ANÁLISIS DE VULNERABILIDADES EN SISTEMAS BIOMÉTRICOS DACTILARES EN REFERENCIA A LOS ATAQUES TIMING Y HILL-CLIMBING

CARLOS ANDRÉS CAMPOS LEGUÍZAMO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.

2021

ANÁLISIS DE VULNERABILIDADES EN SISTEMAS BIOMÉTRICOS DACTILARES EN REFERENCIA A LOS ATAQUES TIMING Y HILL-CLIMBING

CARLOS ANDRÉS CAMPOS LEGUÍZAMO

Proyecto de Grado - Monografía presentada para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTOR DE PROYECTO

Lic. Danny Fernando León Jaramillo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente de Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá D.C., 30 de julio de 2021

A Dios, a mi familia, mis padres, mi hermana, mis sobrinos Pachi y Juancho y a mis amigos quienes con su amor, guía y compañía, me inspiran día a día a ser mejor y entregar lo mejor al servicio de los demás.

AGRADECIMIENTOS

Decidí emprender éste camino, el de la seguridad informática, dejándome llevar por la pasión y la responsabilidad que esto implica. Veo con gran prominencia, un futuro al corto y mediando plazo en relación a la protección de la información, futuro del cual, sin duda, quiero ser participe.

A lo largo de este camino, he logrado aseverar esa pasión por esta materia, lo anterior, por medio del acompañamiento de personas y profesionales que me brindaron su experiencia y conocimiento; a mi director de tesis Lic. Danny León, a todos los docentes del Programa de Especialización en Seguridad Informática y colegas, que durante épocas de incertidumbre por pandemia, hicieron del aprendizaje una de las mejores salidas a tiempos difíciles.

A ellos, un eterno agradecimiento.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ATAQUE INFORMATICO: definida como el intento por medio del uso de herramientas para exponer, alterar, destruir o depurar la información por medio del acceso a un activo de información sin los permisos otorgados.

BIOMETRICO: tecnología que permite la identificación basada en un rasgo o característica física de un individuo.

CIBERSEGURIDAD: área que tiene relación con la informática, cuyo enfoque se da en la protección de la información de las infraestructuras tecnológicas de las organizaciones frente a los ataques maliciosos.

HUELLA DACTILAR: estructura formada por los dedos humanos, que por naturaleza, genera una estructura única por persona, definida en la semana diecinueve de gestación.

ESTÁNDAR: concepto definido para tomar una referencia o patrón. Documento de seguridad informática por consenso, cuyo fin es ofrecer lineamientos o guías para su implementación.

MITIGACÓN: reducción de una vulnerabilidad, lo anterior con el fin de atenuar riesgos y peligros.

MODELO: pauta para ser imitida y replicada. Prototipo de referencia. Mecanismos consistentes y efectivos para la implementación de controles técnicos, procedimentales y de recursos humanos.

SENSOR: dispositivo utilizado para detectar acciones, características y con ello, generar una respuesta por medio de un sistema.

SISTEMA: conjunto de elementos que se encuentran ordenados, con el fin de generar una interacción entre si con el fin de lograr una meta u objetivo.

VULNERABILDIAD INFORMÁTICA: defecto presentado en un sistema permitiendo ataques externos que busquen afectar la información en su disponibilidad, confidencialidad e integridad.

RESUMEN

Por medio del documento realizado se identificó las características, componentes tecnológicos y soluciones que brinda los sistemas biométricos dactilares en diferentes entornos de negocio, entre otros, los implementados con el fin de adoptar lo establecido en la norma ISO27001:2013 (dominio de Seguridad física – objetivo áreas seguras – control físico de entradas) en soluciones orientadas a sistemas de votación electrónicos y en Organizaciones para procesos de autenticación y legitimidad. Con lo anterior, se realizó una validación de las vulnerabilidades respecto a los tipos de ataques Timing y Hill-climbing, considerando indicadores como EER (Coeficiente de eficiencia energética), FAR (False Acceptance Rate) y DET (Detection Error Tradeoff), en referencia a los sistemas NFIS y Match on Card, con base a los parámetros BEAT (Biometrics Evaluation and Testing) y KBOC (Keystroke Biometrics OnGoing Competition).

Se propuso parámetros, recomendaciones, metodologías, normatividad y estándares que llevan a considerar junto a la implementación, buenas prácticas, lo anterior bajo criterios de elección de sistemas considerando pruebas de concepto (PoC) de sistemas biométricos dactilares, además de proponer procesos de mitigación bajo la transformada HAAR, posterior a las vulnerabilidades identificadas, las cuales se obtuvieron por resultados con base en desarrollos experimentales por parte de los autores investigados y que involucraron diferentes tipos de sensores, parámetros y contextos.

Palabras clave: Ciberseguridad, vulnerabilidad, prueba de concepto (Poc), biométrico, mitigación, sensor, buenas prácticas.

ABSTRACT

Through the document carried out, the characteristics, technological components and solutions provided by fingerprint biometric systems in different business environments, among others, those implemented in order to adopt the provisions of ISO27001: 2013, in its domain of Security, were identified. physical - objective secure areas - physical control of entrances, in electronic voting systems and in Organizations for authentication and legitimacy processes. With the above, a validation of the vulnerabilities was carried out regarding the types of Timing and Hill-climbing attacks, considering indicators such as EER (Energy Efficiency Coefficient), FAR (False Acceptance Rate) and DET (Detection Error Tradeoff), in reference to the NFIS and Match on Card systems, based on the parameters BEAT (Biometrics Evaluation and Testing) and KBOC (Keystroke Biometrics OnGoing Competition). Parameters, recommendations and methodologies were proposed that lead to considering, along with the implementation, good practices under system choice criteria by proof of concept (PoC) of defined fingerprint biometric systems, in addition to proposing mitigation processes under the HAAR transform, after the identified vulnerabilities, which were obtained by results based on experimental developments by the investigated authors and which involved different types of sensors, parameters and circumstances.

Keywords: Cybersecurity, vulnerability, Proof of Concept (Poc), Biometric, mitigation, sensor, good practices.

INTRODUCCIÓN

Los sistemas biométricos dactilares son soluciones imprescindibles en una organización, lo anterior, conforme a que su implementación, entre otras, busca adoptar lo establecido en la norma ISO27001:2013, en su dominio de Seguridad física - objetivo áreas seguras - control físico de entradas. Adicionalmente, los sistemas biométricos dactilares brindan soluciones de autenticación con características propias (lo que es) del individuo.

Los sistemas biométricos están constituidos por un sistema definido, que lleva a cabo el procesamiento de la información; a partir de este sistema, ha surgido incertidumbre en cuanto a la seguridad de los datos, en lo que refiere a su autenticidad, confidencialidad y disponibilidad, esto como respuesta ante situaciones acontecidas, como por ejemplo, el 11 de septiembre de 2001 en los Estados Unidos de América, con los ataques a las torres gemelas, que marcó un punto de inflexión en esta área y por supuesto, en aspectos puntuales de la seguridad en sus diferentes ámbitos.

Realizando una investigación e identificación de las vulnerabilidades de los sistemas biométricos dactilares, en particular, sobre los ataques Timing y Hill-climbing, se analizarán sus características y comportamientos conforme sistemas y estándares Internacionales (NIST, MoC, BEAT, KBOC) buscando proponer aspectos para la mitigación de riesgos, con esto, proponer parámetros, recomendaciones y adicional, metodologías conforme buenas prácticas. Para llevar a cabo lo mencionado, se hace necesario el uso de sistemas NFIS y Match-on-Card, que generan un procesamiento referente y característico de la información dactilar.

Este trabajo busca dar a conocer los criterios y metodologías utilizadas para llevar a cabo la evaluación de los sistemas de huella dactilar, con esto, proponer bajo una postura crítica las características a considerar en el sistema para la evaluación de acuerdo a las vulnerabilidades analizadas, buscando fortalecer la postura de seguridad de las compañías que optan por la integración de esta tecnología.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Los sistemas biométricos dactilares presentan características propias conforme su estructura lógica cómo física, con ello, se tiene un sistema que se encuentra definido para llevar a cabo el proceso de toma y procesamiento de la información cuyo resultado genera una decisión. Este sistema presenta vulnerabilidades que afectan de manera concreta la confidencialidad, disponibilidad e integridad de la información, que deben considerarse previo a su implementación y puesta en un ambiente productivo.

Los sistemas biométricos dactilares ofrecen soluciones imprescindibles en las organizaciones, por tanto, ante las circunstancias catastróficas vividas, por ejemplo, ataques terroristas, robo de información y la suplantación de identidad, entre otros, que implican retos en la seguridad de la información, se hace necesario considerar, analizar y evaluar los criterios de validación conforme pruebas de concepto de su sistema, sus vulnerabilidades y aspectos a considerar.

1.2 FORMULACIÓN DEL PROBLEMA

De acuerdo a lo expuesto, se formula la siguiente inquietud: ¿Qué aspectos y parámetros se deben considerar con el fin de mitigar ataques tipo Timing y Hill-climbing en sistemas biométricos dactilares, lo anterior en referencia a sistemas y estándares Internacionales?.

1.3 DESCRIPCIÓN DEL PROBLEMA

Los ataques tipo Timming en los sistemas biométricos consisten en el éxito de obtener una etiqueta de un paquete de datos válida por parte del atacante. Por medio del envío de mensajes, se genera comparaciones a nivel de *Bytes*, permitiendo al atacante medir los tiempos de respuesta en un servidor que revela su clave secreta permitiendo accesos no autorizados. Los ataques tipo Hill-climbing, fundamentan su acción en patrones sintéticos que elevan las puntuaciones sucesivas conforme los parámetros evaluados.

2. JUSTIFICACIÓN

Los sistemas biométricos dactilares son soluciones imprescindibles para el aseguramiento de la identidad en las organizaciones, conforme permiten el acceso legítimo a activos de información importantes y transversales a las líneas de negocio. No obstante, se debe considerar que dichos sistemas son vulnerables, ya que un atacante cuenta con la posibilidad de poner en riesgo la confidencialidad, disponibilidad e integridad de la información, por tanto, es importante identificar la taxonomía de los tipos de ataques Timing y Hill-climbing en búsqueda de proponer, recomendar e informar acerca de metodologías de mitigación de riesgos conforme buenas prácticas, buscando establecer soluciones eficaces a organizaciones que cuenten o consideren implementar esta tecnología.

Existe indicadores y parámetros que evalúan los sistemas, no obstante, es necesario articular estos criterios con estándares internacionales que permiten complementar una postura crítica de elección de acuerdo a las necesidades de identificación, conociendo y aceptando los riesgos existentes.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Identificar las vulnerabilidades de los sistemas biométricos de huella digital en los ataques tipo Timing y Hill-climbing, analizando los parámetros establecidos por estándares internacionales que busquen la mitigación de posibles riesgos.

3.2 OBJETIVOS ESPECÍFICOS

- Describir el sistema biométrico de huella digital, con ello sus características, componentes Software – Hardware, tecnologías y aplicabilidad.
- Considerar las vulnerabilidades relacionadas al sistema biométrico de huella digital respecto a ataques Timing y Hill-climbing, analizando indicadores como EER (Equal Error Rate), FAR (False Acceptance Rate) y DET (Detection Error Tradeoff).
- Generar un análisis de los sistemas NFIS y Match On Card con base en parámetros BEAT (Biometrics Evaluation and Testing) y KBOC (Keystroke Biometrics OnGoing Competition).
- Proponer parámetros, recomendaciones y metodologías conforme buenas prácticas y criterios de elección (modelo Gartner) para las organizaciones en cuánto a dispositivos biométricos dactilares.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 El sistema biométrico y sus vulnerabilidades. Los sistemas biométricos para el procesamiento de información realizan conforme su sistema lo siguiente: recolección de datos, transmisión, procesamiento de señal, decisión y almacenamiento. Cada uno de los procesos llevados a cabo para el tratamiento de la información involucra una parte del sistema que puede llegar a ser vulnerable y afectado por un atacante.

Como se observa en la figura 1 en la página número 18, se tiene esquematizado los diferentes procesos anteriormente descritos. Sin abordar investigaciones puntuales, por ahora, sobre cada parte del sistema, se relacionará en general, las vulnerabilidades presentes en los sistemas biométricos dactilares. En el proceso de transmisión entre el sensor y el extractor de características, se puede presentar ataques de inyección de datos biométricos almacenados de manera previa, esto especialmente en aplicaciones remotas que hacen uso de Internet; además, el sensor puede presentar vulnerabilidades conforme biometría falsa, que consiste en burlar por medio de software que genera imágenes sintéticas, suplantación de identidad haciendo uso inescrupuloso y malicioso de la información obtenida.

En el extractor de características, un atacante puede forzar el sistema para obtener valores escogidos previamente, presentándose el escenario en el cual se inserta un programa que reemplaza a un legítimo extractor.

En el proceso de transmisión de las características extraídas, se puede presentar un ataque que busca reemplazar las muestras originales y actuales por unas falsas, o que en su defecto, se hayan adquirido previamentes de forma ilegal buscando el ingreso al sistema.

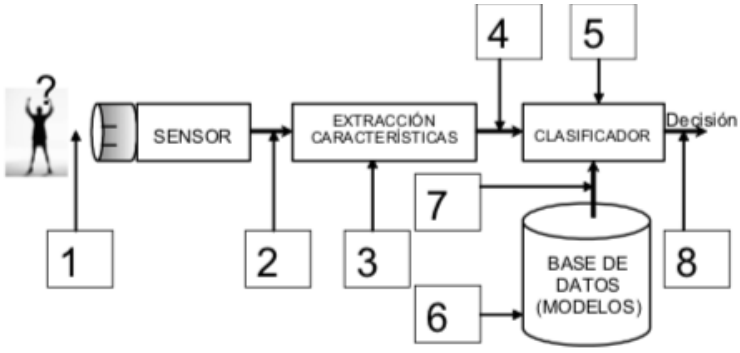
En el clasificador, un ataque puede pretender puntuaciones (Score) válidos obligando al sistema a la aceptación de un instruso o rechazo de un Usuario legítimo.

Conforme Faúndes[1], la base de datos, permiten el resultado de la autenticación dependiendo del proceso de comparación entre las muestras almacenadas y las capturadas. Bajo esta premisa, se considera que los sistemas de almacenamiento pueden llegar a ser vulnerables por medio de las técnicas de ataque tanto a bases de datos relacionales como no relacionales, generando posibles alteraciones a la información afectando su confidencialidad. Los ataques a los servidores de bases de datos, también representan una amenaza, pues de tenerse un caso de éxito, la data puede sufrir eliminación (indisponibilidad), alteración (integridad) y/o manipulación (confidencialidad).

En el proceso de transmisión de los datos de la base de datos (BBDD) al clasificador, se puede presentar suplantación de comunicación, afectando el proceso de transmisión; en el escenario en que la base de datos se encuentre en la nube y sea compartida con diferentes sistemas de acceso, las consecuencias pueden ser altamente negativas.

Por último, en el proceso de decisión, se presentan ataques que omiten todo el sistema biométrico generando cambios de decisión afectando de manera puntual el resultado, de esta manera, materializandose el riesgo. Un sistema de decisión puede basarse en un relé, que de afectarse, burla todo el proceso realizado con simplemente, por ejemplo, la generación u omision de una tensión eléctrica, por muy seguros que sean los otros procesos.

Figura 1. Puntos vulnerables sistema reconocimiento biométrico.



[1] FAÚNDES ZANUY, Marcos. Experimentos prácticos sobre la vulnerabilidad de sistemas biométricos [en línea]. 2016. p. 6. [Consultado 28 de marzo 2020]. Disponible en: https://docplayer.es/10065843-Experimentos-practicos-sobre-la-vulnerabilidad-de-sistemas-biometricos.html

Fuente: FAÚNDES ZANUY, Marcos. Puntos vulnerables sistema reconocimiento biométrico. [En línea]. Experimentos prácticos sobre la vulnerabilidad de sistemas biométricos. España: EUPMT. 2004. p. 10. [Recuperado en 03 de Abril 2020]. Disponible en: https://docplayer.es/36547109-Experimentos-sobre-la-vulnerabilidad-de-sistemas-biometricos.html

De acuerdo al crecimiento exponencial del uso en el mundo de las tecnologías biométricas dactilares, se desarrolla en paralelo estudios conforme los retos a nivel de seguridad de la información para con esta tecnología. Los diferentes estudios abordan desde la estructura propia de los sistemas, anteriormente expuestos, hasta los retos para las nuevas tecnologías involucrando ataques, escenarios y algorítmos.

Existen diferentes tipos de de vulnerabilidades en los sistemas biométricos, que han sido objeto de estudio dada su importancia a nivel organizacional, y en ella, para los procesos de estandarización en referencia al estándar ISO27001:2013 en su dominio de Seguridad física, objetivo áreas seguras y control físico de entradas y demás aplicabilidades.

Es por esto que Lucio[2], desde el punto de vista no informático, genera estudios que infieren acerca de la importancia de los sistemas biométricos de reconocimiento de huella dactilar, reconociendo que estos son vulnerables y buscan ser atacados por medio de la identificación mecánica, esto sin realizar una intervención a la parte lógica del sistema. En tal sentido, por ejemplo, se tiene conocimiento de una familia Taiwanesa que desde cinco generaciones atrás carecen de huellas dactilares, parece extraño, pero es un fenómeno que impide su identificación en los sistemas biométricos, generando un grado de incertidumbre alto en las decisiones. Por otra parte, como vulnerabilidad, el sabotaje presenta diferentes ataques propiamente al sensor, causados por

[2] LUCIO, Cristina. El extraño caso de la familia sin huellas dactilares. En: EL MUNDO [sitio web]. Madrid. Serie “Estudi del ADN”. [Consulta 28 de abril 2020]. Disponible en: https://www.elmundo.es/elmundosalud/2011/08/04/pielsana/1312482983.html

daños físicos representados en el impedimento al normal funcionamiento e infiltración de información al sistema.

Considerando aspectos biológicos, propios del cuerpo humano, la dermatitis como patología causa piel irritada o inflamada, con ello alteración de las crestas papilares, aspecto fundamental para el proceso de extracción de características; esto genera una alteración de lectura, en el peor escenario, genera el acceso a personal no autorizado, causando falsa aceptación materializándose el riesgo. Así mismo, el trasplante de huella, procedimiento por el cual los delincuentes están dispuestos a pagar grandes sumas de dinero, permite el acceso a sistemas, principalmente bases de datos, suplantando una identidad legítima (aspectos a considerar en referencia al estudio a realizar).

Los colaboradores de una organización, incurren en errores sistemáticos, por ejemplo, cuando se genera el retiro de una persona de la organización, eventualmente, la base de datos no es actualizada logrando permitir el ingreso, tiempo después, posibilitando accesos a información a personal no autorizado.

Estos, son algunos de los escenarios que se deben considerar en el estudio de los sistemas biométricos dactilares, reconociendo fuentes propias de incertidumbre que pueden llegar a generar su decisión.

De acuerdo al sistema de biometría dactilar expuesto, con ello, reconociendo los ataques que pueden llegar a ser generados sin realizar accesos a la parte lógica, diferentes investigadores además de abordar los posibles tipos de ataques, proponen soluciones conforme las necesidades latentes por reducir estas brechas de seguridad.

Estudios conforme el sistema biométrico establecen ocho categorías clasificatorias: 1. Ataques al sensor. 2. Ataque al canal entre el sensor y extractor de características. 3. Ataques al extracto de características. 4. Ataques al canal entre el extractor de características y el comparador. 5. Ataques al comparador. 6. Ataques a las bases de datos. 7. Ataques al canal entre base de datos y comparador. 8. Ataques a canal entre comparador y actuador.

Conforme los estudios de Asataño[3], se generan diferentes tipos de pruebas para corroborar las vulnerabilidades del sistema dactilar, haciendo uso de coeficientes que arrojan resultados relacionados con la falsa aceptación (FA) y el falso rechazo (FR). Adicional a estas consideraciones, el autor refiere los siguientes pilares de la información importantes a considerar: integridad, confidencialidad y disponibilidad, adicional al no repudio, con esto, plantea de manera interesante consideraciones de seguridad para implementar sistemas biométricos, esto bajo un esquema integral con aspectos como áreas a resguardar, áreas de control de acceso y areas de control de seguridad.

Gonzaléz, Contreras y Yañez[4], también abordan en sus investigaciones la importancia de considerar los pilares de la información en los sistemas de huella dactilar. Inicialmente sobre diferentes procesos en los cuales, se pretende generar una evaluación a los sistemas biométricos, logrando establecer de manera previa una relación de cuerpo humano y biometría, concluyen. Es de considerar, que el cuerpo humano posee una estructura tanto funcional como característica que posibilita un estudio de los diferentes niveles de complejidad abarcando composición química, biofísica y conductual, pasando por diferentes niveles de detenimiento como células, tejidos, órganos y sistemas. La evaluación de sistemas biométricos se estima en la verificación de múltiples aspectos incluyendo el proceso de adquisición de datos en conjunto a la integración del sistema. Los principales aspectos a evaluar y en los cuales se involucran los pilares de la información mencionados con anterioridad, articulados con las evaluaciones biométricas, son: 1. Rendimiento en concordancia a sus funciones. 2. Confidencialidad, integridad y disponibilidad de la información en el sistema. 3. La fiabilidad y mantenimiento de las herramientas informáticas del sistema. 4.

[3] ASATAÑO ESPAÑA, Julio y ROSALES DIAZ, Estela. La biometría dactilar como una opción para la seguridad informática [en línea]. 2011, agosto–diciembre, nro. 97. [Consultad: 25 de abril 2020]. Disponible en: http://pistaseducativas.itc.mx/wp-content/uploads/2012/02/3-ASATO-PE-97-44-58.pdf. ISSN: 1405-1249

[4] GONZALÉZ, Juan Carlos; CONTRERAS, Walter y YAÑEZ, Carlos. Tecnologías Biométricas aplicadas a la seguridad en las organizaciones [en línea]. Lima (Perú): Universidad Nacional Mayor de San Marcos. 2016. p. 66. [Consultado 28 de marzo 2020]. Disponible en: https://revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/view/3336/2765

La etapa de comercialización del producto con cuya estimación de costos y beneficios se debe considerar. 5. La facilidad y manejo intuitivo del Usuario. 6. El marco legal.

Además de los procesos de evaluación se establece un proceso de seguridad. González, Contreras y Yañez[5], plantean una forma holística de evaluar la seguridad, para esto definen dos aspectos: 1. Considerar los colaboradores como clientes, de esta manera se permite un acercamiento al modelo *Zero Trust* permitiendo que sean participes de los riesgos que se establecen; pilares como protección de datos, acceso local, acceso remoto, costos, disponibilidad del sistema, prevención de denegación de servicios, planes de recuperación de desastres, consideración de pérdida o destrucción de data, respaldos o backups, igualmente son importantes. 2. Identificación de responsables: Los diferentes departamentos de las Compañias deben tener una trazabilidad del desarrollo de los diferentes procesos, bien sea recursos humanos, seguridad física, seguridad informática, áreas de gestión, financieras y usuarios finales. Se establece la importancia de contar con una política de seguridad representando una filosofía de la Compañía, adoptando un modelo relacionado a procesos de auditoría en la infraestructura de las organizaciones.

4.1.2 Los sistemas biométricos y sus vulnerabilidades a nivel sensorial. Haciendo énfasis en los ataques dirigidos hacía el sensor del sistema biométrico dactilar, es de considerar la masiva implementación y con ello, el empleo de diferentes tecnologías biométricas en el mundo, que generan diversas exposiciones a riesgos, entre ellos, algunos que son específicos y otros que son compartidos con otras tecnologías. Conforme la pérdida o robo de información en relación a datos exclusivos y ligados a las personas, haciendo de esto un ataque exitoso y un incidente de seguridad grave, la suplantación de identidad, es un ejemplo del uso de la información biométrica que previamente ha sido usurpada y/o falsificada; escenario en que se utiliza la información para cometer crímenes, y en el cual, el no repudio es algo a considerar. Por su parte, un ataque

[5] Ibid., p. 58.

basado en sabotaje, busca impedir el funcionamiento del sistema, con ello, se infiere que estos tipos de ataques reflejan un desacuerdo con la implementación de sistemas de seguridad biométricos, pues su efectividad, coloca en duda la postura de seguridad de la organización.

Se establece por parte del INSTITUTO NACIONAL DE CIBERSEGURIDAD[6], en Madrid, España, buenas prácticas en el empleo de los diferentes sistemas biométricos con el objetivo de generar una reducción de los riesgos asociados, proponiendo direccionar esfuerzos en el sistema a nivel de seguridad, almacenamiento redundante, doble factor de autenticación, adaptaciones adecuadas e inversión en seguridad tecnológica, esto, en la búsqueda de mitigación de riesgos y vulnerabilidades. Las anteriores consideraciones son realmente importantes, dado que las soluciones propuestas mitigan de manera efectiva algunos de los riesgos a los que se ven expuestos diversos sistemas biométricos dactilares.

Por otra parte, un estudio de la Universidad Oberta de Catalunya (UOC), los investigadores Rifa y Sierra[7], dan a conocer un análisis sobre los retos de seguridad y privacidad de estos sistemas, teniendo en cuenta las siguientes consideraciones: 1. Aseguran que la biometría no es un sistema inequívoco, se ejemplifica respecto a las contraseñas, pues un usuario la sabe o no la sabe, a diferencia de las huellas dactilares, pueden generar similutd a un patrón, no obstante, pueda que no sea del todo idéntica. Se propone plantear un umbral que permite establecer un estricto nivel de coincidencia , lo anterior con el fin de evitar errores de identificación; esto se puede plantear dentro del sistema, en el sensor y en la extracción de características, proponiendo mejoras. 2. Se manifiesta la vulnerabilidad de los datos, ya que se encuentran expuestos, pues

[6] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Una guía de aproximación para el empresario. En: Tecnologías biométricas aplicadas a la ciberseguridad [sitio web]. Madrid: Gobierno de España. Ministerio de Energía, Turismo y Agenda Digital. 2016. 31 P. [Consulta 1 de mayo 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

[7] RIFA, Helena y SIERRA, Jordy. Las cuatro brechas de la seguridad de la biometría. En: Cuadernos de seguridad [sitio web]. Madrid: Universitat Oberta de Catalunya (UOC). p. 200. [Consulta 28 de Abril 2020]. Disponible en: https://cuadernosdeseguridad.com/2019/12/tecnologia-biometrica-expertos-uoc/

nuestras fotografías están en diferentes lugares sociales, y en cuánto a huellas dactilares diferentes hackers de Chaos Computer en el año 2013[8] lograron demostrar que se podía crear una copia de la huella dactilar de la ministra de defensa de Alemania por medio de una fotografía suya en alta definición. 3. En dado caso que nuestros datos biométricos sean suplantados, esta amenaza no lograría contenerse, pues son datos inmodificables, van en nuestro ADN. Se plantea que si una huella es identificada, se debe tener la posibilidad de tomar muestras de cualquier dedo de la mano. 4. Por último, el uso masivo de nuestros datos biométricos para acceder a diferentes plataformas generan un gran problema de privacidad conforme la trazabilidad de acciones en la red, pues bien, generaremos a futuro registros en diferentes sistemas, estos sistemas de datos llevan a un atacante a conocer donde se realizó un registro y donde hemos estado; se plantea como solución utilizar diferentes factores de autenticación, además de investigar más y mucho mejor las tecnologías biométricas. Rifa y Sierra[9] realizan un trabajo interesante, por tanto que se reconocen de manera real y sucinta las diferentes vulnerabilidades a las que se ven expuestos los sistemas biométricos dactilares, a su vez, las soluciones planteadas deben ser consideradas para trabajos futuros, aún cuando estos se enfocan enteramente a la parte técnica.

> El uso de datos biométricos puede generar problemas de privacidad por la trazabilidad. Si se extiende el uso de los datos biométricos y, por ejemplo, se usa la huella en muchos entornos, una persona con la plantilla de esta huella podría hacer consultas en varias bases de datos donde se haya registrado y saber dónde hemos estado. Sin embargo, para que nos pudieran trazar los movimientos, sería necesario, además del dato biométrico, que las otras bases de datos fueran accesibles a todos y solo pidieran este factor de autenticación.[10]

[8] BBC NEWS. Red de hackers afirma que clonó huella dactilar de ministra alemana. En: BBC NEWS Mundo. [sitio web]. Reino Unido. [Consulta 18 de mayo 2020]. Disponible en: https://www.bbc.com/mundo/ultimas_noticias/2014/12/141229_ultnot_hackeo_huella_dactilar_ministra_alemana_men

[9] RIFA, Helena y SIERRA, Jordy. Las cuatro brechas de la seguridad de la biometría. En: Cuadernos de seguridad [sitio web]. Madrid: Universitat Oberta de Catalunya (UOC). p. 200. [Consulta 28 de Abril 2020]. Disponible en: https://cuadernosdeseguridad.com/2019/12/tecnologia-biometrica-expertos-uoc/

[10] Ibid., p. 1.

4.1.3 Los sistemas biométricos y sus vulnerabilidades en sensor y base de datos. Basándose en el sistema biométrico, en el, al proceso de base de datos y almacenamiento, Maya[11], por medio del trabajo desarrollado conforme el control de acceso mediante el reconocimiento de huella, plantea inicialmente la problemática de las vulnerabilidades de estos sistemas para el acceso a las compañías, algunos de ellos descritos anteriormente; además, plantea como posibles soluciones, las siguientes: Implementar un detector de vida, identificando si la solicitud dactilar la realiza un ser vivo y no un objeto o material, considerando esto como una imprescindible solución para los datos almacenados; se plantea un almacenamiento de un patrón detallado, es decir, no generar un almacenamiento de la huella total en la base de datos, y si un almacenamiento de las huellas dactilares con sus características propias detalladas; almacenar en base de datos huellas dactilares que menos sean expuestas a trabajo, por ejemplo, colaboradores que hacen manipulación de sustancias químicas, logrando tomar muestra de la mano que menos utiliza para desempeñar su labor; por último, adquirir sistemas biométricos confiables, con estándares aplicados y pruebas de concepto (PoC) fiables, evitando falsas alarmas o falsos positivos en conjunto con reportes a responsables certeros para la toma de decisiones. Gracias a esta propuesta, se considera importante que el autor incluya reportes de eventos con fines de tener trazabilidad de los intentos de intrusión en una organización, además de las buenas prácticas propuestas a considerar.

