es más amplia, se requiere de métodos sofisticados que brinden seguridad y confiabilidad, bajo esta necesidad ha tomado protagonismo los sistemas de reconocimiento biométrico, sin embargo, esta tecnología aún en maduración es susceptible a ataques de presentación [1], además de los cuestionamientos éticos y los requerimientos de protección a la privacidad.

II. CONTENIDO

a. Biometría

La biometría cubre una variedad de tecnologías en las que se utilizan atributos identificables únicos de las personas para la identificación y autenticación. Estos incluyen (pero no se limitan a) la huella digital, huella del iris, mano, cara, voz, marcha o firma de una persona, que se puede usar para validar la identidad de las personas que buscan controlar el acceso a computadoras, líneas aéreas, bases de datos y otras áreas que puedan necesitar un acceso restringido [1].

b. Selección de una característica biométrica

Cualquier característica fisiológica y/o conductual humana puede ser utilizada como una característica biométrica siempre que satisfaga los siguientes requisitos [2]:

- Universalidad: cada persona debe tener la característica.
- Distinción: dos personas deben ser lo suficientemente diferente en términos de la característica.
- Permanencia: la característica debe ser suficientemente invariante (con respecto al criterio de coincidencia) sobre un período de tiempo.
- la característica se puede medir cuantitativamente.
- Coleccionismo: Debe ser fácilmente obtenible.
- Rendimiento: El rasgo deberá ayudar a encontrar la precisión deseada.
- Aceptabilidad: El rasgo debe ser tal que los individuos permitan voluntariamente el uso de este rasgo como identificador.
- Circunvención: La facilidad con que es posible imitar un rasgo de un individuo [3].

c. Tecnologías Biométricas fisiológicas

Huella Dactilar

La identificación basada en huella dactilar es la más antigua de las técnicas biométricas y ha sido utilizada en un gran número de aplicaciones debido a que se considera que las huellas dactilares son únicas e inalterables. Es el rasgo biométrico más utilizado para autenticación. Se han desarrollado una amplia gama de tecnologías de captura, con distintas características de funcionamiento. Asimismo, tiene como ventajas su alta tasa de precisión y su facilidad de uso [4].

Existen dos tipos de técnicas de búsqueda de coincidencias entre muestras de huella dactilar, una es basada en minucias y la otra basada en correlación:

- *Basadas en minucias*, esta técnica basa su mecanismo de autenticación en las «minucias», es decir, en determinadas formas fácilmente identificables existentes en la huella dactilar. Así, se registra el tipo de minucia y su posición dentro de la huella, estableciendo una serie de mediciones. De esta forma, el modelo o plantilla correspondiente a cada usuario es un esquema en el que se indican las minucias que se han de detectar [Ilustración 1], su posición y las distancias que separan unas de otras [4].

Ilustración 1. Minucias de Huella Dactilar [4].

No obstante, existen algunas dificultades asociadas a este método. Por un lado, no es sencillo extraer de forma precisa las mencionadas minucias cuando la calidad de la muestra no es buena. Por otro lado, no se tiene en cuenta el patrón global de crestas y surcos [4].

- *Basadas en correlación*, mediante la utilización de esta técnica se analiza el patrón global [Ilustración 2] seguido por la huella dactilar, es decir, el esquema general del conjunto de la huella en lugar de las minucias.

Esta técnica requiere un registro preciso, pero su principal inconveniente es que se ve afectada por la traslación y la rotación de la imagen.

Ilustración 2. Patrones de Huella Dactilar [4].

Reconocimiento Facial

El reconocimiento facial es una técnica mediante la cual se reconoce a una persona a partir de una imagen o fotografía. Para ello, se utilizan programas de cálculo que analizan imágenes de rostros humanos. Entre los aspectos clave empleados para la comparación se encuentran mediciones como la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula [Ilustración 3] [4].

Ilustración 3. Patrones de Reconocimiento Facial [5].

A diferencia de otros sistemas biométricos, el reconocimiento facial puede ser utilizado para la vigilancia general, habitualmente mediante cámaras de video. Mejoras en los sistemas de reconocimiento facial han podido discernir entre personas reales y fotografías, sin embargo, cualquier persona puede modificar visualmente su cara de manera sencilla, como por ejemplo utilizando unas gafas de sol o dejándose crecer la barba [4].

Asimismo, debe considerarse que el rostro de las personas varía con la edad. Existen soluciones de software que utilizan esta tecnología para identificación de usuarios en dispositivos móviles y portátiles [4].

- **Oportunidades de reconocimiento facial***,* al igual que con todas las nuevas tecnologías, los usos del reconocimiento facial se multiplican de manera predecible y sorprendente. Pero cada vez está más claro que muchos de estos usos han creado muchos beneficios nuevos y positivos para las personas de todo el mundo [5].

Es sorprendente revisar la amplitud de esta innovación. La policía de Nueva Delhi recientemente probó la tecnología de reconocimiento facial e identificó a casi 3.000 niños desaparecidos en cuatro días. Los historiadores en los Estados Unidos han utilizado la tecnología para identificar los retratos de soldados desconocidos en fotografías de la Guerra Civil tomadas en la década de 1860. Los investigadores utilizaron con éxito el software de reconocimiento facial para diagnosticar una enfermedad genética rara en africanos, asiáticos y latinoamericanos. Y en octubre, el National Australia Bank diseñó una prueba de concepto para permitir a los clientes retirar dinero de un cajero automático mediante reconocimiento facial y un PIN [5].

Reconocimiento de Iris

Utiliza las características del iris humano con el fin de verificar la identidad de un individuo. Los patrones de iris vienen marcados desde el nacimiento y rara vez cambian. Son extremadamente complejos, contienen una gran cantidad de información y tienen más de 200 propiedades únicas [4].

El escaneado del iris se lleva a cabo con una cámara de infrarrojos especializada situada por lo general muy cerca de la persona que ilumina el ojo realizando una fotografía de alta resolución [Ilustración 4]. Este proceso dura sólo uno o dos segundos y proporciona los detalles del iris que se localizan, registran y almacenan para realizar futuras verificaciones [4].

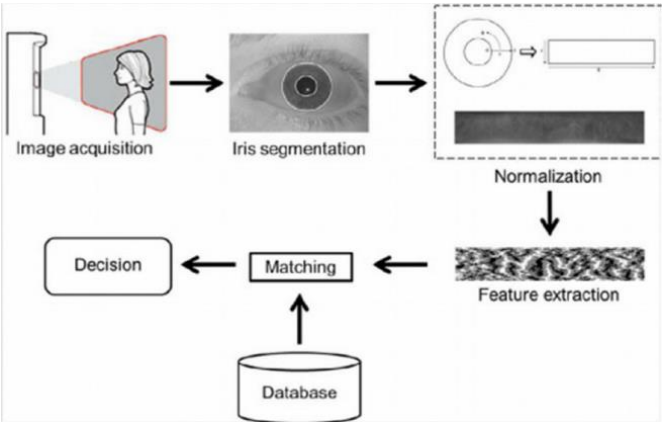

Ilustración 4. Proceso Reconocimiento de Iris [6].

- **Oportunidades de reconocimiento de Iris***:* Varios rasgos del iris que lo convierten en un biométrico muy notable en comparación con otros rasgos biométricos son [6]:

- Incluso los gemelos idénticos tienen iris únicos.
- Un iris posee más de 266 grados de libertad.
- Las huellas digitales pueden ser alteradas con el tiempo, pero el iris está altamente protegido dentro de los párpados y es presumiblemente menos susceptible al daño.
- La degeneración del iris con el envejecimiento no tiene lugar.
- Las gafas o lentes de contacto no tendrán ningún efecto sobre el reconocimiento y la autenticación del iris.

Reconocimiento Vascular

En la biometría vascular se extrae el patrón biométrico a partir de la geometría del árbol de venas del dedo (o de las muñecas). A diferencia de la huella dactilar el patrón biométrico es interno, por esta razón no deja rastro y sólo se puede conseguir en presencia de la persona. Es por tanto muy difícil el robo de identidad [4].

Debido a estas características es especialmente indicado para entornos de alta seguridad, así como en situaciones en que la superficie del dedo pueda estar en mal estado, erosionada o poco limpia [4].

Cómo funciona: El equipo emite luz en infrarrojo. La hemoglobina de las venas absorbe la luz creando una imagen estándar de las venas, el cual es reflejado nuevamente y capturado por el sensor. La imagen es almacenada en el banco de datos, para ser comparada cuando el usuario vuelva a colocar su mano en el lector [7].