Los procesos de registro biométrico y carnetización de una compañía, en particular y a manera de ejemplo se expondrá Frontera Energy, motivan a un estudio de investigación focalizado en la actualización de bases de datos y las vulnerabilidades que allí se puedan peresentar, particularmente en el proceso de

[11] MAYA VARGAS, Adriana. Sistema biométrico de reconocimiento de huella dactilar en control de acceso de entrada y salida. Sistema biométrico de huella dactilar 1 [en línea]. Bogotá (Colombia): Universidad Militar Nueva Granada, 2013. p. 39. [Consultado 30 de marzo 2020]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/11168/MayaVargasAdriana2013.pdf?sequence=1&isAllowed=y

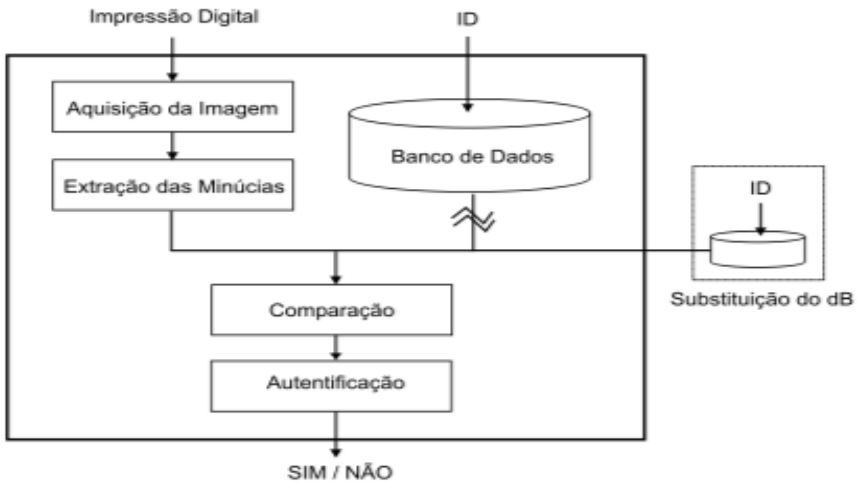
toma de datos y almacenamiento. Cataño[12], plantea, por medio de un diagnóstico previo, dar a conocer debilidades en los tiempos de respuesta de un nuevo registro y controles de acceso en seguridad en los escenarios de retiro de personal, pérdidas de carné y tarjetas de acceso, con esto, se genera la propuesta de ajustes en los procedimientos y en especial, en la retención de data, permitiendo una mejora en la postura de seguridad, que sin duda son imprescindibles. Lo anterior, se genera como respuesta a un sistema de autenticación importante para una compañía que busca fortalecer su sistema de almacenamiento de data, reconociendo el valor en la información.

Reconociendo la importancia de los sistemas biométricos, se establecen tres grupos en los cuales se pueden presentar ataques conforme los sistemas según Shimanuki y Zanini[13]: 1. Ataques mediante impresión digital artificial. 2. Ataques a la base de datos: datos almacenados que se pueden cambiar y/o modificar. 3. Por último, ataques a la interfaz durante la formación de la imagen, generando la intrusión por medio de un sistema que intercepte y modifique los datos. Conforme esto, el autor establece una metodología y un escenario con el fin de conocer las vulnerabilidades, esto con dos dispositivos para la creación de huellas artificiales: mouse Siemens (*Siemens Id Mouse*) que incorpora un sensor capacitivo y la API (*Application Program Interface*) ID SDK 1.9. Se generó la creación de un molde de silicona y goma para representar una imagen negativa de la huella dactilar, con esto se llevaron dos tipos de ataques: El primero, un ataque con el registro de la impresión digital original, el segundo, con el registro de la impresión digital artificial, esto por medio de la autenticación de una huella legítima. Como metodología, al sistema de base de datos se le reemplaza un elemento en el proceso, logrando eludir el sistema, como se representa en la figura número 2.

[12] CATAÑO RIVAS, Faiber. Mejoramiento en el procedimiento de seguridad de registro biométrico y carnetización en la compañía Frontera Energy de la ciudad de Bogotá [en línea]. Trabajo de grado para optar por el titulo de Administración de Empresas. Universidad Minuto de Dios, 2018. [Consultado 28 de marzo 2020]. Disponible en: https://repository.uniminuto.edu/handle/10656/6831?show= full

[13] SHIMANUKI, Mario y ZANINI, Angelo. Vulnerabilidades em Sistemas Biométricos Baseados em Impresso˜es Digitais [en línea]. Brasil: Instituto Tecnológico de Aeronáutica. [Consultado 28 de abril 2020]. Disponible en: https://www.sige.ita.br/anais/VIIISIGE/GE/GE055.pdf

Figura 2. Ataque a base de datos.



Fuente: SHIMANUKI, Mario y ZANINI, Angelo. Ataque a base de datos. [En línea]. Vulnerabilidades en Sistemas biométricos basados en impresiones digitales. Brasil. Instituto Tecnológico de Aeronáutica. p. 5. [Recuperado en 03 de abril 2020]. Disponible en: https://docplayer.es/36547109-Experimentos-sobre-la-vulnerabilidad-de-sistemas-biometricos.html

Un medio preventivo para el tipo de ataque expuesto, por parte de Shimanuki y Zanini se propone definir otros aspectos a nivel de sensor conforme el sistema biométrico: identificar la piel humana. De esta manera se determina que la validación sólo sea hecha por dedos reales, de lo contrario, el sistema aborte el proceso. Adicionalmente, para las bases de datos se propone el uso de funciones hash permitiendo que las modificaciones de archivos sean verificadas e identificadas, esto articulado de una copia de base de datos con fines de auditoria forense. Los investigadores enfocaron sus esfuerzos en el análisis de medición FRR (Tasa de rechazo falso) y tasa de aceptación falsa (FAR), lo anterior permitiendo identificar el comportamiento del sistema. Finalmente, se concluye que existen vulnerabilidades y estas son necesarias corregirlas. Es de considerar, que los autores usan un *mouse Siemens (Siemens Id Mouse)* que incorpora un sensor capacitivo y una API *(Application Program Interface)* ID SDK 1.9, elementos que entregan resultados de un procesamiento de datos previo y

que para futuras investigaciones servirán como modelo para proponer mejoras a nivel lógico y físico de los sistemas biométricos dactilares, lo anterior a pesar de que el software no es libre.

Conforme las vulnerabilidades de sistemas biométricos, en particular, los problemas que se pueden presentar en el almacenamiento seguro de datos, Linnartz y Tuyls[14] proponen un método particular que permite verificar la autenticidad, lo anterior por medio del procesamiento de datos para la verificación biométrica. El sistema consiste en extraer una medida, generar un procesamiento de señal en conjunto a una función criptográfica, con está función buscar encontrar una salida dada la señal de entrada. El procesamiento de las señales planteado por los autores es muy interesante, permite considerar la verificación de señales en los diferentes procesos del sistema, proponiendo un modelo en el cual se hace fácil deducir la señal de salida conforme una señal de entrada, no obstante, se convierte computacionalmente inviable encontrar una señal de entrada válida para una salida concreta; esto lleva a que si un atacante obtiene información de la base de datos, nunca podrá predecir a quien corresponde la información allí almacenada; importante para trabajos a futuro.

4.1.4 Los sistemas biométricos y los ataques tipo Hill-Climbing y Timing. Se logra identificar diferentes ataques indirectos propios de la lógica del sistema de reconocimiento de huella dactilar, lo anterior, con base en los tiempos de comparación algorítmica. Carballo[15], propone el estudio de ataques tipo *Hill-climbing*, que generan una modificación sucesiva de un patrón sintético (huella dactilar de goma) con el fin de que las minucias (valores incorrectos) se modifiquen y con ello eleven la puntuación o score obtenido hasta llegar a un

[14] LINNARTZ, Jean-Paul y TUYLS, Pim. New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates [en línea]. Amsterdam (Holanda): Eindhoven University of Technology, Junio 2003. [Consultado 1 de mayo de 2020] Disponible en: https://www.researchgate.net/publication/221597796_New_Shielding_Functions_to_Enhance_Privacy_and_Prevent_Misuse_of_Biometric_Templates

[15] CARBALLO DOMÍNGUEZ, Sara. Ataques indirectos a sistemas de reconocimiento de huella dactilar basados en los tiempos de comparación algorítmica [en línea]. Proyecto fin de carrera. Madrid: Escuela Politécnica Superior, 2009. p. 63. [Consultado 28 de marzo 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/9991/51301_20090522SaraCarballo.pdf?sequence=1&isAllowed=y

resultado preferiblemente satisfactorio. Estos estudios permiten identificar que existe una relación directa entre respuesta y tiempo de proceso, permitiendo reconocer que esta relación, da lugar a proponer mejoras con el fin de descartar ataques complejos a futuro.

Se hace uso para el experimento del software de referencia NFIS de la NIST; Carballo[16], encuentra dos probabilidades de ataques tipo *Hill-climbing,* con ello, hace un análisis de resultados y con esto invita a investigaciones futuras conforme las mejoras en criptografía adecuadas a los sistemas biométricos en los ataques más avanzados, como los son los tipo *timing-attacks* en relación a *Hill-climbing.*

Por medio del sistema analizando, se evidencia nuevamente que existe una relación directa entre tiempo y puntuación, generando un proceso experimental completo que a futuro, que servirá como referencia para el estudio propio de los ataques y su remediación, así como para las mejoras a los sistemas biométricos de huella dactilar.

4.1.5 Sistemas biométricos y sus vulnerabilidades en la implementación de aplicativos, actualizaciones y roles organizacionales. En el proceso de implementación de token biométrico, se debe considerar dentro de la metodología un análisis de riesgos, logrando identificar los actuales y que son conocidos, además de aquellos que se pueden presentar a futuro conforme las características del sistema, pues el involucrar aplicaciones genera aspectos adicionales a evaluar. Se establecen tres grupos de riesgo identificados inicialmente: 1. Sobre el aplicativo en el cual se articulará el sistema. 2. En las actualizaciones del mismo. 3. En la identificación de responsables. A continuación, se realiza un análisis de cada grupo, involucrando las mejores prácticas para con cada proceso evitando fugas de información:

1. Sobre el aplicativo a implementar la solución biométrica se deben considerar los siguientes aspectos: un usuario y contraseña única, de no tenerse, o de ser vulnerable, se podría concibir un riesgo alto teniendo en cuenta que los

[16] Ibid., p. 64.

accesos son responsabilidad legítima de su función; la auditoría en el control de accesos, que permite un seguimiento a todas las consultas realizadas por un usuario; un desarrollo de aplicativos con controles de seguridad, estableciendo actualizaciones en el *front-end* permitiendo la evolución de las técnicas de programación, llevando esto a imposibilitar a piratas informáticos que puedan ingresar y apropiarse del sistema dejando, por ejemplo, un virus que ocasione denegación de servicios, entre otros.

La fuga de información permite el ingreso no autorizado al aplicativo, consultando datos sensibles de los usuarios, generando a futuro posibles sanciones jurídicas por incumplimiento.

2. Conforme las actualizaciones, no se permite llegar a un punto de obsolecencia en las herramientas, a razón de la demanda actual de seguridad, a manera de ejemplo, a causa de la pandemia COVID-19, en la cual el trabajo remoto se incrementó, un servicio de VPN (Virtual Personal Network), por ejemplo, que a su vez, puede llegar a generar soluciones importantes, también puede llegar a causar brechas de seguridad a razón de la no actualización de las herramientas para su uso. Por otra parte, la falta de conocimiento de las diferentes áreas en cuanto a actualizaciones, impiden conocimientos de procesos haciendo de cada vulnerabilidad detectada una fortaleza para agentes externos que buscan filtrar la información, pues se presentan vulnerabilidades a nilvel de software que están relacionadas de manera proporcional con el licenciamiento y actualización del mismo. El proceso de actualización se hace imprescindible, más aún cuando se tienen procesos críticos de negocio bajo herramientas de VPN, esto a consideración de Parada[17], quien ve en la filtración de información cifrada un índice de compromiso imprescindible a nivel de capa de aplicación.

[17] PARADA SOLÓRZANO, Carlos. Propuesta de Metodología para implementar Token biométrico en la consulta de Clientes de las Compañías de Telecomunicaciones en la Policía Nacional de Colombia [en línea]. Titulo para optar como Especialización en Seguridad Informática. Universidad Piloto de Colombia, 2013. [Consultado: 26 de abril de 2020]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2611/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

3. El último grupo de riesgo abordado en esta parte, hace referencia en la identificación de responsables reflejados en la carencia de roles. Los roles deben ser definidos conforme cada actor de acuerdo a su responsabilidad; la carencia de manuales y documentación conforme el posicionamiento de cada rol en un equipo de trabajo, posibilita que no se tenga conocimiento por parte de los colaboradores del correcto manejo de incidentes, y por ende de su notificación, produciendo desconocimientos de área y procesos, aplicativos, y demás; la no existencia de controles posibilita la carencia de procedimientos y con ello la falta de idoneidad en un sistema o proceso, los cuales pueden llegar a ser apalancados por estándares como la ISO, COBIT, ISACA, ITIL, y demás. La deficiencia de áreas responsables (TI) genera que no se tenga líderes de procesos, teniendo consecuencias en la jerarquía de las organizaciones, generando falta de planeación y orden; la falta de indicadores de gestión impide conocer el estado actual de operación, impidiendo a futuro generar controles que mejoren la postura de seguridad de la compañía, en particular.

Por medio de los grupos de riesgo identificados y anteriormente descritos, es necesario generar una matriz de riesgos asignando a cada aspecto una escala determinada, consignando si el riesgo es alto, medio o bajo, así como una probabilidad de que este ocurra.[18] Este trabajo de matriz de riesgos realizado, da a conocer una visual holística que en el marco de los aplicativos, actualizaciones y roles brinda herramientas importantes a considerar conforme la implementación de sistemas biométricos dactilares, además de otras tecnologías que se vuelven importantes en momentos coyunturales.

4.1.6 Sistemas biométricos y sus vulnerabilidades ante otros tipos de ataque. Por medio de los estudios realizados a los sistemas biométricos, se reconocen sus limitaciones considerando el margen de mejora que se tiene. Las mejoras no sólo se basan en los parámetros de medición, sino también en el uso de los sistemas y la respuesta frente a los ataques (respuesta proactiva). De

[18] Ibid., p. 83.

acuerdo a Ortega[19], se tiene dos tipos de ataques: 1. Ataques de “esfuerzo cero”, los cuales se dan por el aprovechamiento de la tasa de error (Falsa aceptación mayor que cero) y 2. Ataques tipo “Adversario”, los cuales tienen la posibilidad de que un impostor logre suplantar la identidad de un usuario legítimo y autorizado. Con base en lo indicado por el autor, igualmente se reconocen otros tipos de ataques que hacen referencia a los biométricos, entre otros, repudio, confabulación, coacción y/o denegación de servicios. Se establecen dos tipos de estándares: BioAPI y BAPI, lo anterior, con el fin de establecer parámetros para la implementación y evaluación de sistemas biométricos. Por medio de este trabajo realizado, se considera la importancia del estándar BioAPI en el momento de realizar evaluaciones a sistemas biometricos dactilares, propiamente en las API (Interfaz de programación de aplicaciones), no obstante, no se genera una descripción detallada. Para el desarrollo de futuros estudios, se considerará esta información brindada conforme la herramienta de uso.

> Los ataques “esfuerzo cero” hacen uso de la probabilidad de que dos muestras de distintas personas sean muy parecidas, lo cual es posible desde el punto de vista estadístico. Esta cuestión tiene que ver con la individualidad de un rasgo biométrico. La individualidad de un rasgo suele darse por supuesta, pero en la realidad es posible encontrarse con individuos que tienen rasgos muy parecidos, como en la Figura 14. Estadísticamente, si la Falsa Aceptación es del 1 % significa que uno de cada cien intentos de acceso fraudulento tendrá éxito. Para llevar a cabo este tipo de ataques, pueden usarse programas que sintetizan artificialmente rasgos biométricos, generando una gran cantidad de datos y ofreciéndoselos al sistema hasta que se consiga entrar. Por ejemplo, para huella dactilar existe un software de generación de imágenes sintéticas de huellas, que puede encontrarse en http://biolab.csr.unibo.it.[20]

4.1.7 Sistemas biométricos y su importancia en la Industria. Según NARDI, LOPAPA, ZITELLI y VASQUEZ[21], el sistema de voto electrónico en un futuro cercano será imprescindible, esto conforme sus beneficios a nivel de control

[19] ORTEGA GARCIA, Javier. Biometría y seguridad. Madrid: Fundación Rogelio Segovia para el desarrollo de las Telecomunicaciones, 2008. 59 p. ISBN 978-84-7402-350-3.
[20] Ibid., p. 59.
[21] NARDI, Joel, *et al*. Análisis de Riesgos, vulnerabilidades y propuestas de auditoría sobre sistemas de voto electrónico [en línea]. Rosario (Argentina): Universidad Tecnológica Nacional, noviembre 2017. [Consultado 15 de abril 2020]. Disponible en: https://www.researchgate.net/publication/321183010_Analisis_de_Riesgos_Vulnerabilidades_y_Propuestas_de_Auditoria_sobre_Sistemas_de_Voto_Electronico

evitando suplantación, entre otros. Los autores realizaron una investigación de antecedentes, requerimientos de seguridad y estudio de vulnerabilidades planteando planes de mejora y contigencia, a su vez de recuperación; igualmente se incluyen criterios de auditoria para los riesgos en mención, sin duda pertinentes ante procesos de sufragio. En el proceso de voto electrónico se proponen cuatro aspectos a tener en cuenta: 1. Verificación de que el voto se almacene correctamente. 2. Comprobar el conteo. 3. Mantener la privacidad del voto generado. 4. Evitar coerción o venta de votos.
Conforme los aspectos a tener en cuenta, se considera tres tipos de riesgo: 1. Ataque informático por medio de la detección de vulnerabilidades y fallos. 2. Datos adulterados por medio de ondas magnéticas. 3. Asociación de votos a sufrantes que efectivamente ya ejercieron su derecho.

Conforme los riesgos se plantea seis objetivos para el cumplimiento a nivel de seguridad: 1. Autenticación 2. Anonimato 3. Integridad de datos 4. Auditoría 5. Confidencialidad, Integridad y no-denegación de servicio. 6. Seguridad en la interfaz del Usuario.

Para cada uno de los riesgos propuestos, se propone realizar un plan de contingencia, recuperación y tratamiento, entre los propuestos, la utilización del protocolo SSL, algoritmo asimétrico de encriptación RSA, volcado de memoria (registro no estructurado del contenido de memoria) y bloqueo de transferencia de datos, igualmente se realiza propuestas de auditoría. Se hace referencia a la importancia de involucrar algún tipo de estándar o norma, así como a rescatar los riesgos analizados e identificados con el fin de proponer procesos de remediación.

Con lo anterior, se infiere que la biometría dactilar es considerada una opción adecuada para la seguridad de diferentes procesos. Al reconocer sus cualidades, es necesario también identificar sus riesgos y ataques que se puedan presentar. Asi mismo, entre los diferentes ataques, es importante reconocer la agresión al sensor o en su defecto el escáner como un ataque directo al sistema, también ataques indirectos, o en su defecto a módulos propios e internos.

El trabajo realizado por NARDI, Joel, LOPAPA Andrés, ZITELLI, Lucrecia y VASQUEZ, Axel, lo considero oportuno, dado que en muchas ocasiones se ha identificado alteraciones en los resultados de votación, llevando a sensaciones de incertidumbre y aún más grave, a la falta de confianza de la ciudadanía ante un estado de democracia. Es por esto, que es importante considerar este tipo de investigaciones, ya que si bien los sistemas biométricos dactilares son importantes para este tipo de procesos, es igualmente importante considerar sus riesgos.

Otro escenario, por ejemplo, hace referencia a lo acontecido el 11 de septiembre de 2001 en los Estados Unidos, donde se demuestra que las vulnerabilidades, así como las amenazas en un aeropuerto específicamente, están presentes; malas practicas en el uso de los sistemas biométricos, pueden causar tragedias catastróficas. Dado esto, por medio del análisis realizado por Moraes[22], se evaluó y analizó las diferentes soluciones enfocadas en sistemas biométricos aplicados a la seguridad aeropuertuaria, estableciendo diferentes modelos considerando su operación, aplicación y proyección, implementados en referencia a un modelo de evaluación, que está basado en métricas cómo: características en su sistema global, procedimientos para el registro de datos biométricos, tarjeta de identificación, base de datos, infraestructura e indicadores de desempeño; evaluaciones que se consideran pertinentes para sistemas biométricos en otros ambientes y escenarios. Junto a lo anterior, se realiza una evaluación de los sistemas de reconocimiento en función de: la huella digital, el iris, geometría de la mano y la cara. A partir de los estudios realizados, se evalúan fortalezas y debilidades, dando a conocer la importancia de los sistemas biométricos en diferentes sectores.

[22] MORAES, Alexandre Fernandes de. Método para avaliação da tecnologia biométrica na segurança de aeroportos [en línea]. Sao Paulo (Brasil): Universidade de São Paulo, marzo 2006. [Consultado 02 de mayo 2020]. Disponible en: https://repositorio.usp.br/item/001516079

4.1.8 Métodos de evaluación de los Sistemas biométricos (Estándares BEAT, KBOC). Conviene distinguir que por parte de Morales[23], se plantea el uso de la herramienta BEAT (Biometric Evaluation and Testing). El autor indica que es imprescindible su uso para los sistemas biométricos, conforme la búsqueda de reproducibilidad de la experimentación desarrollada; se genera la explicación de una competencia Internacional que se enfoca en la evaluación de los sistemas biométricos (KBOC – Keystroke Biometric Ongoing Competition). Para dicha competición se establece dos modalidades: 1. Sistema de pulsaciones de teclas. 2. Suministro de base de datos. Esto genera una oportunidad para comparar nuestros sistemas con los de los demás investigadores y así poder aprender unos de otros y avanzar de forma conjunta en el área. Morales[24], la biometría de tecleo hace referencia a la información de tiempo que es detallada en la dinámica de presión o no de un teclado, lo anterior, genera parámetros comportamentales de estudio. La metodología de evaluación y competición KBOC, brinda herramientas interesantes para la mejora de los sistemas biométricos dactilares, por ejemplo, si allí se evalua el comportamiento, en una huella digital esta característica puede verse reflejada en la temperatura del dedo, por tanto, se tendria un criterio adicional al verificar autenticidad.

4.1.9 Métodos de evaluación de los sistemas biométricos (NFIS y Match-on-Card). Galbally, Fierrez y Rodriguez[25], realizan la evaluación de tres escenarios: el primero (referencia) bajo circunstancias de datos biométricos reales, con huellas digitales reales, el segundo bajo datos biométricos falsos, huellas digitales falsas; un tercer escenario, se involucra con el fin de evaluar la inscripción de huellas digitales reales y huellas digitales falsas. La evaluación

[23] MORALES MORENO, Aythami. Investigación reproducible: uso de la plataforma BEAT para la evaluación tecnológica de algoritmos de reconocimiento biométrico [en línea]. Trabajo fin de grado para optar por el título de Electrónica. Universidad Autónoma de Madrid, 2016. [Consultado 3 de mayo 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/674163/Daza_Garcia_Roberto_tfg.pdf?sequence=1&isAllowed=y

[24] Ibid., p. 53.

[25] GALBALLY, Javier, *et al.* On the Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks [en línea]. Trabajo de grado para optar por el titulo de Ingeniero Informático. Universidad Autónoma de Madrid, 2009. p. 63. [Consultado 30 de marzo 2020]. Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.206.1024&rep=rep1&type=pdf

se realiza por los autores, esto por medio de sensores ópticos y sensores térmicos, logrando identificar que los dos tipos son vulnerables.

Para llevar a cabo el proceso de evaluación, se ha generado una base de datos de tamaño mediano con huellas digitales reales y sus respectivas imitaciones sintéticas, tomando como referencia el sistema de verificación de minucias de huellas digitales otorgado por la NIST. Los tres escenarios generan resultados en términos de EER y DET, adicionalmente, se concluye por el grupo investigador que los sensores ópticos arrojan mejores resultados en referencia a los métodos de evaluación propuestos por la NIST-NFIS, no obstante, estos son más vulnerables a los ataques directos. En cuanto a las crestas, son más deficientes que las minucias, no obstante, pueden llegar a ser menos vulnerables a ataques directos y adicional su resistencia es mayor a muestras de baja calidad. Esta investigación da a conocer información importante conforme resultados de la metodología de evaluacion NIST-NFIS, reconociendo el compotamiento de sensores tanto ópticos como térmicos, sin involucrarlos en un sistema de biometría dactilar; a futuro sus estudios en el sistema serán viables para considerar.

Continuando con la implementación de metodologías de validación bajo sistemas biométricos, Beisner[26], realiza un análisis experimental conforme los siguientes tipos de ataque: tipo hill-climbing y side-channel. Para con los dos tipos de ataque, se realiza un estudio del sensor térmico y del sensor óptico, por medio del software NFIS y Match-on-Card. Los resultados obtenidos, permiten corroborar la viabilidad de la generación de ataques por medio de su puntuación y tiempo existente, a su vez, los sistemas de reconocimiento de huella dactilar basados en las minucias, pueden llegar a ser potencialmente vulnerables a ataques side-channel en función del tiempo. Este tipo de estudios, complementan lo descrito por Galbally, Fierrez, Rodríguez y Gonzalez[27],

[26] BEISNER MUÑOZ, Alicia. Ataques tipo “Side-Channel” a sistemas biométricos de reconocimiento de huella dactilar [en línea]. Título de Ingeniero Informático. Universidad Autónoma de Madrid, 2010. p. 125. [Consultado 16 de Abril 2020]. Disponible en: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20100426AliciaBeisnerMunoz.pdf

[27] GALBALLY. Op. cit., p. 64.

encontrándose analogías en los resultados conforme los sensores térmicos y ópticos, con ello las crestas de huella dactilar en su grado de vulnerabilidad.

> BEISNER MUÑOZ, Alicia, propone como trabajo futuro Se propone en primer lugar la optimización de los algoritmos utilizados para un menor tiempo de cómputo y numero de iteraciones necesarias en cada ataque. Además podrían adaptarse estos sistemas al estudio de las vulnerabilidades de los sistemas biométricos multimodales combinando por ejemplo cara y huella dactilar para realizar ataques hill-climbing.[28]

Los ataques de tipo Hill-Climbing también son evaluados por NFIS de la NIST. Los ataques Hill-Climbing se sabe que buscan generar un determinado número de "plantillas" de material sintético que generan modificaciones por medio de un proceso iterativo (repetitivo) de acuerdo a una puntuación, con esto, se busca aumentar los cambios o mantenerlos; cuando el cambio se mantiene, se busca modificar aquellos que no dan resultado, incrementando el score por medio de cada proceso.

Para llevar a cabo este experimento de evaluación planteado por los autores Galbally, Fierrez Y Ortega[29], se dispone de un sistema *Finger – print Image Software* 2 (NFIS) de la NIST, el cual es un paquete de *software* público que permite implementar nuevas tecnologías de solución de huella dactilar. Los experimentos se fundamentan en el descubrimiento de una nueva vulnerabilidad, dada por el tiempo de comparación de los sistemas biométricos (que se concluye son fáciles de medir) generando posibilidades de simplificar ataques concebidos, lo anterior para vulnerar puntuaciones de similitud (dificiles de aceder). Los autores, identifican la forma de ataque *Hill-Climbing*, generando una validación de tiempos de respuesta conforme una comparación válida o no; este estudio, confirma la vulnerabilidad del sistema biométrico articulado con el proceso de evaluación involucrado.

---

[28] Ibíd., p. 93.

[29] GALBALLY, Javier; FIERREZ, Julián y ORTEGA, Javier. Análisis temporal de vulnerabilidades de los sistemas basados en huella dactilar [en línea]. Universidad Autónoma de Madrid, 2009. p. 63. [Consultado 30 de marzo 2020]. Disponible en: http://atvs.ii.uam.es/atvs/files/2010_JRBP_Galbally.pdf

Wayman[30] por su parte, afirma de acuerdo a los estudios evidenciados, que las vulnerabilidades de sistemas biométricos han dejado de ser un tema netamente científico para convertirse en un tema y aspecto de importancia global, esto por medio de diferentes iniciativas de estandarización conforme los diferentes problemas de seguridad en las aplicaciones biométricas, por ejemplo, el *Common Criteria* en documentos (*Supporting Documents*) o en su defecto la *Biometric Evaluation Methodology.*

4.1.10 Métodos de evaluación de los Sistemas biométricos conforme coeficientes FAR y FRR. Los sistemas biométricos demandan estudios de factibilidad, obligando a las compañias a generar viabilidades tanto técnicas como monetarias. Es por esto, que se hace imprescindible generar un modelo de evaluación de desempeño que justifique una inversión, utilizando tasas como FAR: *False Acceptance Rate* y FRR: *False Rejection Rate*. Gutierrez[31], puntualiza que con un modelo y estos parámetros, se obtienen datos que se esperan sean concluyentes para la aprobación de diferentes proyectos de seguridad biométrica para una compañía. Así mismo, puntualiza que, por medio del trabajo desarrollado, se logra un análisis de los diferentes métodos de evaluación de los sistemas biométricos, con ello, a nivel técnico, se expone la viabilidad de implementación de un sistema que muestra de manera clara la necesidad particular de la compañía, buscando responder a todos sus requerimientos. Por otra parte, en cuánto aspectos normativos, se realiza una verificación de estándares internacionales buscando evaluar la calidad del sistema articulado en una normativa legal. Las tasas de referencia FAR (*False Acceptance Rate*) y FRR (*False Rejection Rate*), otorgan al autor valores importantes que pueden llegar a ser presentados en un informe técnico, incluso

[30] WAYMAN, James. Biometric Evaluation Methodology Common Criteria Common Methodology for Information Technology [en línea]. 2002. [Consultado 01 de Abril 2020]. Disponible en: https://www.semanticscholar.org/paper/Biometric-Evaluation-Methodology-Common-Criteria-[-Stuart-Australia/e96c1dabba7775c9d029319ec2a769e59cf7d152#citing-papers

[31] GUTIERRES RICARDO, Jorge. Estudio de factibilidad para el control de acceso biométrico, en una empresa empleando lectores de huella digital [en línea]. Trabajo de grado para optar por el titulo de Especialista en gerencia de proyectos. Universidad de la Salle, 2007. p. 79 [Consultado 30 de marzo 2020]. Disponible en: https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1017&context=esp_gerencia_proyectos

gerencial, dando al ingeniero certeza de su proyecto, además supliendo las necesidades de seguridad presentes en una compañía. Sin duda, esto es un proceso necesario ante un proyecto que involucre un sistema de biometría dactilar.

4.1.11 Propuestas de mitigación respecto a vulnerabilidades en sistemas biométricos. GONZALÉZ, CONTRERAS, YAÑEZ[32], plantean para una Institución educativa establecer un estudio previo para las tecnologías biométricas dispuestas, posterior a ello, se propone un sistema biométrico por medio de *software* libre, además de proponer un modelo basado en un control de asistencia para la Facultad de Ingeniería de Sistemas e Informática de la Institución (UNMSM). Los autores generan un proceso de evaluación cualitativo pretendiendo establecer resultados a partir de la relación teórica conceptual de diferentes autores, a su vez, consultados.
Se hace mención en mediciones cualitativas, por tanto, son necesarias conforme estándares descritos en puntos anteriores, logrando identificar una postura en cuanto a los resultados esperados y los realmente obtenidos de acuerdo a las necesidades de la Institución u Organización.

Herramientas como aplicaciones *WEB*, tambien son consideradas por algunos autores. Por ejemplo, Incencio[33], propone el desarrollo de una aplicación *WEB* la cual permita garantizar el proceso de evaluación de los diferentes componentes biométricos del Centro de identificación y Seguridad digital (CISED). El método de evaluación se basa en la norma ISO/IEC 9126 estableciendo una serie de métricas de evaluación por medio de un *framework* que contiene un modelo, una vista y un controlador (MVC – Modelo Vista Controlador). Este *framework* es interesante dado que puntualiza en la

[32] GONZALÉZ. Op. Cit., p. 34.
[33] INCENCIO PIÑEIRO, Grettel. Sistema informático para la evaluación de atributos de calidad en componentes biométricos. [en línea]. Cuba: Universidad de Granma, 2014. Nro 8. p. 19 - 35 p. [Consultado 2 de mayo 2020]. Disponible en: https://www.3ciencias.com/wp-content/uploads/2014/03/SISTEMA-INFORMÁTICO-PARA-LA-EVALUACIÓN-DE-ATRIBUTOS-DE-CALIDAD-EN-COMPONENTES-BIOMÉTRICOS.pdf

visualización específica del procesamiento de la data, evitando ataques propios a este módulo del sistema biométrico dactilar.

Por su parte, Zurita[34], busca determinar el nivel de eficiencia de los diferentes lectores biométricos del Departamento Municipal Canton Baba en el Ecuador, lo anterior lo realiza por medio de un estudio de las vulnerabilidades de los sistemas biométricos basado en seis aspectos: secreto de la información, protección de bienes, procesos de identificación, medidas de prevención, identificación de individuos y reducción de costos. Se brindan recomendaciones en cuanto a recolección de datos y transmisión, no obstante, no hay fundamento en algún estándar o norma.

Los procesos de auditoría son igualmente importantes, pues generan un análisis de temas referentes a automatización, servicios, seguridad, protección, gestión y gobierno; dada la importancia de cumplimiento, Guaman[35], reconoce dicho proceso para la Universidad Técnica de Machala, con ello realiza un proceso de evaluación a los controles en sistemas computacionales, con ello la evaluación de la seguridad física y lógica con el fin de proteger los activos; entre los sistemas verificados, se encuentra los dispositivos biométricos para la identificación personal. La evaluación no contempla ningún estándar, no obstante, reconoce los sistemas biométricos como un aspecto fundamental para el desarrollo óptimo de procesos.

[34] ZURITA BAJAÑA, Jhonn. Nivel de eficiencia de los lectores biométricos de los departamentos del Gad Municipal del Canton Baba [en línea]. Trabajo para obtener el título de Ingeniero de Sistemas. Ecuador: Universidad Técnica de Babahoyo, 2019. p. 21 [Consultado 6 de abril 2020]. Disponible en: http://dspace.utb.edu.ec/bitstream/handle/49000/5526/-E-UTB-FAFI-SIST-000129.pdf?sequence=1&isAllowed=y

[35] GUAMAN POMA, Cindy. Universidad Técnica de Machala. Facultad de Ciencias Empresariales. Auditoría Informática De La Seguridad Física Y Lógica De Las Computadoras Del Centro De Educación Continua De La Utmach. Ecuador. 2019. [Consultado: 30 de marzo de 2020]. Disponible en: http://repositorio.utmachala.edu.ec/bitstream/48000/14931/1/E-11255_GUAMAN%20POMA%20CINDY%20ABIGAIL.pdf

Las técnicas de Benchmarkig también son consideradas como método de evaluación; Gomez; Giraldo y Giraldo[36], con el fin de evaluar diferentes sistemas biométricos, en su desarrollo de estado del arte, dan a conocer resultados interesantes por medio de esta técnica, que a futuro, brindará herramientas importantes de comparación con futuros trabajos de investigación en relación a los sistemas biométricos.

4.2 MARCO CONCEPTUAL

4.2.1 Ciberseguridad. Lanz[37], afirma que la Ciberseguridad se define como la protección de activos de información por medio del tratamiento de las amenazas que ponen en riesgo la disponibilidad, confidencialidad e integridad de la información por medio de su procesamiento, almacenamiento y transporte.

Relacionado al concepto de Ciberseguridad, existe la vulnerabilidad informática, definida como un defecto en un sistema provocando su exposición ante atacantes. Trujillo[38] nos hace saber, que este tipo de debilidades pueden estar presentes en un ordenador o conjunto de diferentes procedimientos. El proceso de mitigación de estas vulnerabilidades se emplea como las medidas aplicadas de manera proactiva con el fin de evitar cualquier tipo de evento que potencialmente sea un desastre en referencia a la seguridad de la información.

[36] GOMEZ RAMIREZ, Diana y GIRALDO GIRALDO, Andrea. Estado del arte de la seguridad en sistemas biométricos [en línea]. Proyecto de Grado Monografía para Optar por el Título de Especialista en Seguridad Informática. Bogotá (Colombia): Universidad Nacional Abierta y a Distancia – UNAD, 2017. p. 94. [Consultado 28 de marzo 2020]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14348/1/52752700.pdf

[37] LANZ, Leonel. Que es la ciberseguridad. [sitio web]. España: OpenWebinars. [Consultado 01 mayo de 2020]. Disponible en: https://openwebinars.net/blog/que-es-la-ciberseguridad/

[38] TRUJILLO TELLEZ, Fernando. Mitigación de riesgos. [sitio web]. Colombia. [Consultado 01 de mayo 2020]. Disponible en: http://riesgosyplanesdecontingencia.blogspot.com/2016/09/mitigacion-de-riesgos.html

4.2.2 Biometría. Medina[39] afirma, que la biometría es la ciencia y además tecnología que se encarga de generar una medición y análisis de datos biofísicos de los seres humanos. Esta tecnología estudia los rasgos físicos de una persona. Los sistemas biométricos cuentan en su sistema con un sensor, definido como un transductor que realiza la transformación de un aspecto físico de un ser humano en una señal eléctrica. GRUPO NOVELEC[40], argumenta que los sensores generalmente realizan la medición de aspectos como la luz, temperatura, latencia, o en su defecto, estímulos energéticos.

> Un sensor biométrico es un transductor que transforma un rasgo físico y concreto de un ser humano en una señal eléctrica. Por lo general, el sensor interpreta o mide aspectos como la luz, la temperatura, la velocidad (en el caso de una voz, por ejemplo), y otro tipo de estímulos energéticos. Esto se consigue mediante sofisticadas combinaciones de redes de sensores y cámaras digitales o micrófonos cuya imagen o sonido son de alta precisión.[41]

Existen diferentes tipos de biometría. Hernandez[42], genera un marco conceptual explicativo conforme los tipos de biometría: estática (rasgos físicos), biometría multimodal (rasgos físicos y comportamiento) y dinámica (comportamientos). El autor propone una evaluación completa de los sistemas, esto teniendo en cuenta cinco aspectos: 1. Rendimiento identificación automática de personas. 2. Seguridad, integridad y confidencialidad. 3. Fiabilidad y mantenimiento. 4. Aceptación y facilidad de manejo. 5. Estimación de costes y beneficios.

4.2.3 Coeficientes de evaluación biométrica. Además de los tipos de biometría existentes, existen coeficientes con el fin de generar procesos de evaluación: FNMR (False Non-Match Rate), FMR (False Match Rate), FRR (False Reject Rate), FAR (False Accept Rate), EER (Error Equal Rate).

---

[39] MEDINA, Matias. ¿Qué es la biometría?. [sitio web]. [Consultado 27 de abril 2020]. Disponible en: https://www.mejoresvpn.pro/que-es-la-biometria/

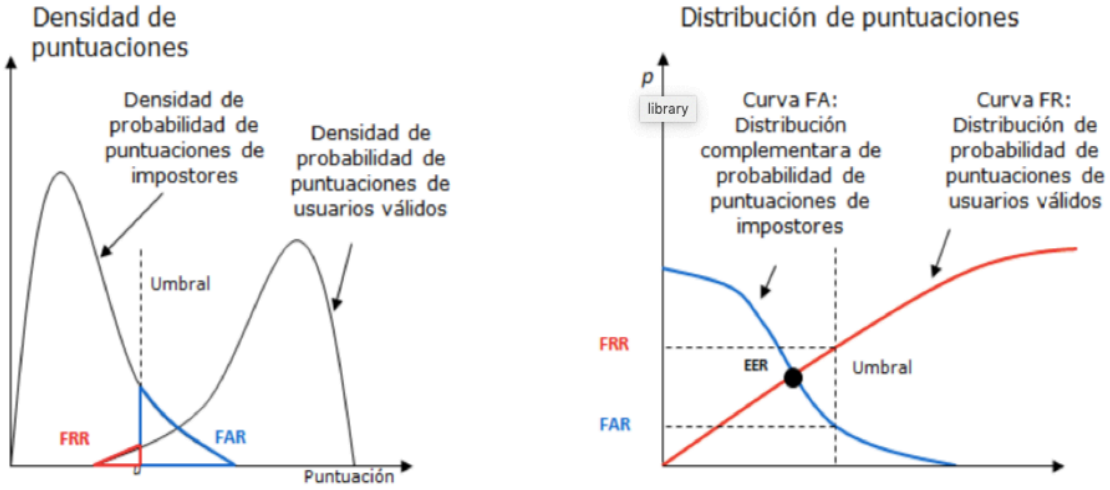
[40] GRUPO NOVELEC. ¿Cómo funciona un sensor biométrico? [blog]. España. [Consultado 17 de mayo 2020]. Disponible en: https://blog.gruponovelec.com/redes-vdi/como-funciona-sensor-biometrico/

[41] Ibid., p. 1.

[42] HERNANDEZ PAZ, Carlos. Estudio del rendimiento biométrico de dispositivos de huella dactilar. Análisis de la influencia del tamaño de la muestra [en línea]. Grado Ingeniería electrónica Industrial. Universidad Carlos III de Madrid, 2015. p. 72 [Consultado 30 de marzo 2020]. Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/23771/TFG_Carlos_Hernandez_Paz_2015.pdf

En la figura tres se observa el lugar del indicador EER, que entre menor sea más exacto es el sistema.

Figura 3. Rendimiento biométrico de dispositivos de huella dactilar.



Fuente: BEISNER MUÑOZ, Alicia. Estudio del rendimiento biométrico de dispositivos de huella dactilar. [En nínea]. Ataques tipo “side-channel” a Sistemas biométricos de reconocimiento de huella dactilar. España. Universidad Autónoma de Madrid 2010. p. 25. (Recuperado en 16 de abril 2020). Disponible en: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20100426AliciaBeisnerMunoz.pdf

4.2.4 Sistemas de referencia de evaluación biométrica. El sistema de referencia NFIS para la modalidad de huellas dactilares, es el *software* de imagen de huellas dactilares recomendado por la NIST. Petrovska[43] nos hace saber que su desarrollo se fundamenta para la Oficina Federal de Investigaciones (FBI), buscando facilitar y apoyar la manipulación automática y el procesamiento de imágenes de huellas digitales. El código fuente NIST da más de 50 utilidades o paquetes diferentes y una extensa guía del usuario se distribuyen de forma gratuita.

Los diferentes sistemas de control de acceso, que se basan en biometría, actúan como una herramienta necesaria contra los desafíos para la autenticación que

[43] PETROVSKA, Dijana y CHOLLET, Gerard. Biometric Reference Systems and Performance Evaluation. Estados Unidos de América: Springer, 2009. 389 p. ISBN 978-1-84800-292-0

enfrentan las organizaciones. Son muchas las ventajas del sistema biométrico, no obstante, aún existen vulnerabilidades, que disminuyen su seguridad. Lo anterior, lleva a proponer un nuevo enfoque para abordar estos problemas y desafíos abiertos para la seguridad de los datos biométricos: Hadid[44] afirma que el sistema *Match On Card*, es utilizado para almacenar credenciales biométricas. *Match On Card*, en el marco biométrico, bloquea los datos dentro del microcontrolador de una tarjeta electrónica, lo que conlleva a disminución de riesgos si se presenta robo o hurto. Es rápido y preciso, además de equilibrado.

El Centro Europeo de Postgrados[45] nos comparte que BEAT (*Biometrics Evaluation and Testing*), promueve, entre otras, la implementación de una plataforma en línea y abierta para evaluar de manera transparente los sistemas biométricos, diseñando protocolos y herramientas para el análisis de vulnerabilidades, en conjunto a documentos de estandarización para evaluaciones de criterios comunes. El impacto de esta planificación se da en tres partes: confiabilidad en los sistemas biométricos que se estandarizan y comparan, lo que puede conducir a un aumento significativo en su proyección de rendimiento; transferencia de tecnología conforme investigaciones a las organizaciones, con el fin de promover marcos interoperable; por último, las autoridades y los tomadores de decisiones se documentan más sobre el progreso realizado en biometría a medida que los resultados impactan en los estándares.

Morales[46], a su vez, indica que KBOC (*Keystroke Biometrics OnGoing Competition),* es una competencia organizada con el fin de establecer una línea base conforme la autenticación de personas usando la biometría por pulsación

[44] HADID, Abdenour. Face Biometrics Under Spoofing Attacks: Vulnerabilities, Countermeasures, Open Issues, and Research Directions [en línea]. IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, 2014. p. 113-118. [Consultado 17 de mayo 2020]. Disponible en: https://www.researchgate.net/publication/286732400_Face_Biometrics_Under_Spoofing_Attacks_Vulnerabilities_Countermeasures_Open_Issues_and_Research_Directions/citation/download

[45] EUROPEAN COMMISION. Biometrics Evaluation and System. Londres. Seventh Framework Programme. 2012. [Consultado 17 de mayo de 2020]. Disponible en: https://cordis.europa.eu/project/id/284989

[46] MORALES, Aythami, *et al.* Keystroke Biometrics Ongoing Competition [en línea]. 2016. [Consultado 17 de mayo 2020]. Disponible en: https://www.idiap.ch/~aanjos/papers/ieee-access-2016.pdf

de teclas, afirma, que *BEAT* incluye una de las bases de datos de pulsaciones de teclas más grandes disponibles públicamente en función de un escenario de texto fijo. Por medio de este mecanismo, se busca identificar patrones propios de cada Individuo buscando fortalecer la autenticidad y con ello los procesos de autenticación, obteniendo beneficios de esta información y articulando con KBOC.

4.2.5 Cuadrante mágico de Gartner. El centro Europeo de Postgrado[47], afirma que el cuadrante mágico de *Gartner* genera una evaluación de herramientas bajo criterios establecidos a fabricantes. Los principales aspectos evaluados: producto/servicio, viabilidad (finanzas, estrategias, organización), precios, capacidad de respuesta, marketing, experiencia del Cliente y operaciones (metas y compromisos).

4.3 MARCO LEGAL

Las vulnerabilidades propias sobre sistemas biométricos no sólo generan implicaciones a nivel operativo y organizacional, legalmente se tiene repercusiones claras.

4.3.1 Ley 527 de 1999. La ley 527 de 1999, por la cual el Congreso de la República de Colombia[48] intenta evitar los delitos informáticos, define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, además se establecen las entidades de certificación.

[47] CENTRO EUROPEO DE POSTGRADO. ¿Qué es el cuadrante mágico de Gartner? [blog]. España. [Cosultado 17 de mayo 2020]. Disponible en: https://www.ceupe.com/blog/que-es-el-cuadrante-magico-de-gartner.html

[48] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527 de 1999. (21, agosto, 1999). Reglamentos de acceso y uso de mensajes de datos. En: Diario oficial de Congreso de Colombia. Bogotá D.C., 1999. 3 p.

4.3.2 Ley 1266 de 2008. La legislación Colombiana estipula la Ley 1266 de 2008, por medio de la cual la Corte Constitucional[49] dictan disposiciones conforme habeas data regulando el manejo de la información personal contenida en bases de datos, entre otras, información financiera, crediticia y comercial. Ante violaciones, se estipula sanciones por parte de la Superintendencia de Industria y Comercio, así como por la superintendencia Financiera, en su alcance, generando multas de carácter personal e Institucional hasta por 1.500 salarios mínimos mensuales legales vigentes, o en su defecto la clausura de establecimientos.

4.3.3 Ley 1273 de 2009. La Ley 1273 de 2009, en la cual el Ministerio de las tecnologías y la información[50], incentiva a modificar el código penal para la tipificación de varios delitos informáticos. Llamada la ley protección de la información y de los datos, endurece las penas hasta en 1.500 salarios mínimos mensuales legales vigentes y penas de hasta 120 meses.
La ley de protección de la información y datos, en el artículo 269ª, se refiere al acceso abusivo a un sistema informático. El articulo 269C, se refiere a la interceptación de datos informáticos sin una orden judicial. Artículo 269F, se refiere a la violación de datos personales. Artículo 269G, se reconocen los indicadores de compromiso que buscan obtención de información personal por medio de suplantación.

5. DESARROLLO DE OBJETIVOS

5.1 DESARROLLO DE OBJETIVO 1

5.1.1 Los sistemas biométricos dactilares y sus características. Los

[49] COLOMBIA. CORTE CONSITUCIONAL. Sentencia C-1011 de 2008. (31, diciembre, 2008). Habeas data y regulación del manejo de la información. En: Gaceta de la Corte Constitucional. Bogotá D.C. Corte Constitucional y consejo de la judicatura, 2008. 9 p.
[50] COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1273 de 2009. (5, enero, 2009). De la protección de la información y los datos. En: MinTIC. Bogotá D.C, 2009. 4 p.

sistemas biométricos dactilares hacen parte del grupo de la biometría estática. Estos sistemas, fundamentan su aplicabilidad en la validación de características exclusivas de huellas dactilares, con ello, identificando características propias que se basan en las siguientes propiedades: 1. Universalidad, considerando que las características biométricas aplican para todos los individuos; 2. Unicidad, considerando que cada individuo tiene características que no se repiten. 3. Permanencia, este tipo de características no cambian en el corto plazo. 4. Inmutabilidad, las características del individuo no cambian a lo largo del tiempo. 5. Mensurabilidad, en el cual se considera que las características pueden ser representadas de manera cuantitativa. 6. Rendimiento, se permite el reconocimiento de manera precisa y oportuna. 7. Aceptabilidad, en referencia a que las características deben ser de calidad para ser aceptadas. 8. Invulnerabilidad, los rasgos identificados son contundentes frente a otros métodos de acceso fraudulentos. Conforme estás propiedades, las crestas papilares, surcos interpapilares, rigurosidades, depresiones, puntos, islotes, horquillas, interrupciones, bifurcaciones, crestas, minutas, poros, entre otros, hacen parte de las características obtenidas por los sistemas en las huellas dactilares de cada individuo.

Se consideran tres tipos de características: como primera característica se tiene las crestas de una huella dactilar, las cuales se ubican en el dedo generando una descripción de diferentes líneas paralelas, considerando que existen regiones con formas singulares que presentan alta curvatura. Las singularidades se clasifican en: 1. Lazo, representado por el símbolo U; 2. Delta, representado por el símbolo Δ, patrones que forman un pico con forma triangular; 3. Espiral, representado con el símbolo O, formas de pequeños círculos.

Como segunda característica se tienen las minutas, definidas como la variación de crestas en una huella digital. Está característica es usualmente utilizada en los algoritmos de *matching*; este tipo de características se considera imprescindible para la autenticidad, lo anterior, considerando que es la densidad de sus puntos los que apoyan su propiedad de unicidad.

Por último, los poros, propiedades de la piel que tiene un tamaño entre 60 y 250 micras, que son suficientes para identificar un individuo. Este tipo de identificación ha sido reemplazada de manera progresiva, lo anterior conforme a que se necesita escáneres de alta resolución para lograr obtener una imagen de buena calidad.

Ocaña[51], indica que existen diferentes técnicas de comparación de huellas dactilares, entre ellas: la técnica de verificación de puntos de minucia, que enfoca esfuerzos en pequeños detalles de las huellas verificando su colocación en el dedo. Por medio de este tipo de características, se valida la discontinuidad de las diferentes líneas de la superficie propia de una huella dactilar; es de considerar, que existen 18 tipos de minucias que se incluyen en las características anteriormente mencionadas.

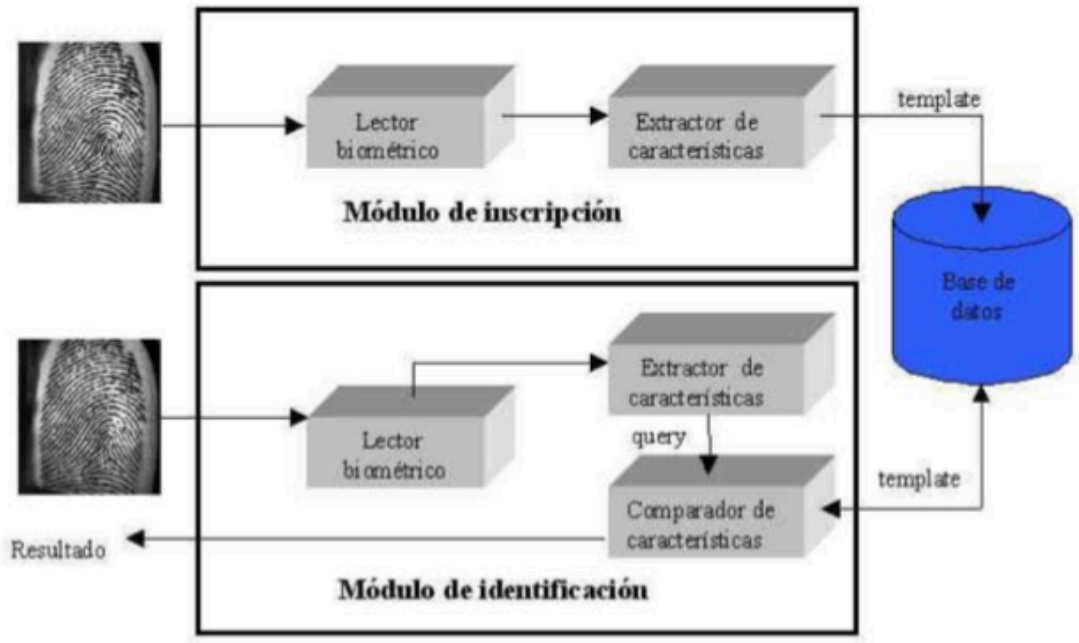
Por su parte, se tiene la técnica del método de correlación, que además de validar minucias en el dedo, verifica con exactitud su ubicación en el mismo, además de la ubicación respecto a otras minucias identificadas. La técnica de correlación igualmente realiza una validación de los pixeles de las imágenes obtenidas de las huellas dactilares, lo anterior con el fin de realizar procesos de comparación.

5.1.2 Sistemas biométricos dactilares y sus componentes. El sistema biométrico dactilar cuenta con cinco fases. Inicialmente se tiene la fase de lectura por parte del biométrico; en esta fase las huellas se obtienen del dedo del individuo por parte de la superficie de un sensor electrónico, sensor que puede ser de tipo óptico, capacitivo o ultrasónico; se obtiene al finalizar esta captura una imagen. Una segunda fase, hace referencia a la extracción de características, encargada de tomar la imagen obtenida por el sensor y realizar

[51] OCAÑA DIEZ DE LA TORRE, Manuel. Algoritmos de Matching entre huellas dactilares [en línea]. Trabajo de grado para optar por el título de Ingeniería electrónica y automática industrial. Universidad Politécnica de Madrid, 2017. 100 p. [Consultado 17 de mayo 2020]. Disponible en: http://oa.upm.es/47958/1/TFG_MANUEL_OCANA_DIEZ_DE_LA_TORRE.pdf

su procesamiento identificando características de huella, como las descritas con anterioridad. La tercera fase, se normalizan los datos obtenidos: esta data es indexada conforme una estructura definida. Cuarta fase, se genera un almacenamiento de la información en un servidor de base de datos, cuyo repositorio se alimentará conforme las huellas dactilares obtenidas. Como quinta y última fase, se genera el proceso de comparación de características; proceso que realiza una validación de la huella obtenida por el sensor, y el repositorio alojada en la base de datos.[52]

Figura 4. Fases de un sistema biométrico dactilar.



Fuente: OCAÑA DIEZ DE LA TORRE, Manuel. Fases de un sistema biométrico dactilar [En línea]. Algoritmos de Matching entre huellas dactilares. España. 2017. p. 16. (Recuperado en 17 de mayo 2020). Disponible en: http://oa.upm.es/47958/1/TFG_MANUEL_OCANA_DIEZ_DE_LA_TORRE.pdf

[52] Ibid., p. 16.

5.1.2.1 Los sensores. Los sensores de los sistemas biométricos dactilares pueden ser de tres tipos: ópticos, estado sólido y ultrasónico.

Los sensores de tipo óptico, se basan en la reflexión de la luz sobre la yema del dedo del individuo. Dentro de este tipo de sensores, se tienen: Los basados en FTIR (Espectroscopia infrarroja por transformada de Fourier), técnica antigua y con uso frecuente; su funcionamiento inicia en el momento en que se apoya el dedo sobre el cristal dispuesto por el sensor, nombrado prisma; en ese momento se proyecta un haz de luz por medio del cristal. Se tiene los sensores basados en fibra óptica, los cuales tiene una distribución bidimensional cuya incidencia se da de manera perpendicular con un haz de luz sobre el dedo del individuo. Por otra parte, los sensores de tipo electro-ópticos, compuestos por dos capas: la primera, compuesta por un polímero que emite luz proporcional al valor de voltaje aplicado sobre un lado del dedo; la segunda capa, generando la verificación de diferencias de crestas y valles por medio de un haz de luz; por último, los sensores sin contacto, basados en cámaras que no producen contacto entre dedo y sensor.

Los sensores de tipo sólido, se desarrollaron en la década de 1980, siendo utilizados comercialmente en la década de 1990. Se tiene cuatro tipos de sensores de este tipo: sensores térmicos, capacitivos, de campo eléctrico y piezoeléctricos. Los sensores capacitivos, su funcionamiento se basa en microcapacitores que se complementan con un dieléctrico (aislante), que por medio de placas conductoras realizan medidas de voltaje cuando se genera apoyo del dedo del individuo, logrando asignar valores a las crestas y valles; los sensores de tipo térmicos, están constituidos por materiales termoeléctricos los cuales generan corrientes eléctricas aprovechando los cambios de temperatura; adicionalmente, los sensores de campo eléctrico, su composición se encuentra constituida por un anillo que emite señales sinusoidales con baja potencia. Las diferentes amplitudes de las señales se producen conforme las diferencias entre crestas y valles; los sensores de tipo piezoeléctricos, sensibles a las deformaciones ejercidas por el dedo del individuo al apoyarse sobre un elemento específico. Por último, los sensores ultrasónicos, logran obtener imágenes de alta definición de las huellas; su trabajo se focaliza en la exploración a detalle de

la superficie dactilar del dedo del individuo por medio de pulsos ultrasónicos. Las diferencias se obtienen por el eco entre crestas y valles.[53]

5.1.2.2 El extractor de características. Posterior al proceso de obtención de la huella dactilar, se genera el proceso de extracción de características por medio de diferentes algoritmos con el fin de obtener minutas y características particulares.

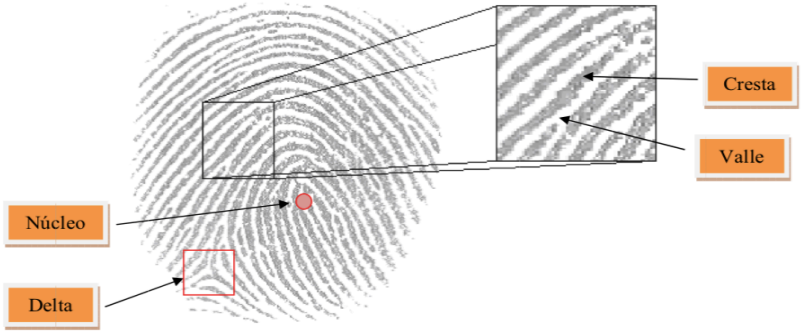
Este proceso contempla cinco fases: la primera fase hace referencia a la normalización, etapa en la cual se toma la imagen y se modifica con el fin de llevar a un valor de luminancia determinado; lo anterior ayuda a una mejor visualización de cada pixel. Como segunda fase, se tiene el proceso de segmentación, proceso en el que se toma la imagen normalizada tomando de esta la parte que interesa, de manera que se elimine lo restante. Tercera fase, proceso encargado de la orientación de las crestas dentro de la huella dactilar, permitiendo dividir la imagen por bloques conforme un tamaño determinado. Como cuarta fase, el proceso de filtrado y binarización, que consiste en tomar la imagen que ya fue orientada y filtrada, con esto, considerar aquellos píxeles que no han sido segmentados, considerando lo demás blanco. Como última fase, se tiene la etapa de adelgazamiento, proceso en el cual se realiza la disminución de grosor a un pixel. Ya concluido esto, se procede a la toma de minutas y zonas particulares.

Figura 5. Proceso de extracción de minutas y zonas de huellas dactilares.

[53] Ibid., p. 22.

Fuente: OCAÑA DIEZ DE LA TORRE, Manuel. Fases de un sistema biométrico dactilar [En línea]. Algoritmos de Matching entre huellas dactilares. España. 2017. p. 22. (Recuperado en 17 de mayo 2020). Disponible en: http://oa.upm.es/47958/1/TFG_MANUEL_OCANA_DIEZ_DE_LA_TORRE.pdf

Figura 6. Principales características de la huella digital.



Fuente: CARBALLO DOMINGUEZ, Sara. Principales características de la huella digital. [En línea]. Ataques indirectos a sistemas de reconocimiento de huella dactilar basados en los tiempos de comparación algorítmica. España. Universidad Autónoma de Madrid. 2009. p. 19. (Recuperado en 28 de marzo de 2020). Disponible en: https://repositorio.uam.es/handle/10486/9951

5.1.2.3 Comparador de características. Este proceso busca identificar el grado de similitud de las huellas dactilares. Se tiene tres técnicas para lograrlo: 1. Técnicas basadas en minutas; 2. Técnicas basadas en estructura de crestas; 3. Técnicas basadas en la información.