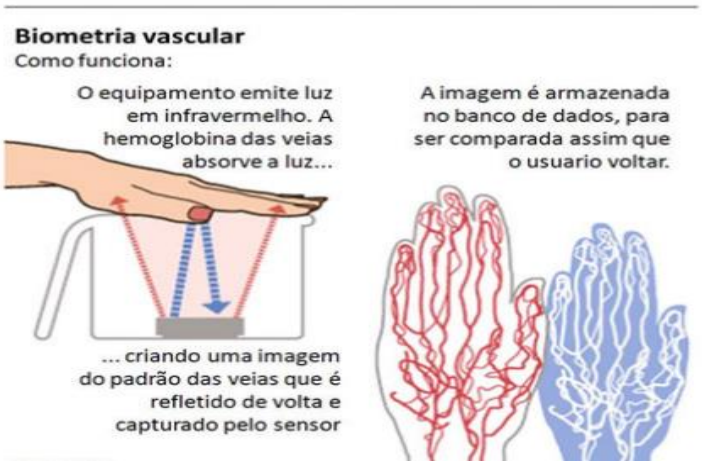

Ilustración 5. Proceso Reconocimiento Vascular [7].

El formato de las venas es capturado a través del principio de la Transmitancia en la imagen, un proceso de diferencia de absorción de haces de luz del espectro infrarrojo (NIR – Near Infrarred y FIR - FarInfrarred),

similar a la utilizada por las cámaras de circuito cerrado de televisión para su visualización en ambientes sin luz visible [7].

Debido a la composición sanguínea ferrosa, la hemoglobina presente en las venas y los capilares de la capa subcutánea absorbe más espectro infrarrojo que los tejidos musculares del cuerpo, y es precisamente ahí que tienen la diferencia de absorción, de la Transmitancia [7]. Por lo tanto, un sensor que detecta sólo el espectro infrarrojo puede diferenciar lo que es tejido muscular y lo que son las venas y capilares. Este sensor puede ser una cámara CCD con un filtro de luz visible [7].

d. Beneficios de la implementación Biométrica

La tecnología biométrica es muy útil para la verificación de identidad en una variedad de organizaciones gubernamentales, bancos e instituciones financieras y áreas de alta seguridad. Los sistemas biométricos son capaces de reconocer a las personas de manera rápida, consistente y confiable. Este ítem está basado en la referencia [8].

> " Una de las principales ventajas asociadas con la tecnología biométrica es la alta precisión de identificación individual. La biometría se basa en el uso de rasgos físicos únicos, como una huella digital, un patrón de iris o características faciales, lo que convierte a la tecnología biométrica en una técnica muy precisa para autenticar a los usuarios finales. La precisión superior es la razón por la cual muchas empresas utilizan la biometría para fines de seguridad. Como las características biométricas no se pueden conjeturar ni robar, los sistemas biométricos presentan un nivel de seguridad superior al de los medios habituales de autenticación.
>
> Biometric technology is less exposed to damage and sudden changes. The behavioral and physical elements accessed for biometric verification like iris/retina, voice, pulse, DNA, vein, etc. are less in danger to damage and sudden changes. Otra ventaja vital de la tecnología biométrica es que consume menos tiempo, es confiable, fácil de usar, difícil de falsificar, requiere capacitación insignificante, es económica y accede a las características de reconocimiento distintivas de las personas, lo que resulta en una verificación precisa. La tecnología biométrica se puede utilizar en muchas industrias como la salud, la identificación civil, las empresas, las escuelas, las industrias financieras, etc. Muchos países ya han utilizado la tecnología biométrica para el registro de votantes, la identificación nacional, los proyectos nacionales de salud o pasaporte electrónico.