Inicialmente la técnica que se basa en minucias busca realizar una comparación tipo euclídea (construcciones geométricas utilizando reglas y brújulas). El proceso realiza transformaciones matemáticas en los diferentes patrones evidenciados, con esto, se busca un grado de similitud. Los métodos iterativos son considerados fiables, por tanto, como ejemplo a estás técnicas se tiene: 1. Técnicas de relajación, la cual consiste en desplazar un patrón de puntos sobre otros puntos, logrando modificar las distancias entre parejas de minutas, por tanto, este valor de distancia queda parametrizado encontrando un grado de

similitud. 2. Técnica de alineamiento de patrones: cuyo estudio se basa en identificar todas las posibles combinaciones entre dos huellas, método costoso en comparación a otros. 3. Técnica basada en transformada de Hough: se genera un comparativo en la detección de máximos identificando las minutas de la huella dactilar en comparación con la huella almacenada; este proceso busca valores de solapamiento obteniendo un *score* comparativo. 4. Técnicas basadas en grafos: generando comparaciones topológicas (propiedades de los cuerpos geométricos).

Por su parte, la técnica basada en estructura de crestas, realiza las comparaciones teniendo en cuenta técnicas de correlación entre imágenes de huellas dactilares. Se busca un grado de similitud, buscando su valor máximo cuando existe coincidencia. Este tipo de algoritmo se complementa con tres tipos de técnicas: inicialmente las técnicas propias en el dominio de la frecuencia, en la cual se calcula la transformada de FFT de las huellas dactilares a comparar; como segunda técnica complementaria, se tiene las basadas en muestreo circular, identificando vectores característicos de las huellas; por último, otras técnicas en general, que usan la estructura de las crestas conforme sus pixeles.

Por último, las técnicas basadas en la información de la textura de la huella, generándose cuatro etapas: 1. Determinación de punto de referencia en las regiones propias de la huella. 2. Mallado sobre las regiones identificadas. 3. Filtrado de la región en ocho direcciones. 4. Cálculo de la desviación conforme los grises obtenidos en la huella.[54]

5.1.3 Desafíos de nuevas tecnologías en sistemas biométricos dactilares. A nivel de Gobierno, diferentes países han optado por tecnologías de biometría, en particular dactilar, con el fin de fortalecer procesos como entrega de beneficios a ciudadanos, identificación de fraude, suplantación y toda clase de delitos; en la actualidad, diferentes Gobiernos se encuentran motivados a llevar a cabo proyectos que busquen fortalecer la biometría digital que involucre a la totalidad de ciudadanos. Es por esto, que establecer una identidad se está

[54] Ibid., p. 25.

volviendo un proceso imprescindible; considerar que alguien es, quien dice ser, que está autorizado, que tiene delitos, si tiene permiso para conducir o en su defecto, tiene permiso de ingreso a un territorio.

A nivel empresarial, las compañías buscan fortalecer sus procesos por medio de las huellas dactilares; anualmente, se tiene conocimiento que la inversión en tecnología biométrica crece, es por tanto, que ya se reemplazan tarjetas o llaves de acceso, por sistemas biométricos que disminuyen gastos operacionales y con ello se fortalecen procesos de acceso, así mismo, las compañías generarían los pagos de productos y servicios por medios biométricos; igualmente, los seguros de sus colaboradores serán corroborados por sistemas biométricos.

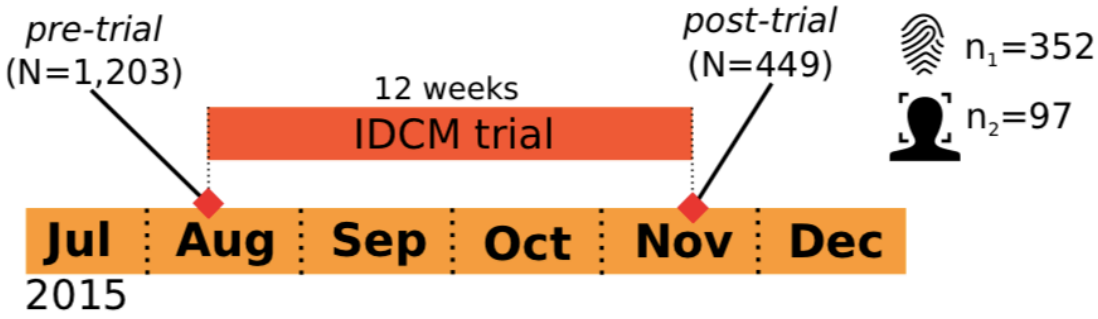
Como ciudadanos, a futuro se verán reflejados cambios significativos que cambiarán muchas costumbres del día a día. No serán necesarias las tarjetas de crédito, en ese sentido, las credenciales de acceso, como correo electrónico, portales web, no se utilizarían, como consecuencia, se anularía las credenciales de usuario y contraseña. Estudio realizado por *Mastercard* y la Universidad de Oxford[55], indica que el 93% de la totalidad de consumidores considera que los sistemas biométricos permitirán su identificación para los procesos de pagos, método considerado seguro por el 93% de los encuestados.

En la figura 6 se logra observar un estudio por Loviss[56] de tres meses en el cual 352 Usuarios utilizaron autenticación de huella dactilar, el restante identificación facial; este estudio refleja el resultado anteriormente descrito conforme las tendencias a futuro del uso de los sistemas biométricos.

Figura 6. Línea de tiempo estudio por un periodo de tres meses uso de Mastercard Identity Check Mobile.

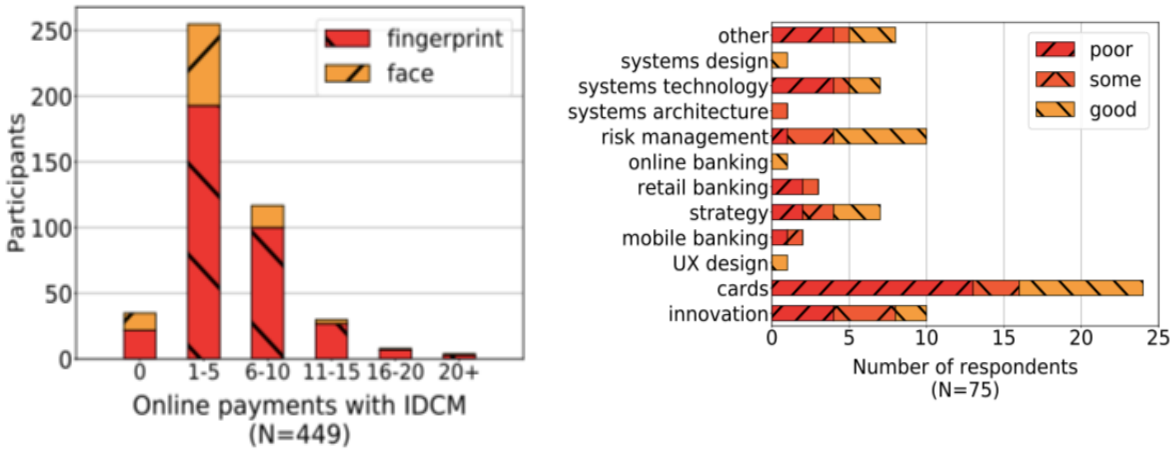
[55] LOVISS, Giulio, *et al.* Mobile Biometrics in Financial Services: A Five Factor Framework [en línea]. Estados Unidos de América: Universidad de Oxford, p. 3. [Consultado 17 de mayo 2020]. Disponible en: http://www.cs.ox.ac.uk/files/9113/Mobile%20Biometrics%20in%20Financial%20Services.pdf

[56] Ibid., p. 4.



Fuente: LOVISS, Giulio; MALIK, Raghav; SLUGANOVIC, Ivo; ROESCHLIN, Marc; TRUEMAN Paul; MARTINOVIC, Ivan. Mobile Biometrics in Financial Services: A Five Factor Framework [En línea]. USA: Department of Computer Science. Universidad de Oxford. p. 3. [Recuperado en 17 de mayo de 2020]. Disponible en: http://www.cs.ox.ac.uk/files/9113/Mobile%20Biometrics%20in%20Financial%20Services.pdf

Figura 7. Relación Usuarios que realizan un número de pagos en línea determinado y uso de tarjeta de crédito con autenticación biométrica.



Fuente: LOVISS, Giulio; MALIK, Raghav; SLUGANOVIC, Ivo; ROESCHLIN, Marc; TRUEMAN Paul; MARTINOVIC, Ivan. Relación Usuarios pagos en línea. Mobile Biometrics in Financial Services: A Five Factor Framework [imagen]. USA: Department of Computer Science. Universidad de Oxford. p. 3. [Recuperado en 17 de mayo de 2020]. Disponible en:

http://www.cs.ox.ac.uk/files/9113/Mobile%20Biometrics%20in%20Financial%20Services.pdf

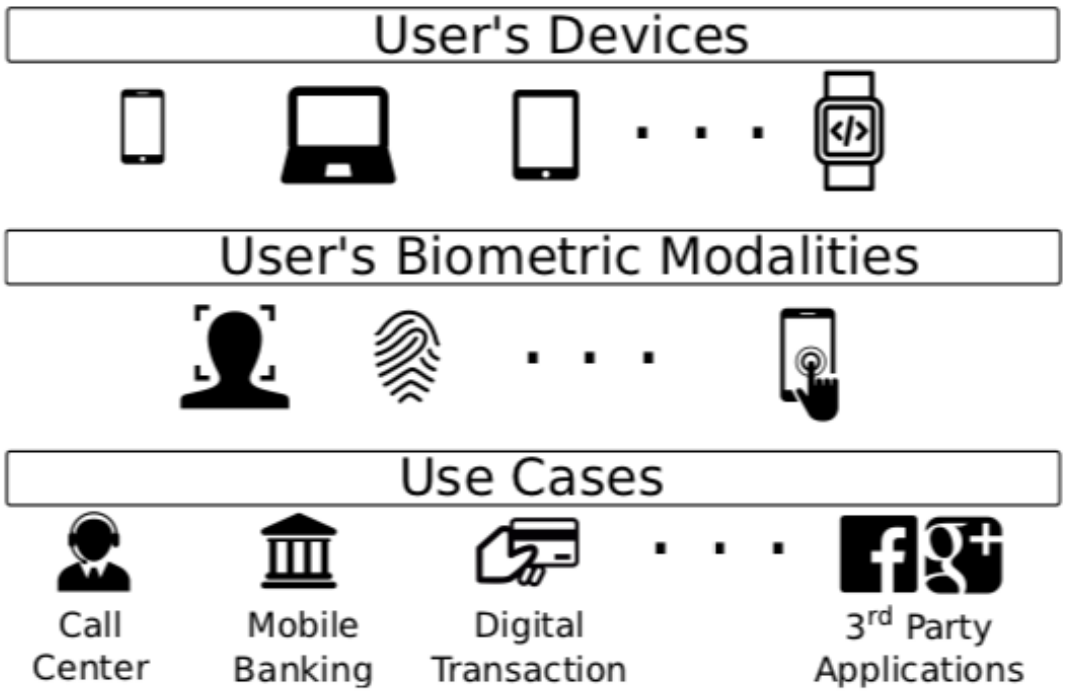
A nivel técnico, de acuerdo a los estudios realizados, a futuro se está considerando en los sistemas biométricos, conforme el desarrollo de los algoritmos de comparación, patrones DELTA, LOOP y CORE, propios de las características de las huellas dactilares y que se identifican en la búsqueda de información conforme características de los sistemas. Estos parámetros son fundamentales, dado que al incluir nuevos elementos de comparación con el fin de mejorar la eficiencia de validación, se evita escenarios de respuesta que involucren huellas legítimas que son rechazadas e intrusos que son aceptados.

Igualmente, Ocaña[57] considera realizar toma de huellas dactilares para varios dedos, de manera que se tenga un procesamiento de diferentes muestras permitiendo resultados con valores mínimos de incertidumbre.

5.1.4 Aplicabilidad de los sistemas biométricos dactilares. La biometría informática es considerada actualmente un tema de trascendencia, conforme la existencia y creación de diferentes aplicaciones y estudios de investigación, además de la demanda del mercado que crece como solución de seguridad a organizaciones. La aplicabilidad de los sistemas biométricos dactilares involucra diferentes dispositivos en los cuales se genera la toma de muestras dactilares, con esto, los casos de uso, entre otro, se tiene: bancos, compras, transacciones y cuentas.

[57] OCAÑA DIEZ DE LA TORRE. Óp. cit., p. 83.

Figura 8. Aplicabilidad sistemas biométricos dactilares en diferentes sectores.

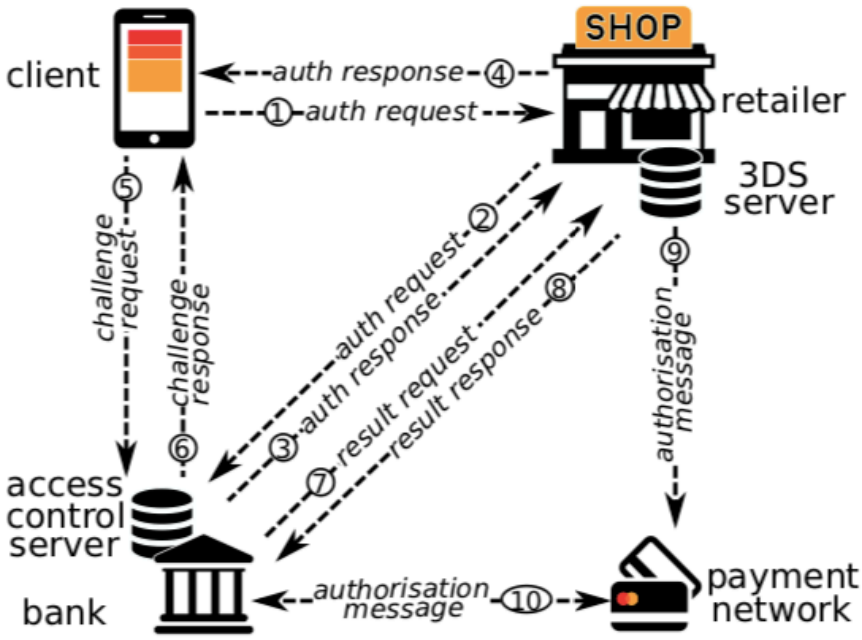


Fuente: LOVISS, Giulio; MALIK, Raghav; SLUGANOVIC, Ivo; ROESCHLIN, Marc; TRUEMAN Paul; MARTINOVIC, Ivan. Mobile Biometrics in Financial Services: A Five Factor Framework [imagen]. USA: Department of Computer Science. Universidad de Oxford. p. 8. [Recuperado en 17 de mayo 2020]. Disponible en: http://www.cs.ox.ac.uk/files/9113/Mobile%20Biometrics%20in%20Financial%20Services.pdf

A nivel Gobierno, se tiene la necesidad de verificar identidad en procesos, por ejemplo, de voto electrónico, mitigación de fraudes, entre otros, además los que implican el manejo de dinero público; a nivel empresarial y privado, conforme los estándares vigentes que pretenden brindar competitividad a las compañías en su negocio, se busca mejorar su postura en referencia a seguridad de la información. Por su parte, como ciudadanos, los sistemas biométricos se involucran en el procesamiento de pagos, bien sea por medio débito o crédito, compras y acceso a portales y cuentas.[58]

[58] LOVISS, *et al*. Op. cit., p. 3.

Figura 9. Uso y aplicabilidad de sistemas biométricos.



Fuente: LOVISS, Giulio; MALIK, Raghav; SLUGANOVIC, Ivo; ROESCHLIN, Marc; TRUEMAN Paul; MARTINOVIC, Ivan. Mobile Biometrics in Financial Services: A Five Factor Framework [imagen]. USA: Department of Computer Science. Universidad de Oxford. p. 3. [Recuperado en 17 de mayo 2020]. Disponible en: http://www.cs.ox.ac.uk/files/9113/Mobile%20Biometrics%20in%20Financial%20Services.pdf

Según un estudio por parte de IBM[59], un 67% de los Usuarios de *smarthphone* se sienten más seguros utilizando tecnologías biométricas para los procesos de autenticación; el 87% de los encuestados manifiesta que a futuro se sentirán cómodos y seguros utilizando este tipo de métodos de autenticación; 44% de los encuestados considera seguro el sistema de huella dactilar; por último, el 78% de la población del continente asiático usa tecnologías biométricas. Por su parte, un estudio recopilado por COMPUTERWORLD[60], *ViewPost* (Organización de

[59] IBM. Las contraseñas son el pasado: los jóvenes prefieren usar la huella dactilar, citado por EL MUNDO España. Madrid: 2018. [Consulta 17 de mayo 2020]. Disponible en: https://www.elmundo.es/tecnologia/2018/01/29/5a6f0791e2704eee408b4600.html

[60] ViewPost. La autenticación biométrica se impone entre los más jóvenes, citado por COMPUTERWORLD. Madrid: 2018. [Consulta 18 de mayo 2020]. Disponible en: https://cso.computerworld.es/seguridad-movil/la-autenticacion-biometrica-se-impone-entre-los-mas-jovenes

pagos vía electrónica), de 1.000 personas consultadas, el 80% apoya los pagos biométricos y el 50% considera que los sistemas biométricos serán utilizados a un corto plazo para realizar pagos electrónicos. La consultora *Technavio*[61] conforme una investigación realizada, pronostica que los puntos de venta que ofrecen sistemas de seguridad biométrica crecerán con una tasa anual del 28% para el año 2021.

Un informe revelado por *Global Market Insights*[62] (Investigaciones de mercado), proyecta que el mercado global superará los 50 millones de dólares para el año 2024, esto como respuesta a las diferentes iniciativas gubernamentales nacientes en el mundo; adicionalmente, el 30% del mercado será para Norteamérica en cuanto a sistemas biométricos se refiere.

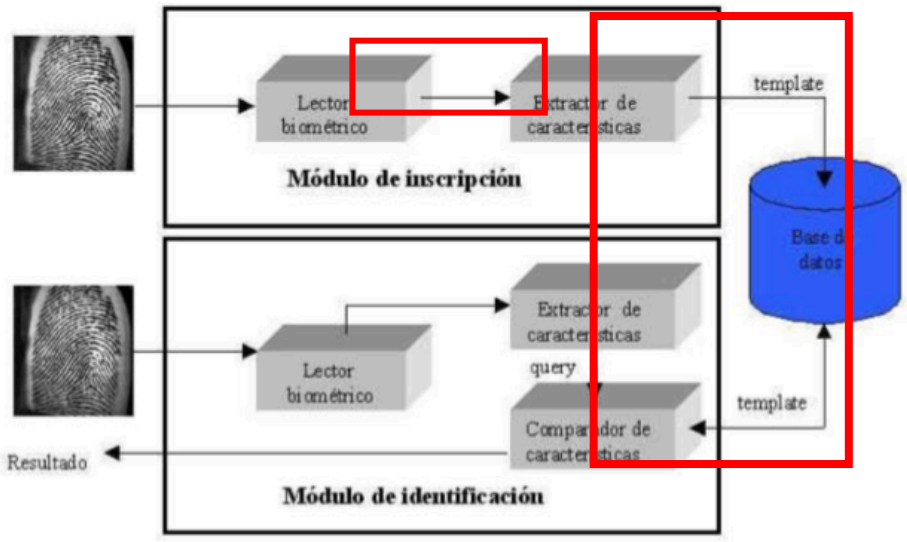
Las anteriores investigaciones y con esto, los datos conocidos confirman las deducciones anteriores respecto al uso actual y a futuro de los sistemas biométricos dactilares de autenticación.

6.2 DESAROLLO DE OBJETIVO 2

6.2.1 Metodologías e indicadores. Los ataques de tipo *Hill-climbing* consisten en generar una modificación de forma sucesiva a un patrón específico de características, patrón estructurado por un material sintético, lo anterior, con el objetivo de que el sistema acepte dicha solicitud de identificación como válida.
Los ataques *Hill-climbing* pueden presentarse en dos escenarios: 1. Como objetivo puede tenerse el canal de comunicación entre el sensor y el módulo de extracción de características. 2. Se puede presentar entre el extractor de características y el comparador. En la figura número 10 se ven representados los escenarios de acuerdo a las fases del sistema.

[61] TECHNAVIO. Global Biometric PoS Terminals Market 2017-2021. En: Technavio [sitio web]. Reino Unido. [Consulta 18 de mayo 2020]. Disponible en: https://www.technavio.com/report/global-computing-devices-global-biometric-pos-market?tnplus
[62] WADHWANI, Preeti y GANKAR, Saloni. Biometrics Market Size By Application. En: Global Market Insights [sitio web]. USA. [Consulta 18 de mayo 2020]. Disponible en: https://www.gminsights.com/industry-analysis/biometrics-market

Figura 10. Escenarios ataque tipo Hill-climbing.



Fuente: OCAÑA DIEZ DE LA TORRE, Manuel. Escenarios ataque Hill-climbing [En línea]. Algoritmos de Matching entre huellas dactilares. Universidad Politécnica de Madrid . 2017. p. 16. [Recuperado en 17 de mayo 2020]. Disponible en: http://oa.upm.es/47958/1/TFG_MANUEL_OCANA_DIEZ_DE_LA_TORRE.pdf

Carballo[96], propone un escenario de ataque entre el extractor de características y el comparador, en el cual se puede aprovechar el análisis del tiempo que tarda un proceso de comparación en procesar la información recibida, de esta manera, generar patrones conforme las minucias obtenidas.

Previo a la generación del ataque, se debe tener un conocimiento específico y claro de la estructura o indexación de la data obtenida por los usuarios, por ejemplo, reconocer que cada minucia conforme la plantilla de un individuo es almacenada en la base de datos como un vector que posee tres características: dos características propias a una posición en un plano de dos dimensiones, la restante, que corresponde al ángulo de la minucia conforme una línea horizontal.

[96] CARBALLO. Op. cit., p. 32.

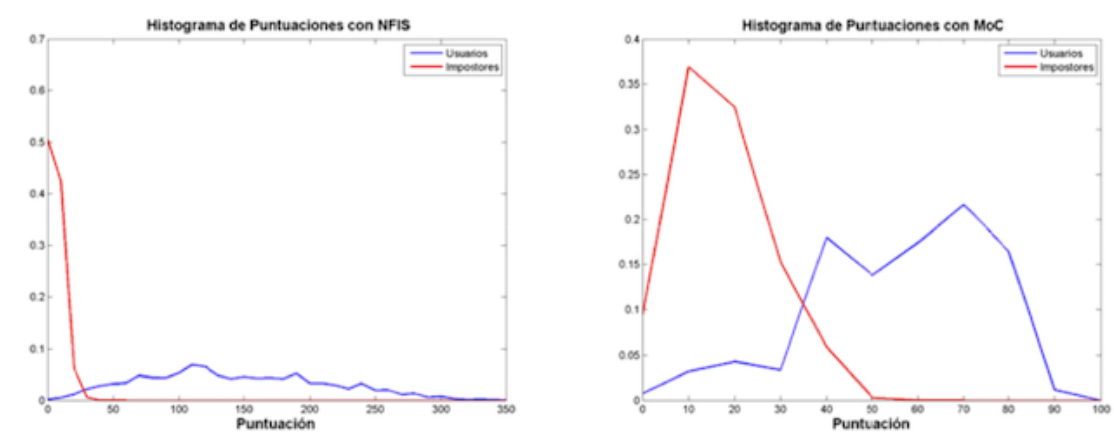
Para con cada tipo de huella se procede a la creación de 100 patrones de minucias de forma aleatoria (puede variar entre un valor superior o inferior), comenzando el ataque con el patrón que mayor puntuación de comparación que se generó. A partir de este, se realizará modificaciones sucesivas hasta el momento que el umbral de aceptación sea superado.

Ya considerado un punto de partida, en referencia a un patrón con cualidades particulares de similitud, se puntualizan cuatro modificaciones que son permitidas en el escenario de ataque principalmente: 1. Perturbación de una minucia existente y que no arroja una buena puntuación. 2. Se permite añadir una minucia para complementar un puntaje. 3. Se realiza sustitución de una minucia que es elegida al azar, considerando su puntaje. 4. Se realiza la eliminación de una minucia de manera aleatoria, igualmente considerando su puntuación. Es válido aclarar que este tipo de ataque enfoca un gran porcentaje de su esfuerzo en los bordes de la huella, lo anterior no para lograr éxito, pero si para mejorar la concentración alta de minucias, que si bien son huellas artificiales, el post-procesamiento se hace necesario, pues permite considerar un análisis en la región de interés (*Region of interest*).

Por medio de procesos de experimentación, se corroborará lo anteriormente descrito, acercando los temas conceptuales y teóricos propuestos en un entorno real, verificando en el análisis de tiempos la relación existente entre el comparador y su tiempo de respuesta, conforme la puntuación obtenida.

Un análisis por medio del sistema NFIS de la NIST y Match-on-card, como se logra ver en la figura 11, da a conocer cuando el usuario es un impostor, su puntuación es menor a 50, por el contrario, cuando el usuario es legítimo su puntuación se encuentra en promedio entre 50 y 250, esto en NIST. Por el contrario, para *Match-on-card (MoC)*, se logra observar un comportamiento intrusivo característico para puntuaciones entre 10 y 20, y para usuarios legítimos una puntuación promedio entre 60 y 80.

Figura 11. Validación de puntajes para Usuarios e intrusos.



Fuente: CARBALLO DOMÍNGUEZ, Sara. Validación de puntajes para Usuarios e intrusos [imagen]. Ataques indirectos a sistemas de reconocimiento de huella dactilar basados en los tiempos de comparación algorítmica. Escuela Politécnica Superior de Madrid. 2009. p. 45. [Recuperado en 28 de marzo 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/9991/51301_20090522SaraCarballo.pdf?sequence=1&isAllowed=y¡

Conforme el falso rechazo (FR) y la falsa aceptación (FA), observamos en la figura número 12, que para el sistema NIST a menor puntuación con referente de 40 (comportamiento intrusivo) crece el porcentaje de error, es decir, con un puntaje en este rango crece la posibilidad de aceptar un usuario intrusivo, mientras que para un falso rechazo, crece el margen de error para puntuaciones mayores a 40, reflejando que la probabilidad de rechazar un usuario legítimo crece. Para con el sistema MoC, igualmente se tiene un umbral de decisión menor a 40 que refleja el comportamiento de un impostor, mayor a este de un usuario legítimo, resultados similares al sistema NIST.[97]

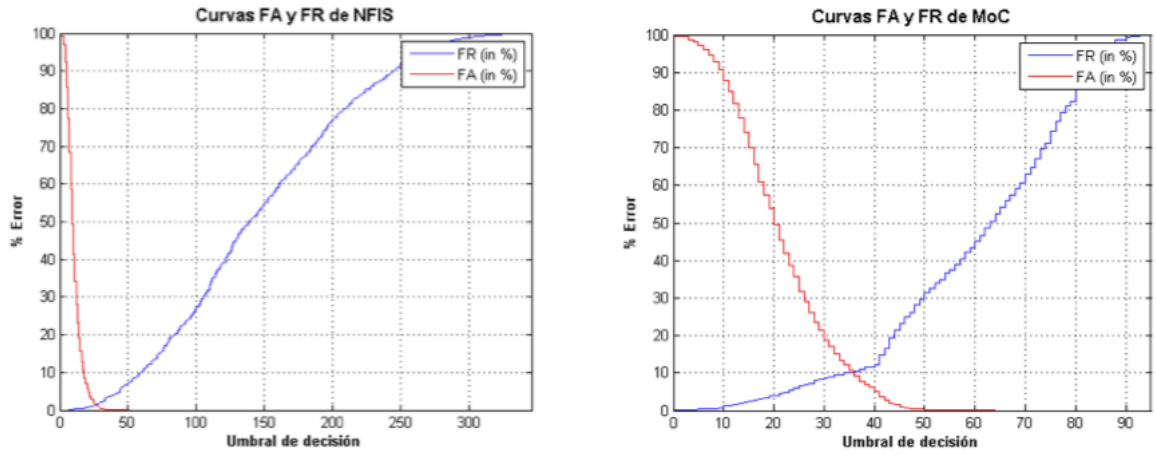
De acuerdo a los valores analizados con anterioridad, se realiza una evaluación de los sistemas de acuerdo al parámetro DET (*Detection Error Tradeoff*),

[97] CARBALLO. Op. cit., p. 45.

obteniendo que la tasa de rechazo es mayor para el sistema MoC y menor a para el sistema NFIS.

Para el sistema de NIST una puntuación de 26.5, con un valor de 1.47% como porcentaje de error, se obtiene en el proceso experimental un valor de 0.1% para FA y 3.33% para FR. Para el sistema MoC, para una puntuación de 36.5, se tiene un porcentaje de error de 9.78%; a partir de esto, experimentalmente se considera puntuación de 55 con un FA de 0.16% y una FR de 37.33%. Lo anterior se puede observar en la gráfica número 12.

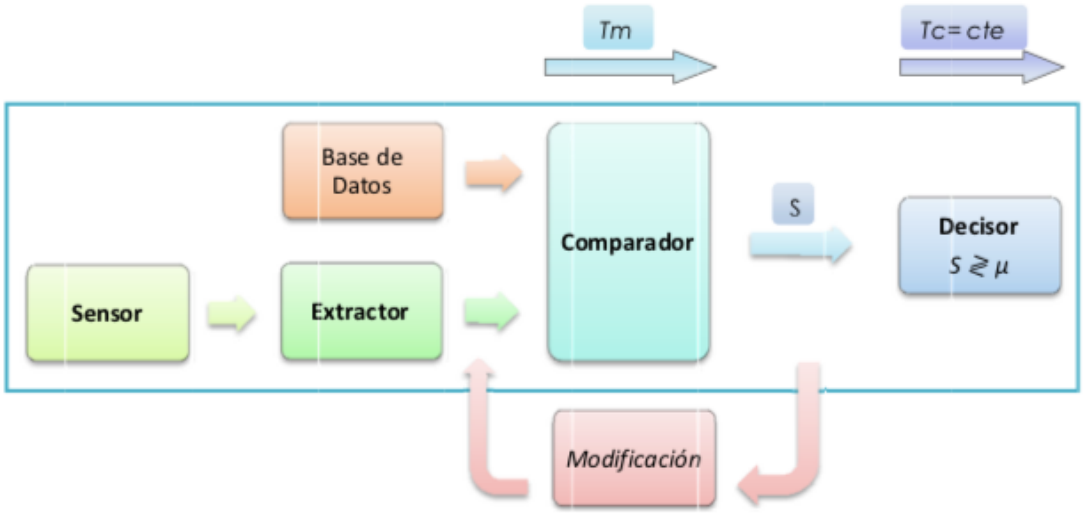
Figura 12. DET (Detection Error Tradeoff)



Fuente: CARBALLO DOMÍNGUEZ, Sara. DET [imagen]. Ataques indirectos a sistemas de reconocimiento de huella dactilar basados en los tiempos de comparación algorítmica. Escuela Politécnica Superior de Madrid. 2009. p. 46. [Recuperado en 28 de marzo 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/9991/51301_20090522SaraCarballo.pdf?sequence=1&isAllowed=y

Para generar el ataque, se debe considerar como objetivo de la investigación el identificar el tiempo de comparación que tarda el sistema en procesar la información recibida.