La tecnología biométrica resulta ser la mejor y más adecuada solución para la identificación segura de transacciones móviles. La tecnología biométrica se puede utilizar para evitar el acceso ilícito a cajeros automáticos, teléfonos celulares, tarjetas inteligentes, computadoras de escritorio, estaciones de trabajo y redes de computadoras. Las contraseñas y los PIN son fáciles de olvidar, lo que hace que las personas los anoten y, en consecuencia, pueden ser robados y, a veces, pirateados. Con la tecnología biométrica, las huellas digitales no se perderán y nadie podrá obtenerlas ni copiarlas con el objetivo de obtener acceso ilegalmente"

e. Riesgos de la implementación Biométrica

La tecnología biométrica, como cualquier tecnología desarrollada por el hombre es susceptible a ataques, un sistema de autenticación biométrica [14] "se define como un conjunto de componentes de hardware, procesos, algoritmos, estructuras de datos, y bases de datos que cumplen interna y / o externa comunicación entre los elementos para el propósito de la autenticación biométrica."

Cada uno de estos elementos es susceptible de ser atacado de diversas maneras y se debe realizar una adecuada evaluación de los riesgos para mitigar y minimizar la posibilidad de que dichas amenazas se materialicen.

los ataques a la seguridad biométrica se pueden clasificar en 3 categorías [14]:

1. Ataques de sensores (copia, falsificación, ataques de similitud)
2. Comunicación de datos ataques (ataques de repetición)
3. Ataques de bases de datos (ataques de integridad)

f. Marco legal de la biometría en Colombia

Los datos biométricos figura dentro de la protección de datos personales definida en la Ley de habeas data, así mismo existen aspectos legales que deben tenerse en cuenta con la finalidad de obtener cualquier tipo de datos biométricos, por lo cual se hace necesario comprender cuál es el tratamiento de datos referido a la biometría, teniendo en cuenta que en Colombia no existe una norma que regule el uso recolección y almacenamiento de datos biométricos; sin embargo el uso de datos biométricos se ceñirá por lo concerniente al tratamiento de datos personales, además vale la pena resaltar que existe regulación sectorial de datos biométricos concernientes con la firma electrónica y la verificación de la huella dactilar por medios electrónicos.

Constitución política de 1991

En principio es relevante precisar que a través del artículo 15 de la Constitución Nacional se consagra el derecho a la intimidad como un derecho de carácter fundamental, así mismo, ha sido diversa la jurisprudencia que define que el derecho al hábeas data es una garantía del derecho a la intimidad como las Sentencias C-1011-08, C-640-10, C-748-11 y T- 077/18 entre otras; así pues, el habeas data se consagra en el artículo 15 en la mención del derecho de todas las personas de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

Ley 527 de 1999

La Ley 527 de 1999 que "define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se dictan otras disposiciones", constituye el marco jurídico del comercio electrónico en Colombia, en el sector público y privado; a través de esta ley se desarrolla la identificación electrónica con la certificación de la firma digital considerada como firma electrónica.

Decreto 2364 de 2012

El Decreto 2364 de 2012 mediante el cual se reglamenta la Ley 567 de 1999, en lo referente a la firma electrónica, tuvo la finalidad de impulsar el comercio electrónico a través de la firma electrónica como un medio de identificación flexible y con base en el documento Conpes 3620 de 2009 que no solo plantea la protección de datos personales, sino que recomendó el uso de la firma electrónica para promover su uso no solo en el sector económico y financiero.

Ley Estatutaria de habeas data

Mediante la Ley 1581 de 2012 se pretendió regular la protección de datos personales en Colombia en la cual se compilaron los criterios y principios desarrollados por la jurisprudencia de la Corte Constitucional, así pues el proyecto de ley estatutaria fue objeto de estudio de constitucionalidad mediante Sentencia C-748-11 de 6 de octubre de 2011 del Magistrado Ponente Dr. Jorge Ignacio Pretelt Chaljub, en dicha sentencia la Corte Constitucional hizo referencia al origen histórico y el alcance del derecho fundamental al habeas data y después de una revisión integral del texto se declaró exequible el proyecto de ley salvo los artículos 29, 30 y 31 del proyecto de ley que se declararon inexequibles por vicios de procedimiento en su aprobación.

Implementaciones Nacionales de Tecnología Biométrica

BIOMIG Migración Biométrica [9]

Es el procedimiento voluntario, por el cual Migración Colombia, recolecta los datos biográficos y biométricas por iris, para permitir su autenticación a través de los pasillos migratorios y facilitar en menor tiempo el ingreso al territorio nacional. El mecanismo funciona a partir del reconocimiento del iris del viajero, técnica que, por su velocidad, estabilidad y seguridad, es ideal para la identificación de grupos numerosos de personas, además de su agilidad, una de las ventajas del sistema Biomig es la seguridad, puesto que son más de 150 patrones de identificación los que se encuentran en el iris y que son inmodificables, salvo un traumatismo sufrido por el individuo. Estos patrones son diferentes en cada ojo, lo que hace aún más seguro el procedimiento. [10]

Identificación biométrica - Registraduría Nacional del Estado Civil [11]

La Registraduría Nacional del Estado Civil ha utilizado durante los últimos 12 años la biometría como una herramienta para identificar a los colombianos, al lograr incluir la información de las huellas dactilares en el código de barras encriptado en la nueva cédula de ciudadanía amarilla con hologramas.

Actualmente la Registraduría Nacional del Estado Civil efectúa el proceso pertinente para lograr la firma de convenios que permitan por primera vez acceder al Sistema de Identificación Automatizada de Huellas Dactilares, Afis de la Registraduría y poder realizar autenticación biométrica de ciudadanos.

Certivoz, Sistema de autenticación biométrica de voz [12]

Certivoz es un servicio que garantiza hasta un 98% la autenticidad de una persona sólo con decir la frase “Mi voz es mi contraseña”. El modelo de servicio que desarrolló Certicámara valida la identidad de una persona en cuestión de segundos y es único en Colombia, pues está concebido para que la entidad que lo implemente pague el servicio por consumo y sin necesidad de invertir en infraestructura física y personal dedicado a la administración de esta.

Precisamente este sistema de autenticación por medio de la voz es de fácil integración con otros sistemas y tiene altos niveles de seguridad pues incluye componentes como firmas digitales y estampas de tiempo en el proceso de enrolamiento y de la transacción, lo que garantiza que hay integridad de los datos y tiene plena validez jurídica y probatoria. Esta herramienta será de especial utilidad en el sector financiero, call centers, entidades que requieran verificar la supervivencia de usuarios y otros procesos que requieran control presencial o no presencial.

Biometría en el sector financiero [13]

Según Asobancaria, En la actualidad, diferentes entidades hacen uso del servicio de autenticación biométrica en transacciones financieras, principalmente en procesos de otorgamiento de crédito en sus diferentes modalidades, como apertura de cuentas de ahorro y CDT's, entrega de tarjetas de débito y crédito, financiamiento en comercios aliados tales como concesionarios de vehículos, clínicas dentales, entre otros.

Dentro de las entidades que hacen uso de la autenticación están: BBVA, Banco Popular, RCI Banque, Compañía de Financiamiento TUYA, Banco Caja Social, Porvenir, Bancoomeva y Bancolombia. Bajo el Convenio se realizan mensualmente cerca de 700.000 procesos de validación biométrica.

Asobancaria indica que el uso de la biometría en los procesos financieros ha traído importantes beneficios para los clientes y usuarios del sistema de capital, ha mejorado la experiencia y reducido las fricciones en la interacción y el acceso a los servicios. Además, los bancos han realizado importantes avances en el cierre de brechas en la reducción del fraude por suplantación de identidad y progresan a grandes pasos en las políticas de "cero papel", lo que garantiza total seguridad, confianza e innovación en sus procesos. Algunas cifras interesantes para resaltar son:

- 60% de las entidades financieras usan biometría dactilar certificada bajo el Convenio de Asobancaria.
- 1,1 y 1,3 millones de validaciones biométricas mensuales.
- Transacciones financieras de minutos a segundos.
- Reducción del fraude en más 98%.

Presentación de datos

Para realizar el análisis, se tomó una muestra poblacional de 52 individuos de diversos géneros, localidades y estratos sociales dentro de la ciudad de Bogotá. A través de una encuesta de 6 preguntas publicadas en redes de mensajería social como whatsApp, facebook y twitter. Por medio de "Google Forms" en la página web https://docs.google.com/forms/d/e/1FAIpQLSc3rL9Wm3RnrlMZjRM0eZLX0KMktttmEkA7sXoQttkw0kmaBw/viewform, Lo anterior se realizó con el fin de medir la percepción sobre la tecnología biométrica en la población de muestra.