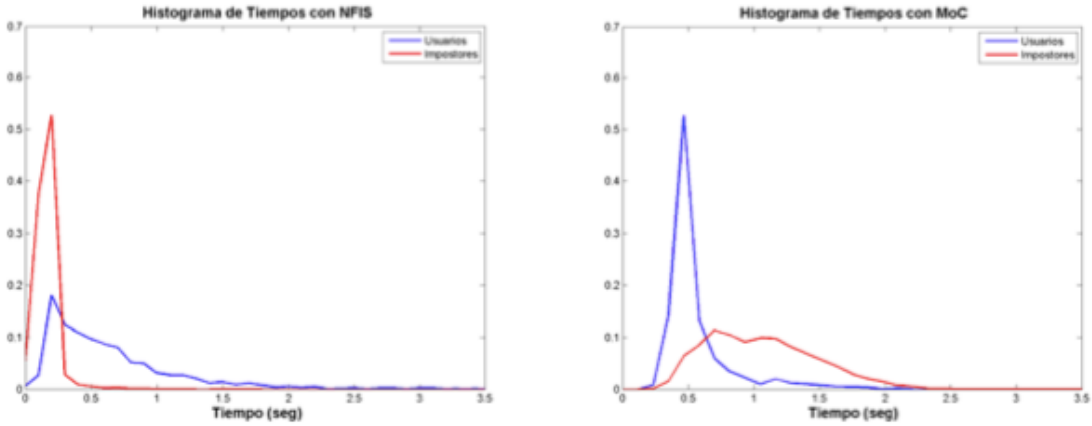
Figura 13. Escenario ataque a realizar por medio de la experimentación.



Fuente: CARBALLO DOMÍNGUEZ, Sara. Escenario ataque [imagen]. Ataques indirectos a sistemas de reconocimiento de huella dactilar basados en los tiempos de comparación algorítmica. Escuela Politécnica Superior de Madrid. 2009. p. 36. [Recuperado en 28 de marzo 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/9991/51301_20090522SaraCarballo.pdf?sequence=1&isAllowed=y

Con base en lo anterior, se considera una base de datos que corresponde a 1.350 valores de puntuaciones para autenticaciones legítimas y 22.350 puntuaciones para autenticaciones falsas. Para con cada una de estas puntuaciones se asocia un valor de tiempo, correspondiente al proceso de comparación por parte del sistema biométrico dactilar; teniendo estos valores, se procede a generar la gráfica correspondiente a la figura número 14.

Figura 14. Tiempos para Usuarios legítimos e impostores. NFIS y MoC.

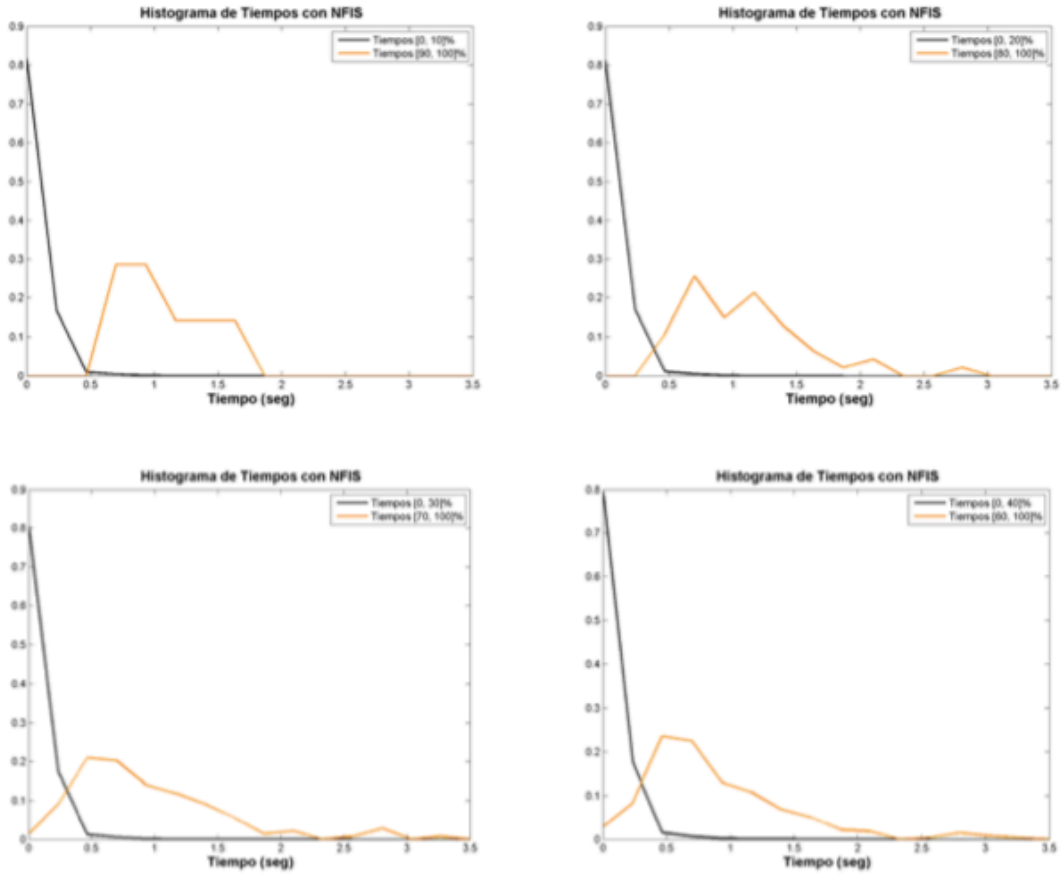


Fuente: CARBALLO DOMÍNGUEZ, Sara. Tiempos Usuarios legítimos [imagen]. Ataques indirectos a sistemas de reconocimiento de huella dactilar basados en los tiempos de comparación algorítmica. Escuela Politécnica Superior de Madrid. 2009. p. 51. [Recuperado en 28 de abril 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/9991/51301_20090522SaraCarballo.pdf?sequence=1&isAllowed=y

Con el fin de realizar una validación más precisa entre tiempo y puntuación, se procede a definir diez regiones iguales, en las cuales se representarán las puntuaciones y la densidad de tiempos, lo anterior, pretende identificar si a rangos de puntuación alejadas corresponden tiempos con mayor o menor solapamiento.[98]

Figura 15. Relaciones puntajes y tiempos para puntuaciones bajas (negro) y altas (naranja) sistema NFIS.

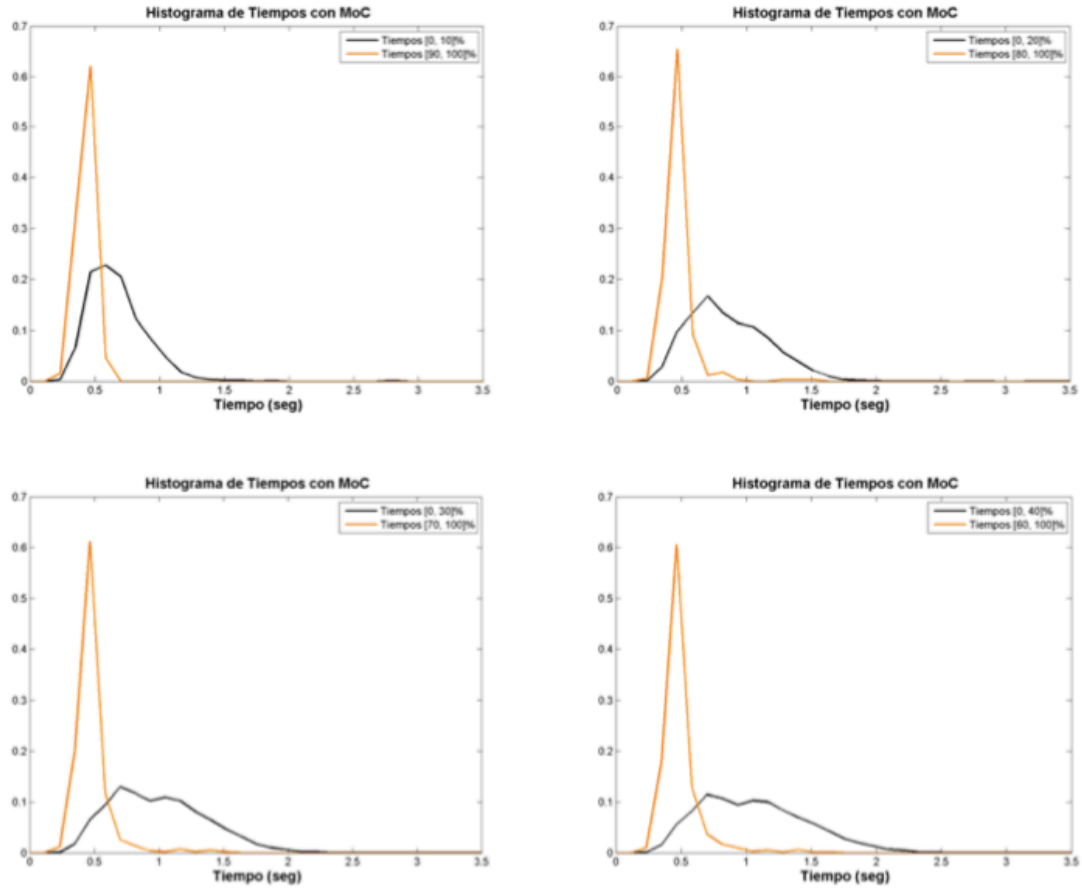
[98] CARBALLO. Op. cit., p. 52.



Fuente: CARBALLO DOMÍNGUEZ, Sara. Relación puntajes y tiempos [imagen]. Ataques indirectos a sistemas de reconocimiento de huella dactilar basados en los tiempos de comparación algorítmica. Escuela Politécnica Superior de Madrid. 2009. p. 36. [Recuperado en 28 de marzo 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/9991/51301_20090522SaraCarballo.pdf?sequence=1&isAllowed=y

De las gráficas obtenidas, se puede deducir que las puntuaciones pequeñas (representadas en color negro) presentan una forma similar, no obstante, los valores de puntuaciones altas (representados en color naranja) su forma cambia y no es predecible, por tanto, considerando que los tiempos inferiores corresponden a puntuaciones bajas, el tiempo de comparación cuando es mayor la puntuación es alta. Estas conclusiones son muy importantes al momento de desarrollar un ataque de Tipo *Hill-climbing* con la obtención de parámetros de tiempos: *Timing*. La experimentación expuesta se evalúa con el sistema MoC.

Figura 16. Relaciones puntajes y tiempos sistema MoC.



Fuente: Fuente: CARBALLO DOMÍNGUEZ, Sara. Puntajes y tiempos [imagen]. Ataques indirectos a sistemas de reconocimiento de huella dactilar basados en los tiempos de comparación algorítmica. Escuela Politécnica Superior de Madrid. 2009. p. 55. [Recuperado en 28 de abril 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/9991/51301_20090522SaraCarballo.pdf?sequence=1&isAllowed=y

Del experimento con el sistema MoC, se puede deducir que a mayor puntaje (línea naranja) menor tiempo de comparación por parte del sistema, a su vez, se observa que el tiempo que tarda el sistema en evaluar esa puntuación alta, siempre es el mismo, esto a diferencia del sistema NFIS, en el cual la puntuación baja tomaba menos tiempo y era siempre igual.

Como resultado de los dos experimentos, se deduce que existe una relación directa entre tiempo y puntuación, siendo altamente viable un ataque *Hill-climbing* por medio del análisis del tiempo materializando el riesgo existente en los sistemas afectando la confidencialidad e integridad de la información.

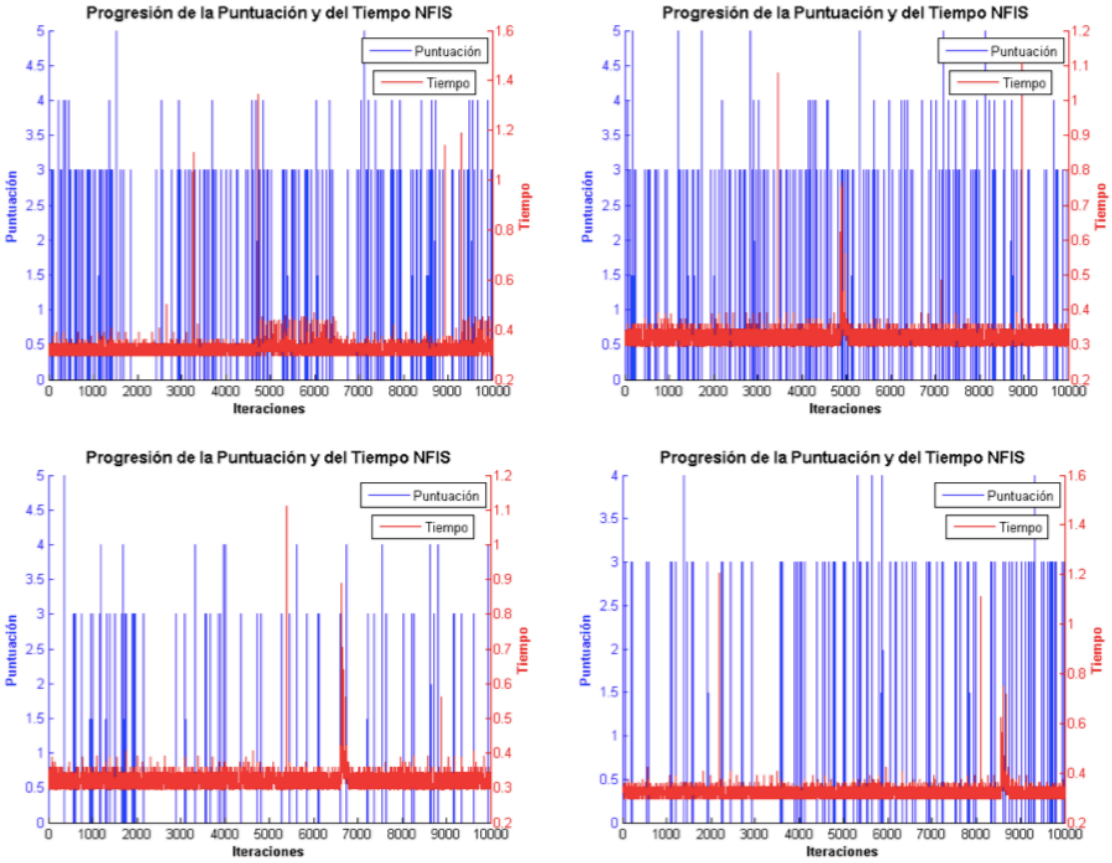
6.2.2 Validación ataques Timing y Hill- Climbing por medio de sistemas NFIS y MoC (Variación de parámetros y tipos de sensores). Se desarrollarán tres tipos de ataques: inicialmente se realizará un ataque básico, en el cual se considerarán 50 plantillas de huella dactilar, 10.000 iteraciones y un cambio, junto a un umbral de 35 con un FA de 0.1% y un FR de 3.33%. Se toma un valor de 10.000 en iteraciones, esto debido a que el sistema es vulnerable a partir de las 1.000 iteraciones conforme la siguiente fórmula.[99]

$$\boldsymbol{Nfuerza_{brutaNFIS}} = \frac{\mathbf{100}}{\boldsymbol{FAR}\ (\%)}$$

Generando el ataque, se identifica que el algoritmo no ha logrado generar un ataque exitoso con ninguna huella, pues los valores de la puntuación oscilan entre 3 y 5, adicionalmente el tiempo se mantiene constante, impidiendo obtener algún tipo de relación entre tiempo y puntuación. Lo anterior se logra observar en la figura 17.

Figura 17. Ataque puntuaciones bajas.

[99] CARBALLO. Op. cit., p. 67.

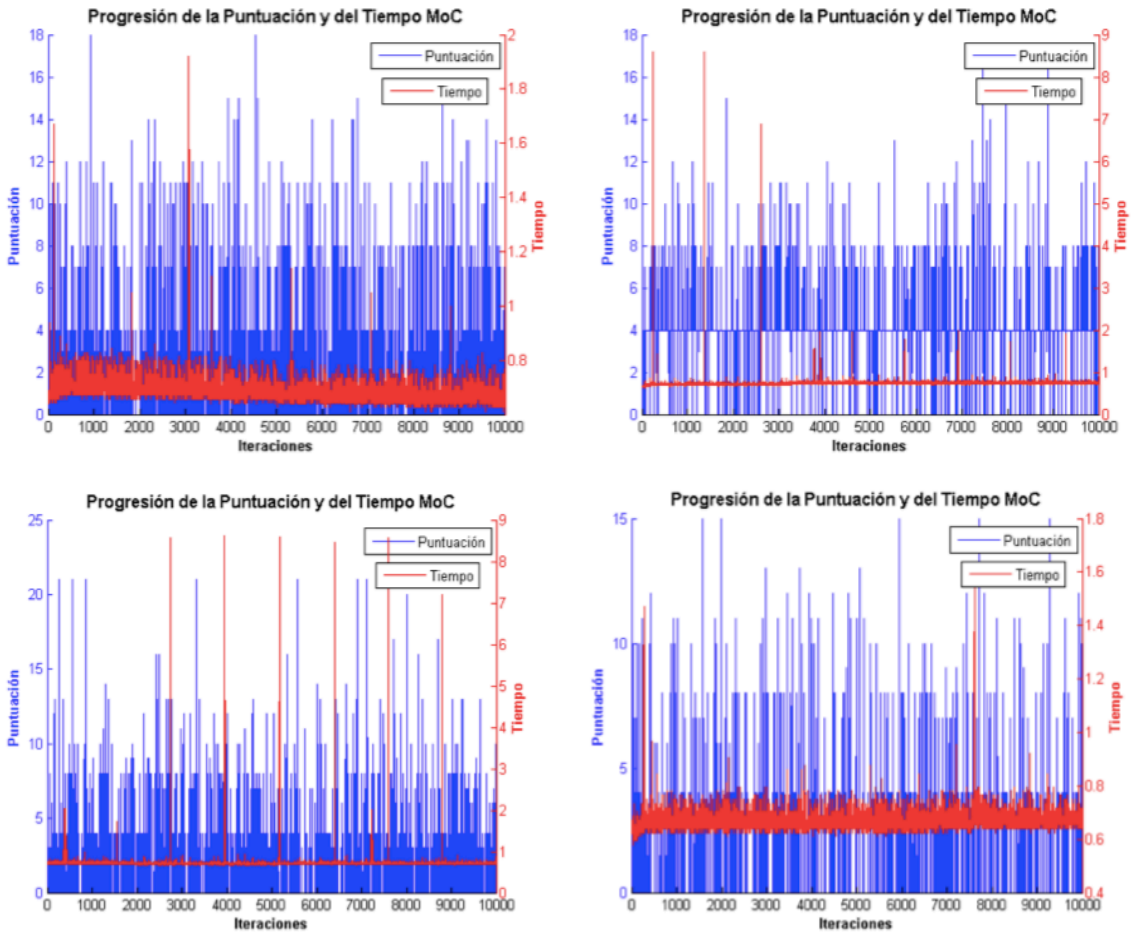


Fuente: CARBALLO DOMÍNGUEZ, Sara. Ataques puntuaciones bajas [imagen]. Ataques indirectos a sistemas de reconocimiento de huella dactilar basados en los tiempos de comparación algorítmica. Escuela Politécnica Superior de Madrid. 2009. p. 69. [Recuperado en 28 de marzo 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/9991/51301_20090522SaraCarballo.pdf?sequence=1&isAllowed=y

El tipo de ataque generado comienza con un valor de puntuación bajo impidiendo vulnerar el sistema.

Generando un ataque adicional, igualmente se identifica que el algoritmo no ha logrado generar un ataque exitoso con ninguna huella, no obstante, los valores de la puntuación oscilan con valores más altos que varían entre 15 y 25, esto como resultado de que el umbral incrementó a un valor de 300. Se observa que el tiempo se correlaciona directamente con la puntuación. Lo anterior se logra observar en la figura 18.

Figura 18. Ataque puntuaciones altas.



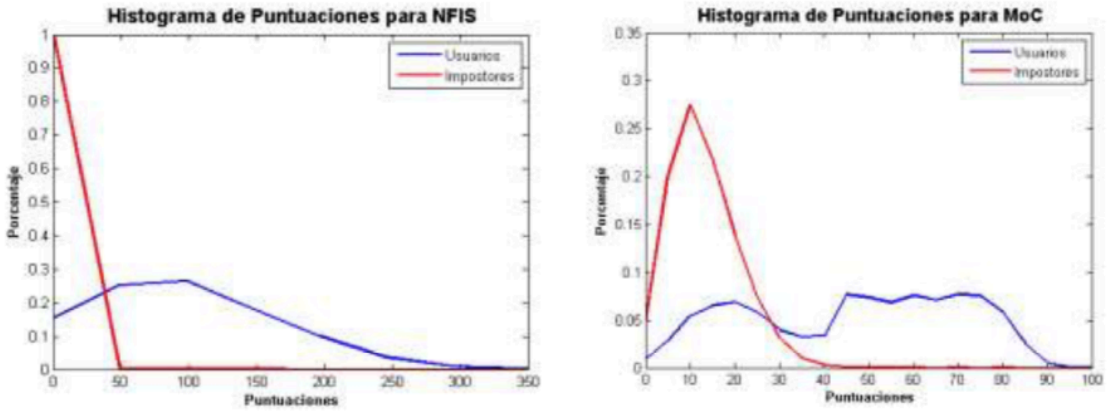
Fuente: CARBALLO DOMÍNGUEZ, Sara. Ataques puntuaciones altas [imagen]. Ataques indirectos a sistemas de reconocimiento de huella dactilar basados en los tiempos de comparación algorítmica. Escuela Politécnica Superior de Madrid. 2009. p. 72. [Recuperado en 28 de marzo 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/9991/51301_20090522SaraCarballo.pdf?sequence=1&isAllowed=y

Para un estudio adicional, el cual se involucran igualmente los sistemas NFIS y MoC como fundamento de la investigación, Beisner[100] toma 160.000 puntuaciones de usuarios impostores y 24.000 para usuarios legítimos. Para esta investigación, se consideran dos tipos de sensores: óptico y térmico. Para

[100] BEISNER. Op. cit., p. 51.

el sensor óptico, en la figura número 19 se da a conocer gráficamente las puntuaciones tanto de usuario como de impostor.

Figura 19. Puntuaciones sistema NFIS y MoC para sensor óptico.

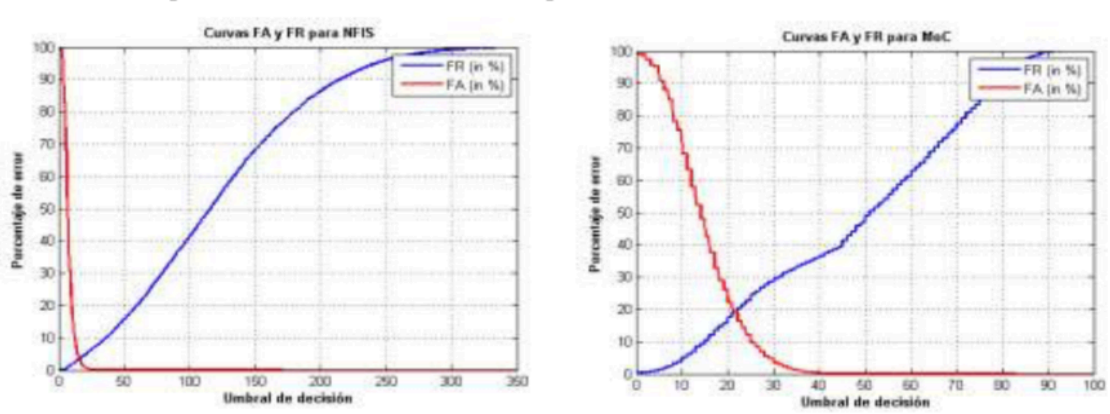


Fuente: BEISNER MUÑOZ, Alicia. Puntuaciones NFIS y MoC. [En línea]. Ataques tipo "Side-Channel" a sistemas biométricos de reconocimiento de huella dactilar. Universidad Autónoma de Madrid, 2010. p. 50. [Recuperado en 23 de Abril 2020]. Disponible en: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20100426AliciaBeisnerMunoz.pdf

Por medio de la anterior gráfica, se puede deducir que los usuarios impostores en el sistema NFIS obtienen puntuaciones pequeñas que se concentran en 0 y 50; por su parte, los usuarios legítimos están a lo largo de las puntuaciones entre 0 y 350, generando un puntaje entre 50 y 100.

Como componente sensor térmico, se realiza los mismos análisis que para el sensor óptico anteriormente expuesto se realizaron, obteniendo los siguientes resultados:

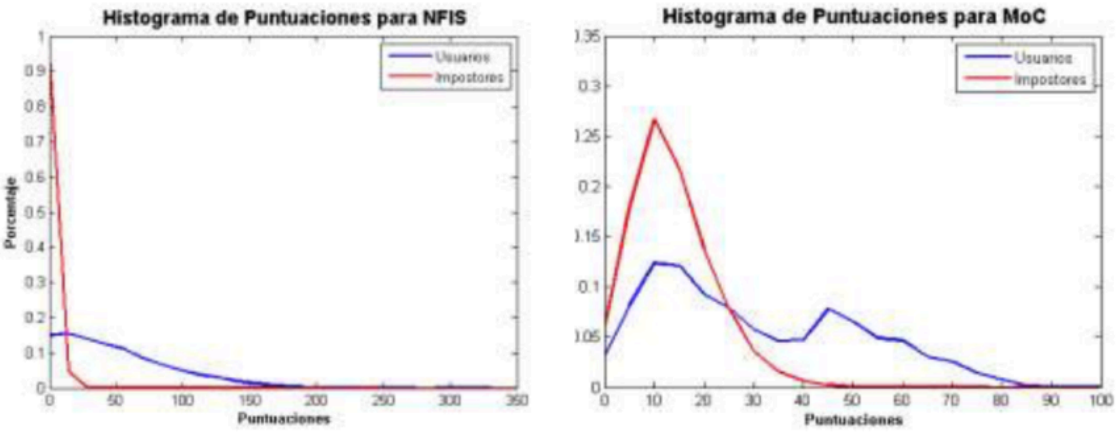
Figura 20. Parámetros FR (Falso rechazo), FA (Falsa aceptación) y ERR (equal error Rate).



Fuente: BEISNER MUÑOZ, Alicia. Puntuaciones FR y FA [En línea]. Ataques tipo “Side-Channel” a sistemas biométricos de reconocimiento de huella dactilar. Universidad Autónoma de Madrid, 2010. p. 51. [Recuperado en 16 de Abril 2020]. Disponible en: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20100426AliciaBeisnerMunoz.pdf

En la figura número 21 se observa que se tiene una acumulación de puntaje por debajo de 30 para los usuarios impostores, por su parte, para el sistema MoC el comportamiento tanto para impostores y legítimos es similar con respecto al sensor óptico, con la diferencia de que se tiene un menor puntaje de las muestras.

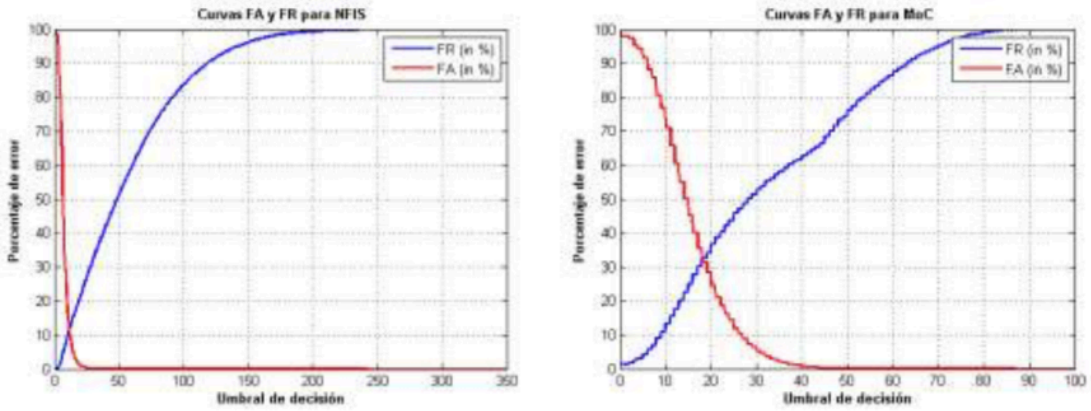
Figura 21. Puntuaciones sistema NFIS y MoC para sensor térmico.



Fuente: BEISNER MUÑOZ, Alicia. Puntuaciones NFIS y MoC. [En línea]. Ataques tipo “Side-Channel” a sistemas biométricos de reconocimiento de huella dactilar. Universidad Autónoma de Madrid, 2010. p. 51. [Recuperado en 23 de Abril 2020]. Disponible en: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20100426AliciaBeisnerMunoz.pdf.

En la figura número 22, se observa a diferencia del sensor óptico, el sensor térmico presenta una mayor tasa de error EER respecto al sensor óptico.

Figura 22. Puntuaciones sistema NFIS y MoC para sensor térmico.



Fuente: BEISNER MUÑOZ, Alicia. Puntuaciones NFIS y MoC. [En línea]. Ataques tipo “Side-Channel” a sistemas biométricos de reconocimiento de huella dactilar. Universidad Autónoma de Madrid, 2010. p. 52. [Recuperado en 16 de Abril 2020]. Disponible en: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20100426AliciaBeisnerMunoz.pdf

La comparación entre el sensor óptico y el sensor térmico, llevan a deducir que su rendimiento en el sistema MoC es menor, esto respecto a que una tarjeta biométrica presenta limitantes claras en comparación a un sistema biométrico dactilar. Igualmente, se logra deducir que el sensor óptico, presenta un mejor comportamiento respecto al comparado en cuanto a la tasa FR (Falso rechazo), dado que su porcentaje de error es menor y el umbral (puntaje) de comparación

es más sensible y mayor, por tanto, para este la puntuación para declarar un usuario legítimo es mayor (validando más detalles) viéndose esto representado en el menor porcentaje de error.