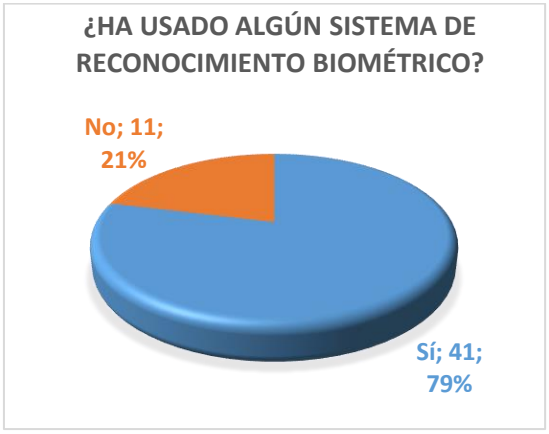

Ilustración 6: El 78.8% de los individuos indicó que si ha hecho uso de la biometría mientras el 21.2% indicó que no.

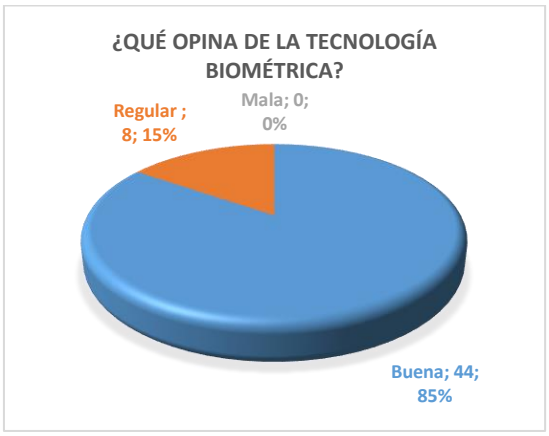

Ilustración 7: El 84.6% opino que esta tecnología es buena mientras el 15.4% le parece regular

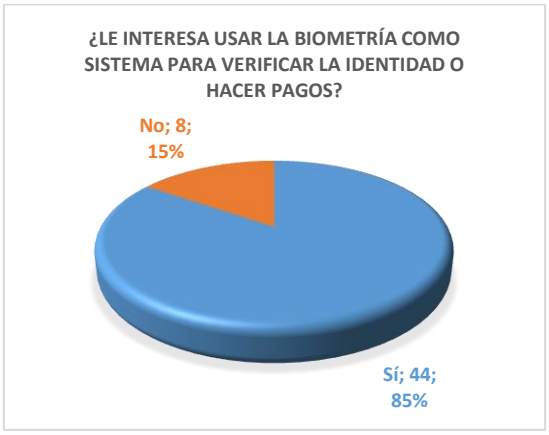

Ilustración 8: Al 84.6% le interesa el uso esta tecnología mientras el 15.4% no está interesado

Ilustración 9: El 90.4% opino que sí, frente al 9.6% que opina que no.

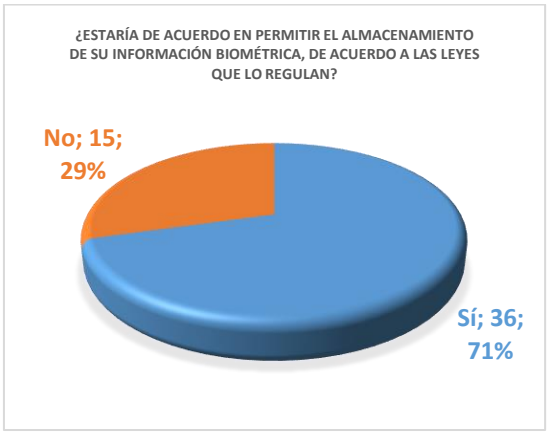

Ilustración 10: El 70.6% indicó que está de acuerdo, mientras el 29.4% no está de acuerdo.

Ilustración 11: El 63.5% confían en la seguridad de esta tecnología, mientras el 36.5% tienen cierto recelo.

Según se observa en los resultados de la encuesta planteada, la mayoría de la población está de acuerdo con el uso de la biometría como herramienta para la identificación y sobre todo asume que es una tecnología que llegó

para quedarse, sin embargo, existe cierto recelo respecto a los riesgos a la privacidad que esta tecnología pueda llegar a implicar.