Los anteriores resultados preliminares, ayudarán a futuro respecto a ataques tipo número 4 entre el extractor de características y el módulo comparador a desarrollar.

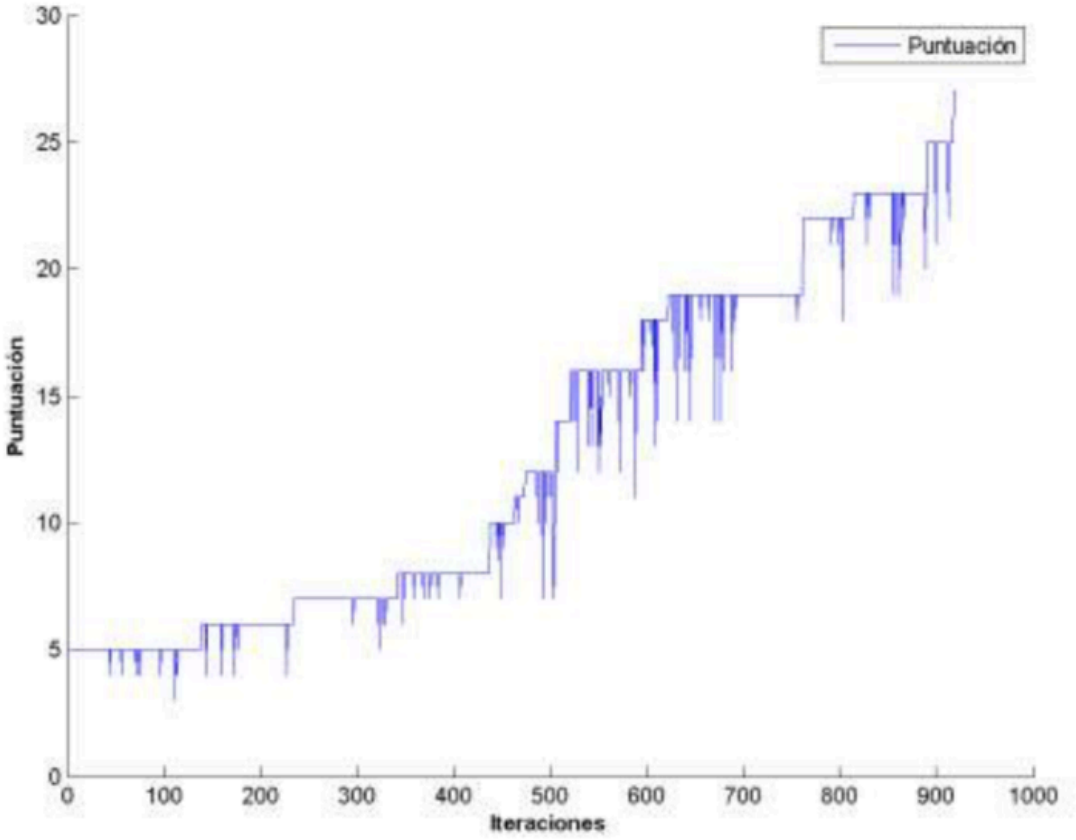
Para otros tipos de ataque desarrollados, inicialmente, es necesario conocer el tipo de sensor implementado en el sistema y con ello deducir la forma de indexación de la data. Se tiene conocimiento a partir de esto, que las minucias son almacenadas de una manera específica, con un vector de tres componentes (dos que pertenecen a la posición y la restante informa el ángulo con respecto a la horizontal).

El algoritmo utilizado lleva a cabo cuatro pasos para ejecutar el ataque: 1. La creación de 100 patrones sintéticos, basados en minucias. 2. Generar el ataque a la huella objetivo almacenando los valores en referencia a las puntuaciones obtenidas por el comparador. 3. Se realizarán modificaciones al patrón que obtenga mayor puntaje, con esto, se buscará perturbar una minucia de la huella existente, añadir una nueva minucia, sustituir una minucia existente y/o eliminarla. 4. Por último, al superarse el umbral el algoritmo se detiene.

En la figura número 23 se observa el éxito de un ataque *Hill-climbing* para un umbral de 26 con un total de 1.000 iteraciones.[101]

Figura 23. Iteraciones que logran un umbral específico.

[101] BEISNER. Op. cit., p. 57.

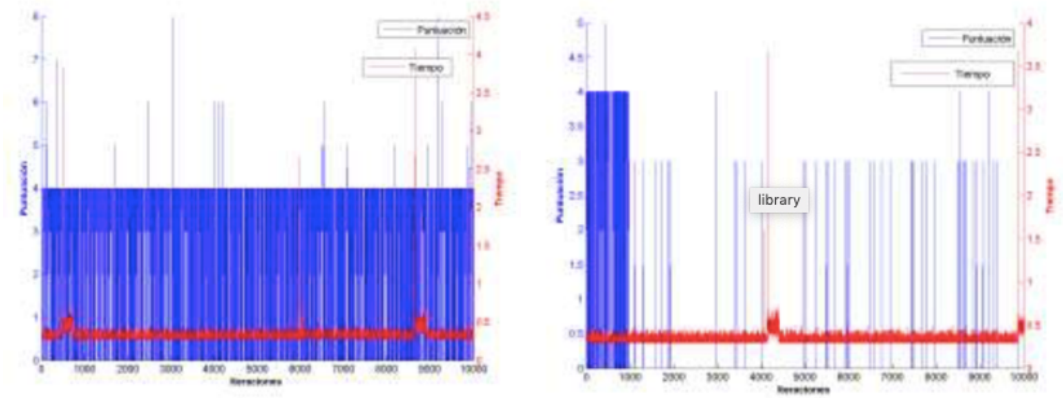


Fuente: BEISNER MUÑOZ, Alicia. Iteraciones. [En línea]. Ataques tipo "Side-Channel" a sistemas biométricos de reconocimiento de huella dactilar. Universidad Autónoma de Madrid, 2010. p. 58. [Recuperado en 23 de Abril 2020]. Disponible en: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20100426AliciaBeisnerMunoz.pdf

Para un primer tipo de ataque básico, se contemplará 10.000 iteraciones, estableciendo un umbral de 26 para el sensor óptico y 38 como umbral para el sensor térmico.

Para este primer escenario, se observa que el algoritmo no ha logrado vulnerar el sistema NFIS, como se logra observar en la figura número 24, el tiempo y la puntuación quedan oscilando en un valor específico, esto sin generar ningún tipo de correlación.

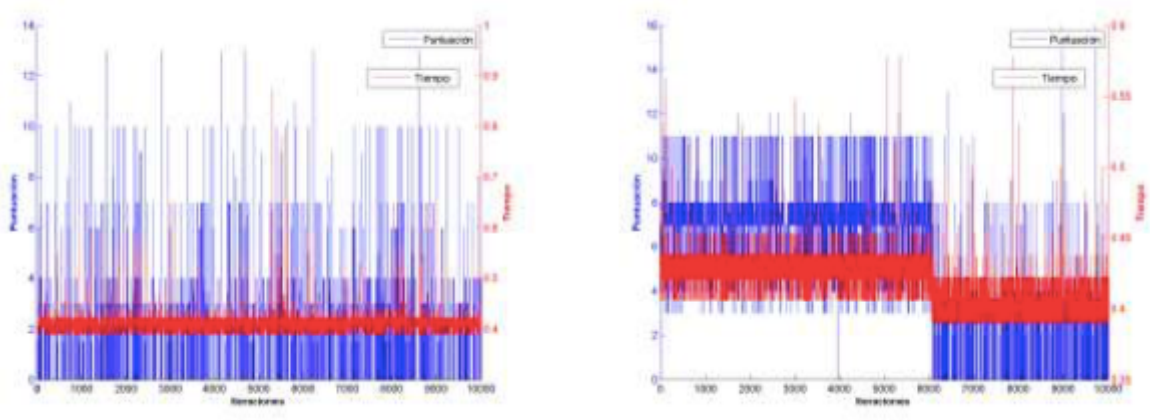
Figura 24. Relación tiempo y puntuaciones sensor térmico y óptico. Sistema NFIS.



Fuente: BEISNER MUÑOZ, Alicia. Relación tiempo y puntuaciones. [En línea]. Ataques tipo “Side-Channel” a sistemas biométricos de reconocimiento de huella dactilar. Universidad Autónoma de Madrid, 2010. p. 82. [Recuperado en 23 de Abril 2020]. Disponible en: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20100426AliciaBeisnerMunoz.pdf

El mismo experimento realizado para el sistema MoC, logra determinar que el sistema tampoco ha sido vulnerado, no obstante, se encuentra correlación entre tiempo y puntuaciones, dada una puntuación mayor. Se puede observar lo descrito en la figura número 25.

Figura 25. Relación tiempo y puntuaciones sensor térmico y óptico. Sistema MoC.



Fuente: BEISNER MUÑOZ, Alicia. Relación tiempo y puntuaciones sensores térmicos y óptico. [En línea]. Ataques tipo “Side-Channel” a sistemas biométricos de reconocimiento de huella dactilar. Universidad Autónoma de Madrid, 2010. p. 84. [Recuperado en 23 de Abril 2020]. Disponible en: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20100426AliciaBeisnerMunoz.pdf

El trabajo realizado, da a conocer que existe una estrecha relación entre tiempo y puntuación, lo anterior expone que los sistemas biométricos dactilares son altamente vulnerables y estás consideraciones deben ser tenidas en cuenta para futuras aplicaciones.

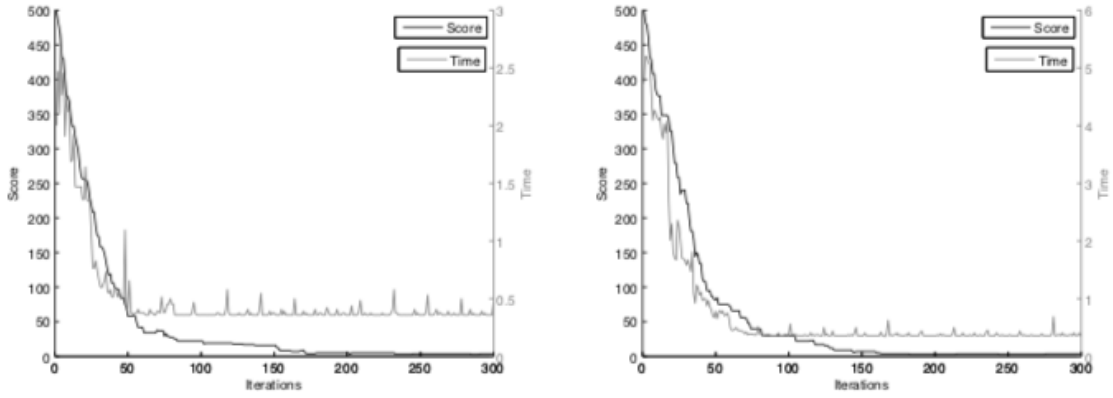
Con el fin de realizar comprobaciones conforme lo anteriormente descrito, en relación tiempo y puntuación para los sistemas de reconocimiento de huella dactilar, Galbally; Fierrez y Ortega[102] por su parte generan dos tipos de experimentos: el primero con el fin de verificar esta correlación (puntuación y tiempo), y el restante, con el fin de identificar el comportamiento del tiempo de acuerdo a la variación de la puntuación.

Analizando la segunda experimentación, se realiza un proceso iterativo conforme 50 plantillas pertenecientes a 50 usuarios diferentes conforme una base de datos preestablecida. Para con cada una de las iteraciones realizadas se genera las siguientes dos modificaciones: primero se perturba la minucia, y segundo, se genera una sustitución de la misma.

Con el uso del sistema NIST, se realiza la modificación de las minucias de las huellas dactilares evaluadas observando una relación directa entre puntuación (500) y el tiempo empleado para obtenerlas, como se logra observar en la figura 26.

[102] GALBALLY; FIERREZ y ORTEGA. Op. cit., p. 3.

Figura 26. Evaluación puntuación (línea continua) y tiempo (línea segmentada).



Fuente: GALBALLY, Javier, *et al.* Evaluación puntuación (línea continua) y tiempo (línea segmentada). [En línea]. On the Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks [en línea]. Universidad Autónoma de Madrid, 2009. [Recuperado en 22 de mayo 2020]. Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.206.1024&rep=rep1&type=pdf

Este tipo de resultados nuevamente presenta información de interés conforme los ataques en sistemas de huella dactilar, permitiendo reconocer la importancia de estándares internacionales que trabajan para la mitigación de estos riesgos.

6.3 DESAROLLO DE OBJETIVO 3

6.3.1 BEAT (*Biometrics Evaluation and Testing*). Se ha establecido un propósito para el desarrollo de métodos de evaluación de pruebas de sistemas biométricos, lo anterior, con el fin de establecer un esquema de evaluación y pruebas biométricas obteniendo un resultado en referencia al uso eficiente de datos y eficacia en resultados.

El establecer un método de evaluación es resultado, y como consecuencia, del costo que implica generar pruebas repetitivas y con ello, el obtener datos de huellas dactilares de diferentes tipos de personas involucradas en el proceso,

adicionalmente, es importante considerar que si bien muchos componentes de los sistemas tecnológicos han sido evaluados y con esto certificados, los sistemas biométricos no han sido un referente en este aspecto; es por esta razón, que se establece BEAT (Biometrics Evaluation and Testing) como una guía de evaluación de diferentes componentes y en general, de sistemas biométricos de acuerdo a criterios comunes establecidos.

BEAT proporciona 5 aspectos en los cuales se establece el proceso de evaluación para los sistemas biométricos, estos a continuación dados a conocer:

- Evaluación objetivo de seguridad y perfil de protección aplicado: para dar inicio a un proceso de evaluación se consideran aspectos en cuanto a delimitación del TOE (Target of evaluation), el entorno de trabajo del sistema y su contexto, como también el reconocimiento de los estándares relacionados a los sistemas biométricos.

El TOE (*Target of evaluation*), se considera un requisito previo para generar la evaluación de criterios comunes. Este tipo de evaluación está compuesta por un algoritmo que hace uso de bases de datos de pruebas con configuraciones técnicas; es posible delimitarla, bien sea al sistema completo o generando exclusiones, por ejemplo, al dispositivo de captura (sensor). No obstante, ante ataques de suplantación como los expuestos en el objetivo dos de este proyecto de grado, se logra identificar que el sensor hace parte de las vulnerabilidades de los sistemas ante ataques de suplantación de identidad. [103]

Los sistemas biométricos al ser evaluados, y posteriormente, certificados, deben alinearse a un perfil de protección que a continuación se reconoce:

[103] N. Tekampe (TUViT), A. Merle, (CEA), J. Bringer (Mor- pho), M. Gomez-Barrero (UAM), J. Fierrez (UAM), J. Galbally (UAM). Biometrics Evaluation and Testing. [En línea]. beat-eu.org/, 2011. [Recuperado en 17 de octubre 2020]. Disponible en: https://www.beat-eu.org/project/deliverables-public/d6-5-toward-common-criteria-evaluations-of-biometric-systems

Tabla 1. Perfiles de referencia evaluación de sistemas biométricos.

Protection Profile	Revision	Shortcut	Date	Certification ID
Common Criteria Protection Profile Biometric Verification Mechanism	1.04	n/a	08/17/05	BSI-PP-0016-2005
Biometric Verification Mechanisms Protection Profile	1.3	BVMPP	08/07/08	BSI-CC-PP-0043-2008
Fingerprint Spoof Detection Protection Profile	1.8	FSDPP	11/23/09	BSI-CC-PP-0063-2010
Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies	1.7	FSDPP-OSP	11/27/09	BSI-CC-PP-0062-2010

Fuente: N. Tekampe (TUViT), A. Merle, (CEA), J. Bringer (Mor- pho), M. Gomez-Barrero (UAM), J. Fierrez (UAM), J. Galbally (UAM). Biometrics Evaluation and Testing. [En línea]. beat-eu.org/, 2011. [Recuperado en 17 de octubre 2020]. Disponible en: https://www.beat-eu.org/project/deliverables-public/d6-5-toward-common-criteria-evaluations-of-biometric-systems

- Como segundo aspecto de evaluación, se presenta los requisitos de desarrollo, proporcionando como referencia el tomar funcionalidades de los sistemas biométricos por medio de la agrupación de subsistemas y módulos.
- Tercer aspecto de evaluación, los repositorios y documentación permiten establecer una preparación propia para la evaluación TOE, reconociendo las funcionalidades específicas del sistema biométricos a evaluar definiendo requisitos para su uso, conforme los roles establecidos y el entorno de aplicabilidad.
- Un aspecto adicional que comprende la evaluación sobre el sistema biométrico TOE, corresponde a la verificación del ciclo de vida, el cual involucra criterios de disciplina y control para con los diferentes procesos de afinamiento para con los criterios a evaluar, permitiendo reconocer, entre otros aspectos, aquellos propios de ciberataques y su detección por medio de mecanismos de relación por firmas.

- Como quinto aspecto a evaluar, se involucra todo lo referente a los test de verificación y pruebas de concepto POC, estableciendo criterios comunes que involucran características intrínsecas. Como aspecto particular de sus características, se hace referencia a que los sistemas biométricos son probabilísticos, relacionados con tasas de error asociadas a su funcionamiento. Estas tasas de error, se consideran un aspecto importante dado que garantizan un desarrollo de los sistemas con el objetivo de contar con un funcionamiento esperado.

Las pruebas tipo ATE (Equipo de prueba automatizado), se refieren a los *test* de funcionamiento de los sistemas en un escenario común, por ejemplo, un usuario cualquiera solicita el acceso al sistema; para este escenario, se presenta dos tipos de accesos: el primero, en el cual el individuo presenta para el proceso de *Login* sus propias y legítimas características biométricas, el restante, se presenta un impostor para el acceso, contexto en el cual el impostor presenta sus propias características biométricas de acceso, intentando una verificación exitosa frente a una plantilla de un usuario diferente, tal como se observó para los sistemas NFIS y *Match On Card* en las pruebas de experimentación expuestas con anterioridad, y que reflejan el acercamiento del proceso establecido por los investigadores al parámetro BEAT (Biometrics Evaluation and Testing).

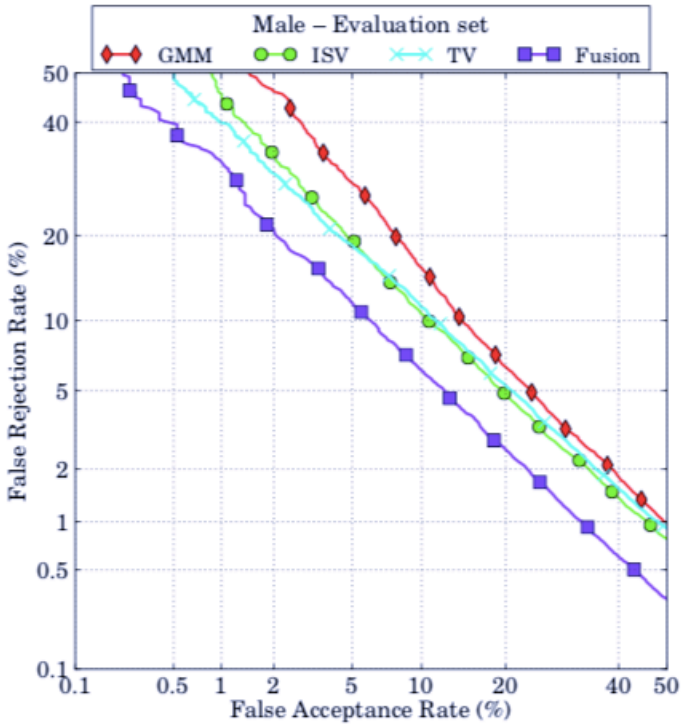
Se presenta desafíos para con un segundo escenario, que permite considerar la evaluación de dos tipos de tasas de error, en las cuales, ya nos encontramos relacionados: FAR (Tasa falsa de aceptación) y FRR (Tasa falsa de rechazo). Adicionalmente, BEAT considera tasas que se encuentran directamente relacionadas con FAR y FRR, estas son FNMR (Tasa falsa de coincidencias) y FMR (Tasa de coincidencia falsa). FNMR y FMR concentran esfuerzos al proceso de comparación, por otra parte, FAR y FRR principalmente se dan por errores en el sistema y su resultado. BEAT en la práctica, indica que la evaluación se debe dar por las tasas FAR y FRR, establecidas y determinantes para los procesos de experimentación expuestos.

Dentro del proceso de evaluación del sistema biométrico, la guía de evaluación proporcionada por BEAT involucra la detección de ataques, considerando que

estos eventos deben visualizarse en cada proceso y parte del sistema biométrico, adicionalmente, establece que todos los sistemas deben contar con la capacidad de detección de ataques PAD (Presentation Attack Detection). Dentro de esta etapa de evaluación, se aclara dos aspectos conforme ATE (Equipo de prueba automatizado): primero, los mecanismos de defensa ante ataques deben ser aprobados y segundo, los ataques a nivel sensorial deben ser considerados dentro de un análisis de vulnerabilidades.

Las pruebas de desempeño definidas por BEAT, reflejan la correlación de las tasas de error FAR y FRR, ilustradas por medio de curvas ROC (Receiver operating characteristic) o DET (Detection Error Tradeoff). Por medio de ROC, se define las características propias del funcionamiento del receptor, permitiendo identificar tasas de falsos positivos (intentos de impostores aceptados) y tasa de verdaderos positivos (intentos genuinos aceptados) logrando reconocer el umbral de decisión. [104]

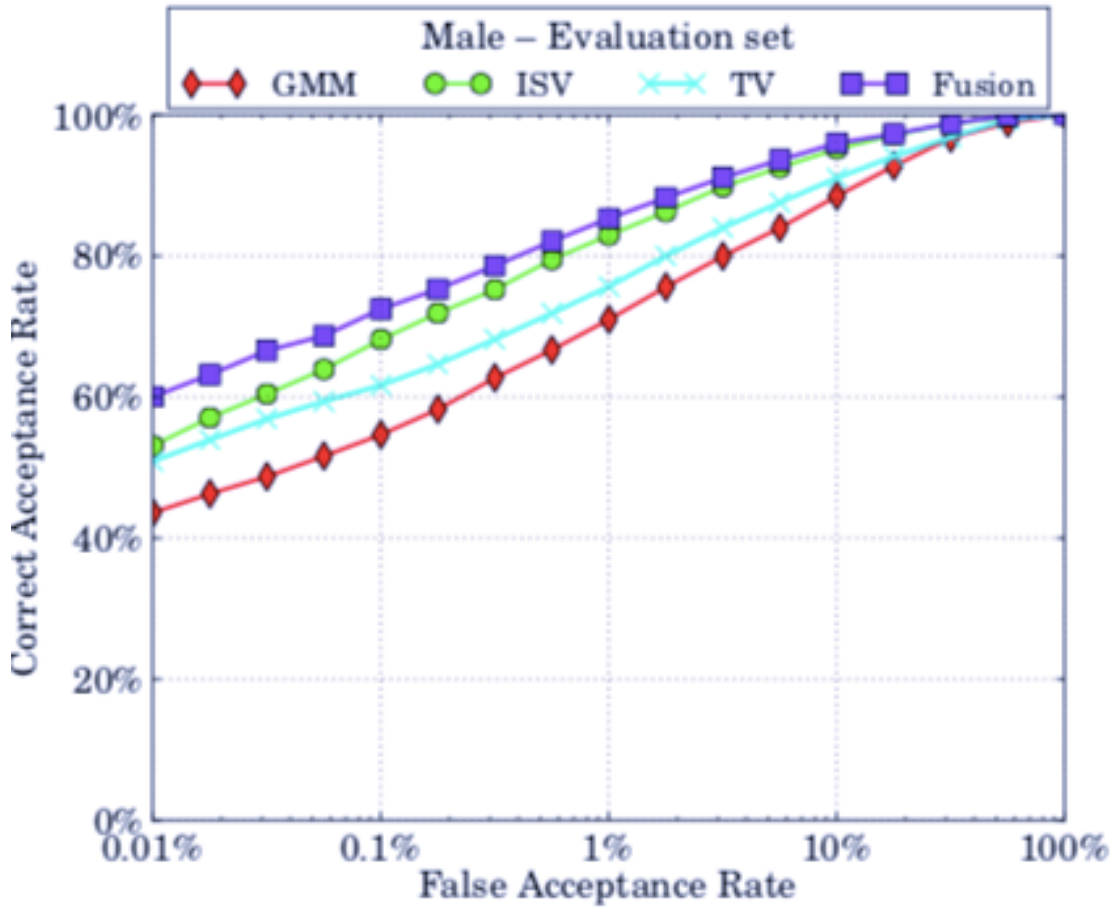
Figura 27. Ejemplo gráfica DET - FRR (Detection Error Tradeoff).



[104] Ibíd., p. 42.

Fuente: N. Tekampe (TUViT), A. Merle, (CEA), J. Bringer (Mor- pho), M. Gomez-Barrero (UAM), J. Fierrez (UAM), J. Galbally (UAM). Biometrics Evaluation and Testing. [En línea]. ḃeat-eu.org/, 2011. [Recuperado en 17 de octubre 2020]. Disponible en: https://www.beat-eu.org/project/deliverables-public/d6-5-toward-common-criteria-evaluations-of-biometric-systems

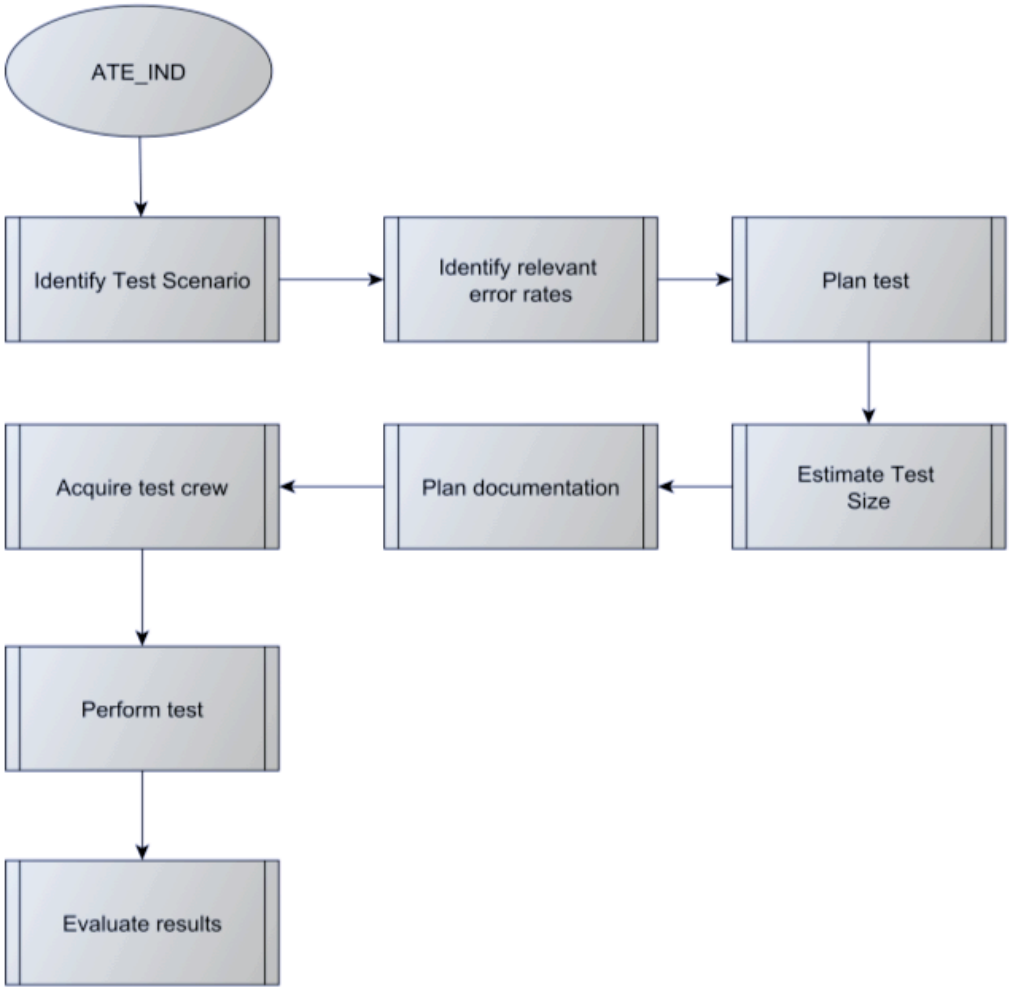
Figura 28. Ejemplo gráfica DET (Detection Error Tradeoff).



Fuente: N. Tekampe (TUViT), A. Merle, (CEA), J. Bringer (Mor- pho), M. Gomez-Barrero (UAM), J. Fierrez (UAM), J. Galbally (UAM). Biometrics Evaluation and Testing. [En línea]. ḃeat-eu.org/, 2011. [Recuperado en 17 de octubre 2020]. Disponible en: https://www.beat-eu.org/project/deliverables-public/d6-5-toward-common-criteria-evaluations-of-biometric-systems

Las curvas representativas ROC y DET son imprescindibles para obtener de una manera clara y visual el rendimiento de los sistemas biométricos, con esto, establecer responsabilidades ante mejoras del sistema según lo establecido en el TOE.

Figura 29. Proceso de evaluación.



Fuente: N. Tekampe (TUViT), A. Merle, (CEA), J. Bringer (Mor- pho), M. Gomez-Barrero (UAM), J. Fierrez (UAM), J. Galbally (UAM). Biometrics Evaluation and Testing. [En línea]. ḃeat-eu.org/, 2011. [Recuperado en 17 de octubre 2020]. Disponible en: https://www.beat-eu.org/project/deliverables-public/d6-5-toward-common-criteria-evaluations-of-biometric-systems

En la gráfica número 30 se logra identificar los pasos que hacen parte del proceso de evaluación, en el cual se establecen enfoques tecnológicos por medio de pruebas basadas en bases de datos hasta una evaluación del rendimiento del sistema.

Inicialmente, se realiza actividades conforme la identificación del escenario de prueba logrando distinguir el tipo de evaluación del sistema biométrico: evaluación tecnológica, permitiendo identificar algorítmos y con ello, su comparación en referencia con muestras preexistentes y evaluación de escenarios, determinando el rendimiento.

Posterior a actividades de identificación de escenario, se realiza identificación de tasas de error relevantes. Es necesario tener el prescedente en relación a que no existe una repuesta completa en cuanto a que tasas de error se consideran relevantes para un tipo de sistema biométrico, respecto a lo anterior, el profesional que realicé la evaluación tendrá a su consideración una serie de factores con el fin de determinar un concepto en referencia a las probabilidades de que el sistema genere un reconocimiento a un usuario incorrecto como legítimo. El índice de tasa de error, sin duda, está directamente relacionado con el modo de operación del sistema biométrico, delimitando su evaluación a valores y conceptos relevantes según la unidad de negocio.

Otro aspecto definido por la guía de evaluación, hace referencia a la planificación de pruebas a realizar sobre el sistema biométrico: inicialmente, es relevante que la prueba represente un escenario muy cercano al mundo real en el entorno de laboratorio; por otra parte, considerar de manera detallada y signifiticativa la relación estadística de las pruebas buscando obtener resultados significativos.

El plan de prueba se establece para lograr los siguientes objetivos: Lograr una configuración de la prueba lo más cercana posible al funcionamiento previsto por el sistema biométrico, identificando los pasos relevantes para tomar las pruebas correspondientes; lograr una descripción detallada de los datos de prueba con los que se realizará la evaluación; por último, definir un protocolo en el cual se

haga referencia al uso de los datos de prueba, reflejando su normalización, usabilidad y propósitos por conjunto de datos.

Los planes de prueba permiten realizar una verificación de las tasas FMR (FAR) y FNMR (FRR) logrando primero una inscripción de la muestra por usuario, luego, realizar una comparación de las puntuaciones bien sea de los usuarios legítimos o impostores. Un ejemplo típico de prueba, hace referencia a los intentos de acceso genuinos que son procesados por medio de una muestra inscrita y una muestra de prueba, por otra parte, los intentos de acceso impostores se procesan entre la muestra inscrita y muestra de prueba para con diferentes usuarios, escenarios descritos y analizados en las actividades de experimentación mencionadas.

La documentación del proceso de pruebas se considera un aspecto fundamental; es necesario planificar esta tarea antes de comenzarla, por tanto, es importante abordar aspectos como el escenario exacto, tasas de error relevantes y que son involucradas, características demográficas del equipo de prueba, tamaño y características de los datos y explicación del tratamiento a generar sobre los diferentes conjuntos de puntuaciones.

En referencia a la adquisición de bases de datos y conformación de equipos de pruebas, BEAT proporciona en su guía diferentes factores que se consideran imprescindibles, esto con el fin, de obtener resultados precisos:

- La adquisición y toma de datos estará bajo control y responsabilidad exclusiva de un evaluador, quien tendrá trazabilidad de todos los procedimientos.
- El proceso de adquisición de datos es costoso, por tanto, es necesario considerar si los datos de prueba obtenidos pueden reutilizarse en diferentes evaluaciones a ejecutar, de ser así, el proceso debe incluir acciones para que esto se cumpla sin inconvenientes.
- Los diferentes sistemas biométricos involucrados en las pruebas se encuentran diseñados para trabajar con un perfil de usuario específico,

por tanto, los datos deben estar lo más cercanos al perfil y su caracterización.

- Para el proceso de adquisición de datos, se debe establecer una nomenclatura coherente para los archivos a crear, de manera que cada fichero contenga un ID determinado y su normalización sea correcta.
- Los datos deben ser los suficientes con el fin de obtener resultados estadísticamente significativos.
- De considerarse relevante por el equipo de investigación, es posible incluir otros tipos de metadatos por parte de los usuarios, entre ellos, género, edad, uso de ayudas audiovisuales, entre otros.
- Las legislaciones locales deben ser consideradas, lo anterior dado que los datos biométricos hacen referencia a información de identificación personal (PII). La protección de datos personales debe ser considerada, por tanto, es necesario establecer documentos como consentimiento informado, entre otros pertinentes.

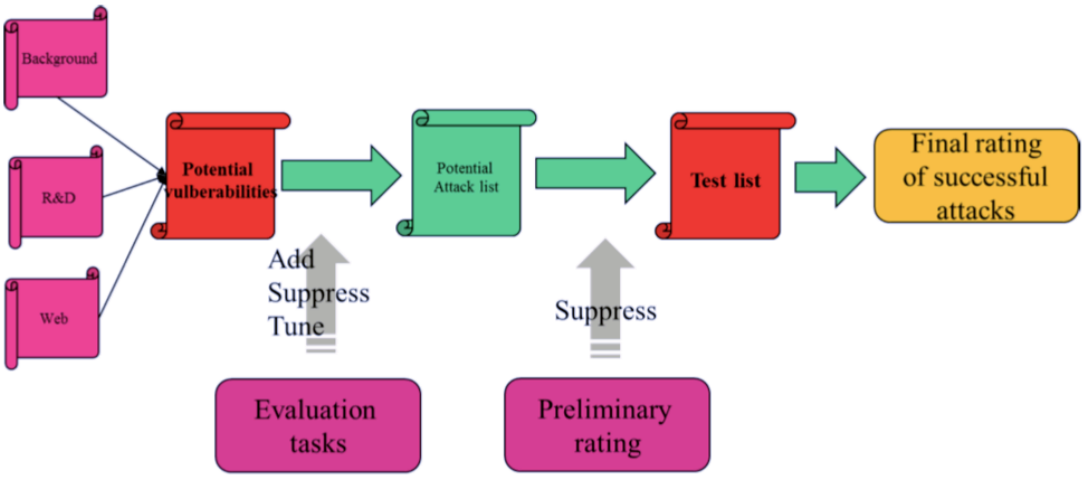
Cómo último aspecto a considerar, la guía da a conocer de manera detallada, la forma de evaluación de las diferentes vulnerabilidades de los sistemas biométricos en el contexto del aseguramiento. Se establece cuatro aspectos:

- Establecer una metodología para las tareas propias de AVA (Análisis de vulnerabilidades).
- Metodología para establecer la protección del sistema.
- Definición de niveles de criterios comunes (estimación de riesgos).
- Ejemplos de tipos de ataques y su respectiva calificación.

Dentro de la metodología de evaluación de vulnerabilidades, se establece como objetivo la búsqueda de brechas de seguridad demostrando que el TOE puede llegar a ser resistente ante un potencial ataque predefinido. El proceso de evaluación se centrará en encontrar un tipo de ataque, el cual, obtendrá un nivel de calificación que logrará identificar fallas en los objetivos de seguridad del sistema evaluado. Previo a esto, se debe establecer una lista de pruebas, en las

cuales, el evaluador ejecuta ataques, y de ser exitosos, imparte una calificación final. [105]

Figura 30. Metodología de evaluación de vulnerabilidades.



Fuente: N. Tekampe (TUViT), A. Merle, (CEA), J. Bringer (Mor- pho), M. Gomez-Barrero (UAM), J. Fierrez (UAM), J. Galbally (UAM). Biometrics Evaluation and Testing. [En línea]. beat-eu.org/, 2011. [Recuperado en 17 de octubre 2020]. Disponible en: https://www.beat-eu.org/project/deliverables-public/d6-5-toward-common-criteria-evaluations-of-biometric-systems

Considerando un marco de evaluación establecido, en particular para los sistemas biométricos NFIS y Match on Card, conociendo de manera preliminar la existencia de algunas iniciativas por Europa, Estados Unidos y Asia que se consideran aisladas, desorganizadas y/o limitadas en el tiempo, desencadenando esfuerzos discontínuos y no integrados, BEAT establece este marco de evaluación como estándar para tecnologías biométricas, lo anterior, por medio de una plataforma que permite un proceso de verificación transparente e independiente por medio de tres aspectos: plataformas establecidas, diseño

[105] Ibíd., p. 69.

de protocolos y herramientas para análisis de vulnerabilidades y por último, estandarización de criterios comunes. Por medio de BEAT se pretende:

- Establecer confiabilidad en los sistemas biométricos, que sean medibles.
- Transferencia tecnológica de las investigaciones a las organizaciones que sea mucho más sencilla junto con un marco interoperable.
- A los tomadores de decisiones y autoridades informar acerca de los avances en las tecnologías biométricas logrando un impacto articulado en lo estándares nuevos y existentes.

6.3.2 KBOC (Keystroke Biometrics OnGoing Competition). La competencia continua de biometría de pulsaciones de teclas (KBOC), representa una línea base que permite establecer la autenticación de personas por medio de la biometría de pulsación de teclas. Este tipo de competencias ha sido desarrollada por medio del marco de evaluación BEAT, mencionado con anterioridad, involucrando una base de datos que contiene pulsación de teclas de gran tamaño tanto para usuarios legítimos como para impostores.

Este tipo de eventos presenta interés conforme el modelado y coincidencia de las diferentes secuencias con diferentes rangos de variabilidad, lo anterior, permite definir la competencia KBOC como aquella que supera las limitaciones presentadas conforme competencias tradicionales por medio de un *Benchmark* público que involucra aproximadamente 3.600 secuencias de acuerdo a la pulsación de teclas de 300 usuarios, acercándose a un escenario realista por medio del cual cada uno escribe su propias identidades y 3.600 usuarios generan ataques propios de impostores.

Existen dos modelos de participación para *Keystroke Biometrics OnGoing Competition*: Inicialmente, se tiene la participación continua que se dará en el marco de la plataforma BEAT, con ella, la implementación de la evaluación tecnológica biométrica, permitiendo: 1. Acceso gratuito a comunidad investigadora. 2. Cálculo del alto rendimiento. 3. Entorno WEB. 4. Compatibilidad con código Python. 5. Eventos públicos y privados de participación.

Un segundo escenario, en el cual los participantes tendrán acceso a un entorno de entrenamiento generando el envío de hasta quince presentaciones en una fecha límite estipulada, que está directamente relacionada con algoritmos que representan los escenarios de iteración. [106]

Keystroke Biometrics OnGoing Competition ha sido un referente de evaluación biométrica, esto es demostrado por investigadores de la Universidad Autónoma de Madrid quienes incluyeron secuencias de pulsaciones de teclas de aproximadamente 300 usuarios en cuatro sesiones diferentes; los resultados obtenidos en este proceso investigativo, arrojan tasas EER (Equal Error Rate) del orden de los 5.32%, representando un referente para las nuevas y existentes tecnologías.

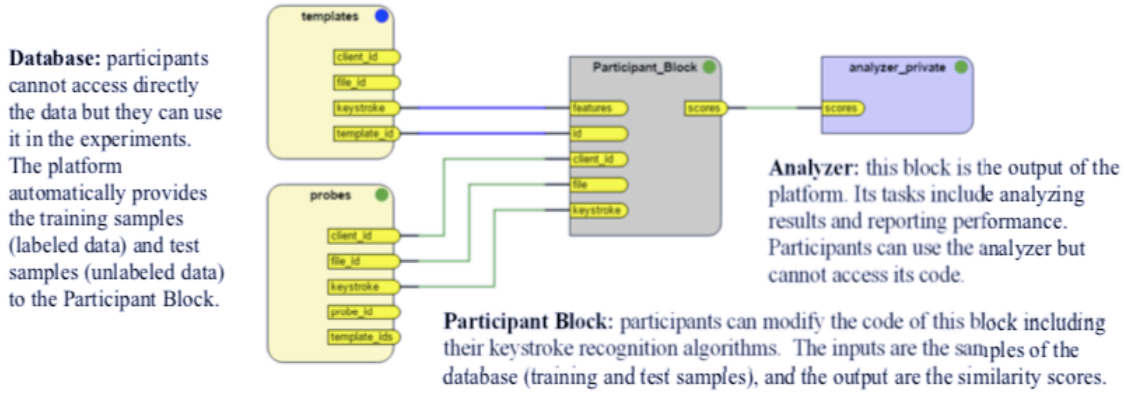
Como etapa inicial del proceso, los datos obtenidos corresponden a una secuencia de pulsaciones de 300 participantes, muestras tomadas en cuatro sesiones de adquisición diferentes, lo anterior conforme una variable de tiempo: 1. Muestras dentro de una misma sesión. 2. Muestras dentro de semanas (dos sesiones consecutivas). 3. Muestras en meses. Ya tomados los datos necesarios, se procede a establecer el marco de trabajo basado en la plataforma BEAT, creada bajo el proyecto FP7 EU BEAT, aprovechando sus utilidades en referencia a la experimentación y el reconocimiento de patrones, que entre otros, permite generar la evaluación de sistemas sin límite y los resultados proporcionados se dan de manera automática.

En la figura número 31, se logra identificar los módulos involucrados por medio de KBOC para la evaluación y la experimentación llevada a cabo: inicialmente, se involucra la base de datos por medio de los módulos de pruebas, aclarando que no se tiene acceso a esta información (manteniendo su confidencialidad), no obstante, su uso se puede dar en los procesos de evaluación; la base de datos genera información que presentan una normalización y etiquetado, como también datos que no se encuentran normalizados. Se específica un bloque

[106] A. Morales, J. Fierrez, M. Gomez-Barrero, J. Ortega-Garcia, R. Daza, J.V. Monaco, J. Montalvão, J. Canuto, A. George, "KBOC: Keystroke Biometrics OnGoing Competition", Proc. 8th IEEE International Conference on Biometrics: Theory, Applications, and Systems, Buffalo, USA, pp. 1-6, 2016. Disponible en: https://sites.google.com/site/btas16kboc/home

correspondiente a participantes, en el cual se permite la manipulación y modificación de su código, estableciendo cambios en los datos de entrada y la puntuación de salida. Por último, el módulo de análisis, que permite un análisis de los resultados obtenidos articulado a un reporte de desempeño del sistema evaluado.

Figura 31. Herramientas KBOC y módulos involucrados en la evaluación.



Fuente: A. Morales, J. Fierrez, M. Gomez, J. Ortega, R. Daza, J. Monaco, J. Montalvo, J. Canuto, A. George. KBOC: Keystroke Biometrics OnGoing Competition. [En línea]. [Recuperado en 7 de noviembre de 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/681563/kboc_morales_btas_2016_ps.pdf?sequence=1&isAllowed=y

Para la presente competición, se tuvo el registro de 12 instituciones de 7 países: E.E.U.U., India, Noruega, Argelia, Holanda, Brasil y China, obteniendo la presentación de cuatro sistemas dando a conocer a continuación, los dos mejores, evaluados durante la competencia.

6.3.2.1 U.S. ARMY RESEARCH LABORATORY. El sistema presentado por el laboratorio de investigación de las fuerzas armadas de los Estados Unidos, presentó resultados pequeños en cuanto a la tasa de error ERR (Equal Error

Rate), 6.95%: Los resultados satisfactorios son atribuidos al pre-procesamiento y normalización de la información.

6.3.2.2 Universidad Federal de Sergipe (Brasil). Por medio de los estudios realizados por la Universidad Federal, se establecieron tres parámetros para el proceso experimental: 1. El número de muestras por persona no se conocen. 2. Se desconoce el número de muestras genuinas e impostores. 3. Las muestras secuenciales identificadas y obtenidas, no pueden ser utilizadas para mejorar puntuaciones anteriores; reconociendo los anteriores lineamientos, para con cada muestra se determinó un par de vectores: PP (*Press-Press*) y H (*Hold-time*), el primero que considera el patrón empleado por el usuario para el registro de caracteres, el restante, que hace referencia al tiempo dispuesto; ya para el proceso de evaluación, se establece como parámetro la geometría de distancia de Manhattan, en la cual se estipula que la distancia entre dos puntos es la suma de sus diferencias (absolutas), y para la experimentación, se incluye una variable adicional en referencia a las longitudes de las muestras tomadas, obteniendo un valor ERR de 8.0%.

Las pruebas realizadas se basaron en indicadores EERG (Tasa de error global), EERU (Tasa de error dependiente del usuario) y el ya conocido DET (Curva de errores de detección), logrando reconocer por medio de las características del sistema el mejor sistema presentado, como se logra observar en la tabla número 2:

Tabla 2. Características mejores sistemas competencia KBOC.

Participant	Preproc.	Features	Feature norm.	Matcher	Score norm.
P1 – Indian Institute of Technology Kharagpur	No	Hold+RP	No	Combined	No
P2 – Federal University of Seripe	Yes	Hold+PP	No	Manhattan	No
P3 – Anonymous participant	No	RP	No	Kendall's tau	No
P4 – U.S. Army Research Laboratory	Yes	Hold+PP	Yes	Manhattan	yes

Fuente: A. Morales, J. Fierrez, M. Gomez, J. Ortega, R. Daza, J. Monaco, J. Montalvo, J. Canuto, A. George. KBOC: Keystroke Biometrics OnGoing Competition. [En línea]. [Recuperado en 7 de noviembre de 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/681563/kboc_morales_btas_2016_ps.pdf?sequence=1&isAllowed=y

En la tabla número 2 se logra observar los mejores sistemas, y en ellos, si se tuvo aspectos de pre-procesamiento, vectores utilizados, normalización (características y puntuación) y por último, parámetro de comparación. Así mismo, en la tabla número 3, se logra observar los porcentajes de error obtenidos por cada sistema evaluado, enfocándonos en particular en el número 4 (U.S. Army Research Laboratory), estableciendo para el mejor escenario una tasa ERR de 5.32%, cuya referencia es desafiante hacía futuras investigaciones. Allí es posible identificar la tasa EERg (umbral que es independiente del usuario), EERu (umbral que es dependiente del usuario), así mismo, resultados de las diferentes sesiones de competición efectuadas conforme la periodicidad de datos que se determinó.[107]

Tabla 3. Resultados mejores sistemas.

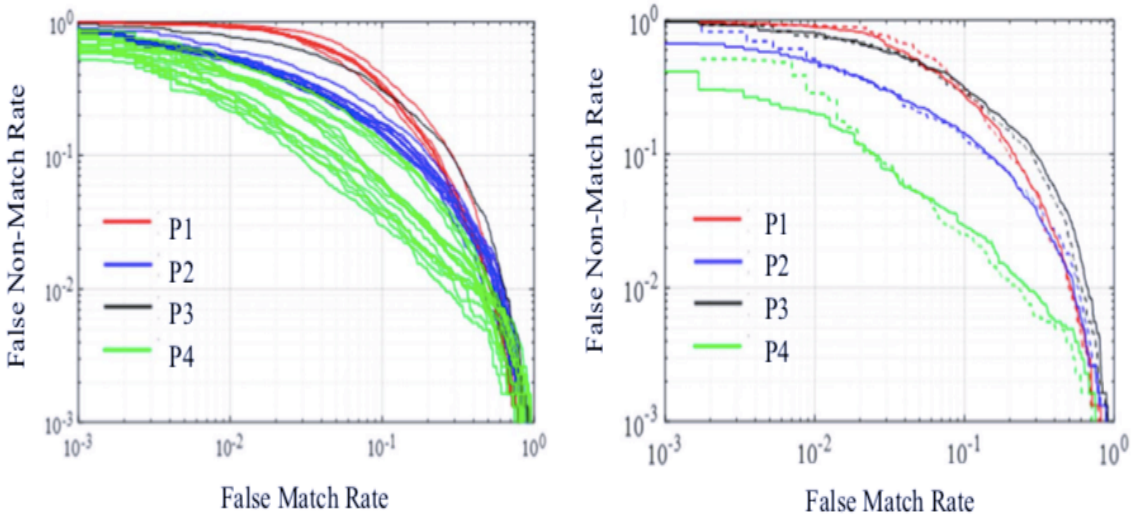
ID	EERG.	EERU	FMR100	Second Session	Fourth Session
P1	15.73%	11.95%	51.13%	15.28%	16.13%
P2	11.82%	7.96%	54.65%	11.60%	11.96%
P3	17.90%	13.66%	64.60%	17.01%	18.21%
P4	5.32%	4.72%	28.36%	5.09%	5.10%

Fuente: A. Morales, J. Fierrez, M. Gomez, J. Ortega, R. Daza, J. Monaco, J. Montalvo, J. Canuto, A. George. KBOC: Keystroke Biometrics OnGoing Competition. [En línea]. [Recuperado en 7 de noviembre de 2020]. Disponible en:

[107] Ibíd., p. 3.

https://repositorio.uam.es/bitstream/handle/10486/681563/kboc_morales_btas_2016_ps.pdf?sequence=1&isAllowed=y

Figura 32. Curvas DET resultados conforme sistemas evaluados.



Fuente: A. Morales, J. Fierrez, M. Gomez, J. Ortega, R. Daza, J. Monaco, J. Montalvo, J. Canuto, A. George. KBOC: Keystroke Biometrics OnGoing Competition. [En línea]. [Recuperado en 7 de noviembre de 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/681563/kboc_morales_btas_2016_ps.pdf?sequence=1&isAllowed=y

6.4 DESAROLLO DE OBJETIVO 4

Los sistemas biométricos dactilares, deben ser verificados, analizados y puestos a prueba por medio de pruebas de concepto POC, estándares, recomendaciones, entre otros. Los anteriores procesos deben considerarse imprescinbibles, pues en escenarios de acceso a sistemas de información que implican un grado de criticidad a nivel gobierno, en el sector privado y en las personas naturales, cualquier tipo de error o ataque informático, entre otros, como los descritos en la presente monografía, puede materializar riesgos catastróficos generando afectaciones incalculables.

En referencia a disposiciones legales, que buscan establecer responsabilidades y compromisos para con aspectos directamente relacionados con la protección de datos, y con ello, que se encuentran directamente relacionados con el uso e implementación de sistemas biométricos dactilares, como referente de carácter internacional, se tiene la ley de protección de datos francesa de 1978 titulada "ley de tecnología de la información, archivos y libertades civiles"[108], que establece requisitos particulares para con el tratamiento de los datos biométricos; así mismo, el Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos personales[109], del año 1981, la Directiva europea sobre la protección de las personas con respecto al tratamiento de los datos personales y la libre circulación de estos datos[110], del año 1995, la Resolución de las Naciones Unidas del 14 de diciembre de 1990, por último, el proyecto Reglamento General de Protección de Datos, adoptado por el parlamento europeo, que establece disposiciones que son relativas a los datos personales y son viables para adoptar a los sitemas biométricos dactilares, estos, por nombrar los más relevantes y significativos en cuánto a referentes a considerar para con los sistemas biométricos dactilares que daremos a conocer de manera mas detallada.[111]

6.4.1 A nivel normativo y reglamentario. Considerando que las primeras normas establecidas, y con ello, la reglamentación generada a nivel Gobierno y entes de seguridad asociados al mismo, en los años 1980, se establecieron estatutos en referencia a las huellas dactilares mencionadas en el punto anterior; tomando esto como referente para lo que en el año 2002 fue un punto de inflexión en referencia a la creación de estándares y normatividad internacional en

[108] CNIL - Comission Nationale de l'Informatique et des Libertés. Act Nº78-17 6 de enero de 1978. On Information Technology, Data Files and Civil Liberties [en línea]. Derecho y libertades informáticas – República de Francia, 1978. 45 p. [Consultado 3 de diciembre de 2020]. Disponible en: https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf
[109] Conseil de l'Europe - Consejo Europeo. Convenio para la protección de las personas con respecto al tratamiento automático de datos personales [en línea]. Conseil de l'Europe, 1981. 1 p. Consultado 3 de diciembre de 2020]. Disponible en: https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108
[110] Ibíd., p. 1.
[111] Ibíd., p. 1.

referencia principalmente a la seguridad de la información; se consignará a continuación los aspectos más relevantes de esas normativas creadas tomadas como parámetro y punto de partida para llegar a los que actualmente se tiene.

6.4.1.1 Ley de tecnología de la información, archivos y libertades civiles (Comisión nacional de informática y libertades (CNIL) enero de 1978). En el capítulo número tres dispuesto, y en el cual, se designa a la comisión nacional de informática y libertades como una autoridad administrativa independiente, con esto, se le hace responsable por la protección de los datos personales en su tratamiento biométrico, asegurando los sistemas de manera integral estableciendo el derecho al usuario de emitir reclamaciones, peticiones y quejas en referencia al tratamiento de sus datos personales.[112]

6.4.1.2 Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos personales. Se refiere al primer instrumento que, de carácter internacional, establecido en el año 1981, tiene como objetivo principal la protección a las personas en referencia al uso indebido que se le pueda dar a sus datos personales en sistemas automatizados, adicionalmente, con un alcance de flujo transfronterizo (restricciones en estados donde no existe protecciones equivalentes). Se establece exclusiones, por ejemplo, en cuanto a intereses a nivel Gobierno en referencia a seguridad pública, defensa, entre otros.[113]

6.4.1.3 Directiva europea sobre la protección de las personas con respecto al tratamiento de los datos personales y la libre circulación de estos datos. Establecida por el parlamento europeo, por medio de la cual se establece en varios de sus puntos controles referentes a la protección de datos personales; se hace hincapié en unos de sus puntos, en el cual se busca garantizar el uso de los datos personales de una forma lícita y leal, en particular, en el uso adecuado, pertinente y no excesivo conforme los objetivos inicialmente

[112] CNIL - Comission Nationale de l'Informatique et des Libertés. Óp. Cit., p. 6.
[113] Conseil de l'Europe. Óp. Cit. ., p 1.

establecidos; estos, no deben discrepar con los fines establecidos de manera preliminar.[114]

En referencia a naciones unidas, se establecen los siguientes principios entre los más relevantes: 1. Principio a la exactitud: Aquellos responsables de la compilación de repositorios, deben realizar validaciones periódicas con el fin de garantizar la integridad de la información. 2. Especificación de la finalidad: Los datos almacenados y registrados deben ser pertinentes y usados para el fin determinado, evitando fines incompatibles. 3. Principio de seguridad: Se consigna la necesidad de establecer controles para salvaguardar los datos personales ante la destrucción natural o accidental, el acceso no autorizado, el fraude y los virus informáticos.[115]

6.4.1.4 Reglamento General de Protección de Datos. Conforme el reglamento establecido por el parlamento europeo y el consejo de la unión europea establecido en el año 2016, se establece los datos biométricos como datos personales que hacen relevancia a características físicas, fisiológicas y/o de conducta de una persona; lo anterior, establece una serie de responsabilidades en el tratamiento de datos estableciendo competencias en organismos nacionales de carácter estatal y privado para su obtención, almacenamiento y manipulación.

Adicionalmente, en la sección número 2, se establecen medidas técnicas para una gestión del riesgo: 1. Técnicas de cifrado. 2. Controles para garantizar la confidencialidad, integridad y disponiblidad de los datos personales. 3. Planes

[114] Parlamento Europeoy del Consejo. Directiva 95/46/CE [en línea]. Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, 1995. 1 p. [Consultado: 3 de diciembre de 2020]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

[115] Naciones Unidas. Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales [en línea], A/RES//45/95, 1990, 1 p. [Consultado: 3 de diciembre de 2020]. Disponible en: https://www.un.org/es/documents/ag/res/45/list45.htm

de contingencia. 4. Planes de auditoría sobre los controles y salvaguardas establecidos.[116]

6.4.2 Estandarización nacional e internacional. En la actualidad, diferentes normas y estándares se están desarrollando por diferentes organizaciones, a destacar, la Organización Internacional de Normalización (ISO), la Comisión Electrónica Internacional (IEC) y el Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T); en lo que a consorcios se refiere, la Organización Internacional del Trabajo (OIT) establece directrices en referencia a la identidad biométrica.

El comité técnico mixto (JTC) de la ISO/IEC establece un número aproximado de 30 normas de carácter internacional en referencia a la biometría, con esto, técnicas de seguridad en referencia a plantillas y suplantación, algoritmos y auditoria a nivel de seguridad. La UIT-T, complementando lo mencionado, establece más de 70 recomendaciones en relación a seguridad a nivel infraestructura, servicios y aplicaciones, lo anterior, incluyendo terminales móviles y servicios que requieren métodos de autenticación que sean seguros y convenientes para los usuarios en biometría.[117]

6.4.2.1 Organización Internacional de Normalización ISO/IEC.

6.4.2.1.1 (ISO/IEC JTC1) Sub-Comité 17 (SC17). Conforme la clasificación internacional de estándares ISO (ICS) 35.240.15, se involucra marcos de trabajo enfocados en tarjetas de identificación, involucrando tecnologías biométricas en

[116] Parlamento Europeo News. Data protection reform - Parliament approves new rules fit for the digital era 2016. En: News Parlamento Europeo [sitio web]. Reino Unido. [Consulta 4 de diciembre 2020]. Disponible en: https://www.europarl.europa.eu/news/en/press-room/20160407IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era

[117] THALES Group. Biometría para identificación y autenticación [sitio web]. Francia. [Consulta 4 de diciembre 2020]. Disponible en: https://www.thalesgroup.com/es/countries/americas/latin-america/dis/gobierno/inspiracion/biometria

diferentes sectores: bancarios, comercio, telecomunicaciones y transporte. Con esto, se establecen métodos técnicos que se consideran adecuados y pertinentes para la identificación de individuos buscando proteger su identidad y con ello, los datos directamente relacionados a sus características físicas.

Este subcomité establece ocho grupos de trabajo, en los cuales cada uno realiza tareas específicas en cuánto al desarrollo y estudio de normalización en el área de identificación personal. Los grupos a resaltar, y en específico sobre la tecnología biométrica, se tiene el grupo número 9 (Estándares de tarjetas de memoria óptica) en referencia a tres aspectos que se disponen desde esta normativa: 1. Se proponen tecnologías cuyos fines permiten establecer una mayor capacidad a nivel de datos junto a un mejoramiento en referencia a la confiabilidad. 2. Componente software para un acceso seguro y oportuno (disponibilidad) a los contenidos biométricos. 3. Estructuración de datos por medio de un estándar de los datos.[118] Otro grupo importante a considerar, hace referencia a los estándares biométricos; allí se propone la interoperabilidad en cuánto a los sistemas implementados en el sector gobierno e industrias del sector privado, logrando establecer parámetros y estándares en cuánto a recomendaciones y buenas prácticas.

6.4.2.1.1.2 ISO/IEC 18013-3:2017 Control de acceso, autenticación e integridad.

Se establece por medio de este ítem mecanismos para la implementación de controles conforme el control de acceso a los datos, con ello, características a considerar conforme los tipos de datos abordados, las tecnologías utilizadas y los controles necesitados. Se establecen controles conforme un tipo de autenticación activa y pasiva; para con un tipo de autenticación pasiva, se pretende confirmar que los datos no han sufrido algún tipo de cambio desde su emisión, con ello, se establece la implementación de una firma digital junto con un tipo de codificación bien sea estándar, utilizando mensajes firmados

[118] International Organization for Standardization. ISO/IEC JTC 1/SC 17 Cards and security devices for personal identification [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/committee/45144/x/catalogue/p/0/u/1/w/0/d/0

digitalmente o compacta, utilizando una clave privada que mantiene el mensaje en secreto. Para con un tipo de autenticación activa, se establecen claves públicas y privadas, logrando por medio de la clave privada seguridad a nivel de la memoria estableciendo restricciones en cuanto a la confidencialidad de la información, por otra parte, por medio de la clave pública establecer un almacenamiento seguro.