Adicionalmente se encuentra que:

- La mayoría de la población ha hecho uso de tecnología biométrica.
- La biometría es considerada como una buena tecnología útil.
- La mayoría de las personas ven con buenos ojos la implementación de sistemas biométricos para la identificación durante transacciones bancarias.
- Aunque hay aceptación de esta tecnología, existe cierto recelo respecto al almacenamiento de la información y su posterior uso.

III. CONCLUSIONES

Como resultado de la investigación estadística realizada es posible concluir lo siguiente:

- En Colombia no existe una regulación específica relacionada con el uso de la información biométrica adicional a la ley de protección de datos personales.
- Aunque el uso de la tecnología de reconocimiento biométrico en el país aún es reducido, se presenta como un campo amplio de trabajo y con mucho futuro.
- Los sistemas de identificación biométrica son susceptibles a ser atacados como cualquier tipo de sistema informático, se debe realizar un análisis de riesgos y vulnerabilidades para mitigar la posibilidad de que estos riesgos se materialicen.
- La tecnología biométrica tiene una buena aceptación dentro de la población, son reconocidas sus ventajas y beneficios, aunque existe cierto recelo ante los posibles riesgos a la privacidad.

IV. REFERENCIAS

[1] Responsible and Ethical use of Biometrics - Biometrics Institute.” [Online]. Available: https://www.biometricsinstitute.org/. [Accessed: 08-Sep-2019].

[2] S. Prabhakar, A. Jain, and A. Ross, “An Introduction to Biometric Recognition,” IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 4–20, 2004.

[3] P. S. P. Wang, “Biometrics Intelligence Information Systems and Applications,” 2007, pp. 1454–1454.

[4] Instituto Nacional de CiberSeguridad, “Tecnologías biométricas aplicadas a la ciberseguridad,” Una guía aproximación para el Empres., vol. Vol. 1, 2016., pp. 7–10.

[5] “Facial recognition: It’s time for action - Microsoft on the Issues.” [Online]. Available: https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/. [Accessed: 06-Oct-2019].

[6] “Eyes open to the world with Biometric Iris Reader | Iris Recognition System.” [Online]. Available: https://www.screencheckme.com/biometric-iris-technology/. [Accessed: 06-Oct-2019].
[7] “Biometría vascular ¿Es el futuro? | Anixter.” [Online]. Available: https://www.anixter.com/es_la/about-us/news-and-events/news/vascular-biometrics-is-it-the-future.html. [Accessed: 06-Oct-2019].
[8] “Top ten mind blowing advantages of biometric technology - M2SYS Blog On Biometric Technology.” [Online]. Available: http://www.m2sys.com/blog/biometric-hardware/top-ten-mind-blowing-advantages-of-biometric-technology/. [Accessed: 10-Nov-2019].
[9] Ministerio de Relaciones Exteriores Colombia, “BioMig - Migración Colombia,” 2019-10-04. [Online]. Available: https://migracioncolombia.gov.co/subdireccion-de-control-migratorio/39-subdireccion-de-control-migratorio/biomig. [Accessed: 03-Nov-2019].
[10] EL TIEMPO Casa Editorial., “Habilitan registro biométrico para procesos de migración en El Dorado | Gobierno | Economía | Portafolio,” 2018-02-27. [Online]. Available: https://www.portafolio.co/economia/gobierno/entra-en-funcionamiento-registro-biometrico-para-procesos-de-migracion-en-el-dorado-514696. [Accessed: 03-Nov-2019].
[11] Registraduría Nacional del Estado Civil, “Identificación biométrica: cada vez con más usos en la vida cotidiana- Registraduría Nacional del Estado Civil.” [Online]. Available: https://wsr.registraduria.gov.co/Identificacion-biometrica-cada-vez.html. [Accessed: 03-Nov-2019].
[12] Colombia Digital and Certicámara, “Virtualización y Seguridad de la Información,” Colomb. Digit., vol. 4, p. 33, 2019.
[13] ASOBANCARIA, “Biometria en el Sector Financiero Colombiano - Asobancaria.” [Online]. Available: https://www.asobancaria.com/biometria/. [Accessed: 03-Nov-2019].
[14] A. Brömme, “A risk analysis approach for biometric authentication technology,” Int. J. Netw. Secur., vol. 2, no. 1, pp. 52–63, 2006.

Publicación Facultad de Ingeniería y Red de Investigaciones de Tecnología Avanzada – ITA

REVISTA

TIA