Las acciones anteriormente descritas, en referencia a los tipos de autenticación, establecen protección ante ataques MitM (man in the middle attack) y con ello, intentos de lectura desconocidos, vulnerabilidades visibilizadas en el objetivo dos del presente trabajo monográfico.119

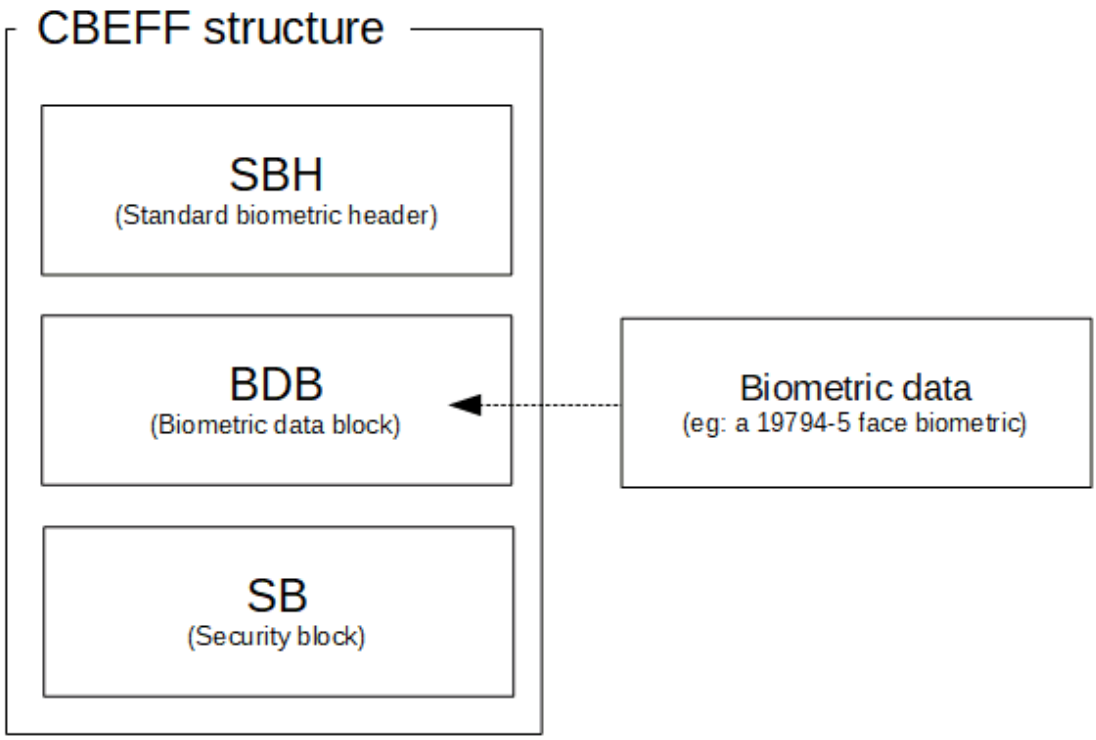
6.4.2.1.2 ISO/IEC (JTC1) Sub-Comité 37.

6.4.2.1.2.1 ISO/IEC 19785-4:2010 Marco de trabajo formatos de intercambio biométrico: Especificaciones formato bloque de seguridad. Por medio de este marco de trabajo, se establece la importancia de la implementación de técnicas que busquen disminuir los riesgos con base en la autenticación del usuario. Se establece que los datos provenientes de los diferentes usuarios deben garantizarse en cuánto a su legitimidad, por tanto, la integridad es un aspecto importante a considerar. La integridad, como el cifrado de los datos se establece en este marco de trabajo 19785, adhiriendo un concepto en referencia a bloque de seguridad (SB), el cual establece un formato de usuario CBEFF (Common Biometric Exchange File Format). En el formato CBEFF, es posible identificar el elemento CBEFF_BDB_encryption_options estableciendo el criterio que concluye la existencia de no encriptación y no integridad por medio del elemento CBEFF CBEFF_BIR_integrity_options. [120]

[119] International Organization for Standardization. ISO/IEC 18013-3: 2017 - Especificaciones formato bloque de seguridad [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/70486.html

[120] International Organization for Standardization. ISO/IEC 19785-4 2010 Especificaciones formato bloque de seguridad [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/50860.html

Figura 33. Common Biometric Exchange Formats Framework.



Fuente: Organización Internacional de Normalización (ISO/IEC JTC1). Common Biometric Exchange Formats Framework. [En línea]. [Recuperado en 6 de diciembre de 2020]. Disponible en: https://www.w3.org/2008/08/siv/Slides/Daon/CBEFF-Tilton-2009-short.pdf

Respecto al bloque de seguridad, se establecen dos formatos para abordar las necesidades expuestas en cuanto a seguridad: un primer formato, para fines de protección en cuanto a integridad y confidencialidad, haciendo uso de RFC 3852 *Cryptographic Message Syntax (*CMS), estándar promovido por la IETF (Grupo de trabajo de Ingeniería de Internet) cuyo fin es establecer parámetros para el cifrado de mensajes, establece modificaciones en los siguientes criterios: *EnvelopedData, EncryptedData, SignedData y AuthenticatedData*, estableciendo las configuraciones necesarias y los parámetros a modificar, buscando satisfacer de manera articulada las necesidades expuestas conforme el formato CBEEF. Un segundo formato, es definido por RFC 3852,

estableciendo parámetros de autenticación buscando niveles de seguridad satisfactorios en cuanto aspectos de autenticación.[121]

6.4.2.1.2.2 ISO/IEC 19795. Biometric performance testing and reporting. Se establece un marco de trabajo que se define en cinco partes que buscan estandarizar pruebas en sistemas biométricos: 1. Principios y marco de trabajo. 2. Metodologías de pruebas y escenario de evaluación. 3. Informe técnico. 4. Pruebas de rendimiento en diferentes formatos de datos. 5. Rendimiento sistemas de control de acceso biométrico.

- **ISO/IEC Evaluación de desempeño biométrico y reporte:** Este tipo de pruebas prestablecidas permiten determinar las diferentes tasas de error y rendimiento logrando comprender y además, predecir el comportamiento de los sistemas biométricos. Las tasas de rendimiento obtenidas hacen hincapié en el número de usuarios procesados por unidad de tiempo, tomando variables en relación a velocidad de cálculo e interacciones en sistemas biométricos dactilares.[122] Se establecen tres tipos diferentes de pruebas biométricas: según la tecnología, según el escenario y según su operatividad. Así mismo, se articulan recomendaciones conforme documentos fuente como el desarrollado por el Instituto Nacional de Normas y Tecnología (NIST) *Overview methodology, systems, results, perspective*[123]

  La ISO|IEC 19795 especifica métricas en relación al rendimiento de los sistemas biométricos, requisitos en referencia a métodos de prueba, registro de datos e informes obtenidos, marcos de referencia para desarrollo de pruebas y desarrollo, buscando definir términos de tasa de error y rendimiento.[124]

[121] Ibíd., p. 1.
[122] International Organization for Standardization. 19795-1:2006 Evaluación de desempeño biométrico y reporte [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/41447.html
[123] Ibíd., p. 1.
[124] Ibíd., p. 1.

- **ISO/IEC 19795-2:2007 Metodologías de pruebas y escenario de evaluación.** En este segundo aspecto, se involucra dos tipos de pruebas en el rendimiento de los sistemas biométricos: inicialmente, una basada en la tecnología y la restante, se enfoca en una evaluación de acuerdo a los escenarios. En cuanto a los aspectos relacionados con tecnología, se realiza una evaluación en cuánto a los algoritmos de inscripción y comparación, por otra parte, en los escenarios se evalúan diferentes sensores y algoritmos conforme el procesamiento de muestras que fueron recolectadas en tiempo real.

  La ISO/IEC 19795 permite proporcionar a los desarrolladores, implementadores y adicionalmente, usuarios finales, mecanismos, estándares y herramientas para el diseño, ejecución y desarrollo de los informes correspondientes a las pruebas de rendimiento biométrico logrando identificar una evaluación comparativa permitiendo observar de manera significativa datos en referencia al rendimiento en diferentes escenarios.[125]

- **ISO/IEC 19795-3:2007 Pruebas conforme las diferentes modalidades de sistemas biométricos.** Conforme el sistema biométrico evaluado, se debe incluir la siguiente característica que corresponden un parámetro a evaluar en los sistemas biométricos y que inciden en los resultados obtenidos: se debe verificar los resultados obtenidos conforme las características de los usuarios y los impostores; en los impostores debe definirse dos modalidades: inicialmente, la modalidad conforme la recopilación de múltiples datos, donde se hace necesario definir una regla permisiva y una regla restrictiva en cuánto a los intentos impostores; por otra parte, la modalidad basada en comportamiento, en la cual es relevante la tasa falsa de aceptación (FAR) que permite identificar si un impostor imita un usuario legítimo. En el momento en que un impostor rastrea y con ello, hace seguimiento a un tipo de huella de un usuario, se

[125] International Organization for Standardization. 19795-2:2007 Metodologías de pruebas y escenario de evaluación [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/41448.html

obtiene valores atípicos y característicos. Esta parte de la normativa ISO 19795, toma como referencia seis informes técnicos conforme estandarización publicada por la Asociación Japonesa de Normas JIS-TRs, cuyo objetivo es definir procedimientos claros y específicos para el desarrollo de pruebas y la recopilación de datos.[126]

- **ISO/IEC 19795-4:2007 Pruebas de rendimiento en interoperabilidad.** Se define un formato estándar con fines de intercambio de datos biométricos que permite definir características para imágenes, señales y en general datos, restringiendo propiedades de las muestras que buscan ofrecer un mayor rendimiento en cuánto al proceso de reconocimiento y con ello, establecer un nivel de confidencialidad. El estándar ISO/IEC 19794-2 establece implementar un tipo de codificación XML, que es atribuido por el estándar como plantilla de implementación; así mismo, en referencia a la interoperabilidad se establece tres tipos de pruebas en los sistemas:
    - Prueba en línea: se define una población de voluntarios con el fin de utilizar sistemas de verificación de identidades por medio de muestras genuinas y de impostores.
    - Prueba fuera de línea: las pruebas realizadas fuera de línea, corresponden a muestras que han sido capturadas y almacenadas con el fin de verificar los procesos de identificación conforme intentos genuinos e impostores.
    - Prueba híbrida: este tipo de pruebas busca contextualizar y simular un entorno de condiciones operativas generando posteriormente un almacenamiento con fines de análisis fuera de línea. [127]
- **ISO/IEC 19795-5:2007 Control de acceso y esquema de calificación:** se establece un control de acceso y con ello, un escenario común, con el fin de establecer un proceso de evaluación que permita tomar como

[126] International Organization for Standardization. 19795-3:2007 Pruebas conforme las diferentes modalidades de sistemas biométricos [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/41449.html

[127] International Organization for Standardization. 19795-4:2007 Pruebas de rendimiento en interoperabilidad [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/46329.html

referencia parámetros cuantitativos junto con niveles de rendimiento. ISO/IEC 19795 establece una tasa mínima de falsa aceptación (FAR) de 0.1%.[128]

6.4.2.1.2.3 ISO/IEC 30107. *Biometric presentation attack detection*. Respecto al aumento del uso de los sistemas biométricos, con esto, el interés del mercado por los procesos de autenticación de usuarios, de forma paralela los diferentes tipos de ataques han incrementado a nivel sensorial que llevan a considerar los siguientes aspectos en la presente norma establecida: 1. Marco de trabajo que define parámetros para los diferentes tipos de ataques. 2. Formato de datos. 3. Pruebas e informes. 4. Perfil de prueba en dispositivos móviles. La ISO/IEC 30107 aborda las técnicas para la detección de ataques a nivel de presentación PAD (Detección de Ataques de Presentación).

- **ISO/IEC 30107-1:2016 PAD:** Considerando los diferentes tipos de ataques posibles en los sistemas biométricos, en particular, aquellos generados en la presentación y recopilación de características dactilares, se establecen contramedidas para detectar y prevenir intentos de acceso ilegítimos. La ISO/IEC 30107-1 establece una técnica automatizada denominada PAD (Detección de ataques de presentación), delimitando esfuerzos de visibilidad y control en el punto de recopilación de datos, lo anterior, por medio de la verificación de falsos positivos como falsos negativos ante diferentes tipos de aplicaciones en sistemas biométricos; el PAD es proporcionado con el fin de definir los términos a utilizar así como un marco que permita identificar los tipos de eventos de ataque en la etapa de presentación, permitiendo su clasificación, categorización, detalles e información detallada para la toma de decisiones. Por último, es necesario aclarar que esta norma internacional no determina una

[128] International Organization for Standardization. 19795-5:2007 Control de acceso y esquema de calificación [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/51768.html

herramienta PAD estándar a utilizar, no obstante, determinar los lineamientos a considerar. [129]

- **ISO/IEC 30107-2:2016 Formato de datos**: Se establece por medio de este apartado formatos de datos comunes considerando los tipos de ataque en la presentación y transmisión, con ello, esquemas de encriptación de datos y codificación que corresponde a un formato de tipo binario y de esquema XML (*Extensible Markup Language*).
- **ISO/IEC 30107-3:2016 Pruebas e informes**: Conforme el PAD establecido en la parte 1 de esta normativa, se establecen los siguientes aspectos a considerar para la clasificación y presentación de la información obtenida: 1. Información estadística relevante. 2. Comparativa de resultados entre sistemas. 3. Cooperación conforme hallazgos. 4. Evaluaciones automatizadas. 5. Calidad y rendimiento.
    - Se realiza un set de pruebas de rendimiento buscando obtener datos representativos en cuánto a tasa de error y con ello, tomando como referencia el valor establecido de 0.1%. Adicionalmente, se considera que día a día los tipos de ataques cambian siendo imposible determinar un PAI (Ataque de Presentación Potencial) definido, por tanto, para con cada tipo de PAI a analizar la incertidumbre estará directamente relacionada con la estimación de tasa de error en referencia al número de muestras procesadas y al sistema involucrado.
    - Para establecer un rendimiento biométrico por medio de una comparativa de resultados, se debe considerar el sistema evaluado y con ello, se reconoce las tasas de error específicas logrando representar los resultados con otro sistema de configuraciones diferentes. Adicionalmente al PAI identificado, igualmente se debe reconocer las especies de PAI identificados, y con ello, su criticidad y materialización del riesgo.

[129] International Organization for Standardization. 30107-1:2016 Biometric presentation attack detection — Part 1: Framework [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/53227.htm

- Los hallazgos que se logran observar pueden verse representados por los individuos que se involucran en la toma de datos, con ello, se deduce que en las pruebas de control de acceso existe por parte del usuario la falta de conocimiento, la inexperiencia y falta de orientación que genera errores en la toma de datos y con ello, fallas en las tasas de error obtenidas para evaluar el desempeño del sistema biométrico si se considera un contexto ideal. Las pruebas PAD mencionadas en este ítem, hacen hincapié en el conocimiento del evaluador del sistema para cambiar drásticamente las tasas de éxito de un posible ataque.
- La automatización de pruebas no se considera un acierto al momento de generar una evaluación de un sistema biométrico, por tanto, que los datos de un sensor biométrico en una prueba PAD pueden cambiar en relación a otro sistema, generando errores e información que no es acertada para el sistema que se pretende verificar su rendimiento.
- En referencia a la calidad y desempeño del sistema, se considera que los datos están directamente relacionados a los resultados obtenidos: las muestras con una calidad deficiente, generarán un valor de tasa de error considerable, por el contrario, si las muestras corresponden a una calidad alta de datos, la tasa de error disminuirá. No obstante, en ausencia de un modelo de ataque definido, se debe asumir el “peor caso” en el cual un atacante utiliza la mejor calidad de datos para asumir un caso de ataque de éxito. Se definen tres aspectos importantes para el análisis: 1. Los diferentes tipos de PAI (Ataque de presentación potencial) deben ser analizados y verificados por separado. 2. Para un tipo de PAI, cuya tasa de error sea diferente de 0%, debe considerarse que un ataque puede llegar a tener éxito. 3. Las diferentes tasas de error obtenidas están determinadas por las aplicaciones utilizadas, el

método de prueba utilizado, el evaluador y el mecanismo PAD (Detección de ataques de presentación) considerado.[130]

6.4.2.1.3 (ISO/IEC JTC1) Sub-Comité 27 (SC27). Por medio del Sub-comité CS27 se abordan temas relacionados con técnicas de seguridad TI, que establecen objetivos principalmente en la protección de plantillas biométricas, seguridad de algoritmos y marcos de evaluación de seguridad.

6.4.2.1.3.1 ISO/IEC SC27/WG 1. Information security management systems. El primer equipo de trabajo perteneciente incluye métodos, técnicas, y diferentes tipos de pautas genéricas con el fin de abordar aspectos en relación a la seguridad y confidencialidad estableciendo metodologías conforme la captura de datos y la gestión de la información. Se establecen mecanismos en referencia a la criptografía involucrando terminología, directrices y procedimientos conforme componentes de seguridad estipulados en referencia a la gestión de identidad, biometría y privacidad de los datos.

6.4.2.1.3.2 ISO/IEC SC27/WG 2. Mecanismos de seguridad y criptografía. En este grupo de trabajo se establece criterios técnicos con el fin de cumplir con la confidencialidad, integridad y disponibilidad de la información por medio de técnicas de criptografía. Conforme lo anterior, se han desarrollado diferentes tipos de estándares que han sido desarrollados en diferentes épocas generacionales: una primera generación, establece parámetros para la autenticación de identidades y firmas digitales estableciendo algoritmos de cifrado estándar por medio de la aritmética modular; una segunda generación, caracterizada por el desarrollo de encriptación avanzada incluyendo el grupo de trabajo SC17 mencionado con anterioridad, la ITU-T y la IETF. A diferencia de la primera generación, para esta ocasión se involucra encriptación en base

[130] International Organization for Standardization. 30107-3:2016 Biometric presentation attack detection — Part 3: Testing and reporting [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/51768.html

logarítmica. Para una tercera generación, este grupo de trabajo direcciona y enfoca sus investigaciones y trabajos en la definición de estándares criptográficos con mecanismos y algorítmos con fines de cumplimiento empresarial en el marco de la ciberseguridad. En los últimos desarrollos, se involucran mecanismos en referencias a técnicas de cifrado de tipo simétrico y asimétrico.[131]

6.4.2.1.3.3 ISO/IEC SC27/WG 3. Evaluación, prueba y especificación de seguridad. Este grupo de trabajo permite establecer criterios con el fin de definir estándares internacionales para la evaluación de productos y sistemas TI; hasta ese momento, los diferentes gobiernos y entidades privadas habían generado el desarrollo individual de los diferentes enfoques para la evaluación de los productos y en general, sistemas de TI. Es por esta razón que nace el *Common Criteria* (CC), definiendo criterios propios proporcionando recursos como marco para garantizar la seguridad a nivel de TI en conjunto con una guía que establece perfiles de protección y objetivos enfocados a proteger la información.[132]

El *Common Criteria* establece un TOE (*Target of Evaluation*), con el fin de describir las funcionalidades del sistema de verificación biométrica definiendo unos requisitos funcionales y de garantía por medio de los diferentes procesos del sistema biométrico mencionados en esta monografía descartando aquellos que no se consideren relevantes.[133]

6.4.2.1.3.4 ISO/IEC SC27/WG 4. Estandarización frente ataques avanzados de ciberseguridad. Por medio del grupo de trabajo número cuatro, en el marco

[131] Yoshida, H. The overview of SC 27/WG 2 and lightweight cryptography [sitio web]. [Consulta 11 de diciembre 2020]. Disponible en: https://www.il-pib.pl/images/stories/FSC/pdf/7_Dr-Hirotaka-Yoshida_The-overview-of-SC-27WG-2-and-lightweight-cryptography_17092020.pdf

[132] CSRC NIST. ISO/IEC JTC 1/SC 27 "IT Security Techniques [en línea]. NIS. p. 1 [Consultado 9 de diciembre 2020]. Disponible en: https://csrc.nist.gov/csrc/media/publications/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999/documents/papers/o24.pdf

[133] ISO/IEC. Information technology - Security techniques - Identity management and privacy technologies [sitio web]. ISO/IEC JTC 1/SC 27/WG 5, Alemania. [Consultado 9 de diciembre 2020]. Disponible en: https://www.din.de/resource/blob/78926/97764df63cb1d7efa02a351c4f3b7b8e/sc27wg5-sd4-data.pdf

del sub-comité 27, se establecen aspectos en referencia a controles y servicios de seguridad, estableciendo un énfasis en los estándares de seguridad TI y la aplicación de seguridad a productos, así como también la seguridad en el ciclo de vida del sistema evaluado. En este marco de estandarización se consideran los siguientes aspectos:

- En relación a las operaciones de seguridad en las TIC, se hace referencia a la preparación, continuidad, gestión de incidentes y eventos.
- El ciclo de la información debe considerarse, por tanto, la creación, el procesamiento, el almacenamiento, la transmisión y eliminación de la información son procesos que involucran mejores prácticas propuestas en el marco del ISO / IEC TR 29149. Adicionalmente, en referencia a las buenas prácticas allí descritas, se dan incluyen consideraciones técnicas cuyo fin se basa en proporcionar y garantizar los tiempos salvaguardando la integridad de los datos y el no repudio.[134]

6.4.2.1.3.5 ISO/IEC SC27/WG 5. Gestión de identidad y privacidad. Por medio de este punto, se pretende definir un proceso de evaluación para los estándares (SPA - Standards Privacy Assessment); implicito a este proceso de evaluación, se busca fortalecer la privacidad, dado que esta evaluación se enfoca en el posible impacto que se pueda generar en la privacidad de un estándar. Se consideran principios de privacidad aplicables junto con requisitos de protección pretendiendo evaluar amenazas potenciales buscando su mitigación.

El proceso SPA establece 7 pasos: 1. Identificar de manera clara la descripción del funcionamiento del sistema. 2. Identificar y analizar el flujo de datos de los diferentes componentes del proceso. 3. Generar una clasificación de los datos con el fin de lograr comprender los datos procesados identificando su ciclo de vida. 4. Establecer principios de privacidad que se crean convenientes. 5. Listar

[134] ISO/IEC. Standards Application against Advanced Cybersecurity Attacks [sitio web]. China, 2018. [Consultado 9 de diciembre 2020]. Disponible en: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180828/Documents/Jinghua%20Min.pdf

amenazas identificadas respecto al flujo de datos analizado, posterior a su clasificación y los requisitos de privacidad aplicables. 6. Más alla del análisis en referencia a la privacidad, se consideran reglas de trnasferencia segura y reglas a nivel de autenticación e identificación.[135]

6.4.2.1.3.6 ISO/IEC 24745. Técnicas de seguridad – Protección de información biométrica. Por medio de este apartado se establece una guía para estandarizar un nivel de protección en la seguridad biométrica bajo requisitos en referencia a la confidencialidad, integridad y control frente al almacenamiento y transferencia de la información. Por medio de esta norma se especifica: un análisis de vulnerabilidades y salvaguardas conforme los modelos de aplicación de los sistemas biométricos; requisitos de seguridad en referencia al proceso de identificación; modelamiento de los sistemas biométricos en diferentes escenarios en referencia al almacenamiento y comparativas con otros sistemas; orientación y recomendaciones en cuánto a la protección de la privacidad de los individuos durante el procesamiento de los datos biométricos.[136]

6.4.2.1.3.7 ISO/IEC 19989. Criterios y metodología para evaluación de seguridad en sistemas biométricos. Se establece una serie de criterios con el fin de establecer la evaluación en referencia a la seguridad del reconocimiento biométrico junto con la detección de ataques de presentación en referencia a la verificación e identificación biométrica.[137]

6.4.2.1.3.7.1 ISO/IEC 19989. Parte 1. Marco de referencia. Los sistemas biométricos son vulnerables en referencia a técnicas que pretenden copiar

[135] Dawson, F. Creating Privacy Considerations for W3C Technical Specifications [sitio web]. 2013. [Consultado 9 de diciembre 2020]. Disponible en: https://yrlesru.github.io/SPA/
[136] ISO/IEC. Information technology — Security techniques — Biometric information protection [en línea]. ISO/IEC 24745:2011. 2011. [Consultado 9 de diciembre 2020]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:24745:ed-1:v1:en
[137] ISO/IEC. Information security — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework [en línea]. ISO/IEC 19989-1. 2020. [Consultado 9 de diciembre 2020]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:19989:-1:ed-1:v1:en

caracteristicas y con ello falsificar datos. Este tipo de ataques de presentación, identificados en el objetivo dos de esta monografía, pueden llegar a presentarse durante la inscripción, identificación y/o verificación, con ello, se consideran salvaguardas que permiten discriminar entre intentos de autenticación genuinos o diferencias entre características naturales.

En este marco de trabajo, se considera fundamental determinar y evaluar el rendimiento del sistema dado que es un aspecto influyente para la detección de ataques directamente relacionados con la seguridad del sistema biométrico; este punto, es aplicable al TOE conforme las características concluyentes del análisis del sistema.[138]

6.4.2.1.3.7.2 ISO/IEC 19989. Parte 2. Rendimiento del reconocimiento biométrico. En referencia a los ataques a sistemas biométricos en los cuales, se busca vulnerar la política de seguridad existente, que evita evadir las características biométricas de un individuo, se considera imprescindible la capacidad para que un sistema biométrico pueda discriminar entre ataques genuinos e impostores. En la parte dos de la ISO/IEC 19989 se cita la norma ISO/IEC 15408, que establece una guía como criterio estándar que se utiliza como base de evaluación de las propiedades y características de seguridad de los sistemas TI. Este modelo de evaluación de seguridad, establece siete niveles de evaluación (EL1 – EL7), en los cuales se involucra un perfil de proteccion, un objeto de evaluación, un objeto de seguridad y un nivel de evaluación de seguridad. Un perfil de protección, se define como un conjunto de requisitos de seguridad que se cumplen para una serie de necesidades de cara al consumidor; un objeto de evaluación, por ejemplo, en una aplicación se define como objetivo su sistema operativo, puertos publicados y servicios asociados; en referencia al objeto de seguridad, se determinan los requisitos de seguridad que se deben cumplir y con ello, definir los requerimientos para una aplicación o servicio; por último, se considera un nivel de evaluación de seguridad EAL (*Evaluation Assurance Level*) que define un conjunto de características y principalmente,

[138] Ibid., p. 2.

requisitos en relación a la seguridad buscando proporcionar un nivel de confianza.

Tabla 4. EALs.

EAL	NAME	TSEC
EAL1	Functionally Tested	
EAL2	Structurally Tested	C1
EAL3	Methodically Tested / Checked	C2
EAL4	Methodically Designed, Tested & Reviewed	B1
EAL5	Semiformally Verified Design & Tested	B2
EAL6	Semiformally Verified Design & Tested	B3
EAL7	Formally Verified Design & Tested	A1

Fuente: C. Ficano. El Qualcomm Snapdragon 855 recibe la certificación de seguridad EAL-4+ [En línea]. [Recuperado en 12 de diciembre de 2020]. Disponible en: https://www.gizlogic.com/snapdragon-855-eal-4/

Como se logra observar en la tabla número 4, se identifica los 7 EAL citados en la ISO/IEC 19989; mencionando lo más relevante, EAL1 (funcionalidad aprobada) proporciona aspectos que generan relevancia en sistemas en los cuales se necesita un nivel de confianza alto conforme una operación correcta del sistema, no obstante, las amenazas no toman una relevancia grande; EAL2 (estructuralmente aprobado), define criterios para la ejecución de prueba caja negra (black-box) por parte del desarrollador del producto; EAL3 (probado y verificado metódicamente) se valida pruebas conforme caja-gris (grey box) para el desarrollador; EAL4 (diseñado, probado y revisado metódicamente) se considera que el desarrollar ejecuta acciones conforme buenas prácticas para el desarrollo comercial, las cuales son rigurosas, no obstante, no necesitan un nivel de conocimiento avanzado para su ejecución; EAL5 (diseñado y probado semiformalmente) se establece una máxima garantía para con los procesos de seguridad, por tanto, se realiza un análisis de vulnerabilidades conforme los posibles ataques de penetración; EAL6 (diseño verificado y probado

semiformalmente) la búsqueda de vulnerabilidades en este nivel, deben establecer una alta resistencia a los diferentes ataques de penetración, es por esto que se debe establecer un valor de protección alto de acuerdo a la estimación de los bienes o activos a evaluar; por último EAL7 (diseño verificado y probado formalmente), establece procesos de evaluación conforme un análisis formal y extenso conforme acciones de caja blanca (White-box).[139]

6.4.2.1.3.7.3 ISO/IEC 19989. Parte 3. Detección ataques de presentación. Se enfoca este ítem en la evaluación de seguridad conforme los ataques de presentación proporcionando recomendaciones conforme la ISO/IEC 19989-1 que establece un objetivo para un tipo de característica biométrica de múltiples características. La serie ISO/IEC 19989 establece una articulación entre la ISO/IEC 19792 antecesora de la mencionada ISO/IEC 19795, la cual estable los principios de evaluación para productos y sistemas biométricos y la ISO/IEC 15408 *Common Criteria*.[140]

6.4.2.2 Gartner Inc. Gartner Inc es una consultora e investigadora, mundialmente conocida, por sus aportes en referencia a la investigación tecnológica en cuánto al mercado, sectores y temáticas; igualmente, genera aportes en cuánto al análisis de las investigaciones realizadas enfocadas en los profesionales del sector TIC, empresas de tecnología y la comunidad en general, por medio de herramientas como lo son el cuadrante mágico; por último, el área de consultoría, brinda apoyo al sector privado y Gobierno en referencia a la adquisición de tecnología.

Gartner Inc, en referencia a los sistemas biométricos, reconoce esta tecnología como una base exclusiva para los procesos de autenticación humana, que reconociendo su implementación exponencial, establece la necesidad de

[139] ISO/IEC. Information security — Criteria and methodology for security evaluation of biometric systems — Part 2: Biometric recognition performance [en línea]. ISO/IEC 19989-2:2020. [Consultado 9 de diciembre 2020]. Disponible en: https://www.iso.org/standard/72403.html
[140] ISO/IEC. Information security — Criteria and methodology for security evaluation of biometric systems — Part 3: Presentation attack detection [en línea]. ISO/IEC 19989-3:2020. [Consultado 9 de diciembre 2020]. Disponible en: https://www.iso.org/standard/73721.html

generar en los próximos 2 y 3 años controles a nivel de seguridad y protección de datos. Gartner, establece una evaluación que involucra el análisis de los rasgos biométricos considerados en los sistemas, la autenticación e integración en dispositivos móviles de está tecnología, los riesgos, ataques de presentación y características, arquitectura, recomendaciones y proveedores representativos.

Figura 34. Magic Quadrant for Access Management.

Source: Gartner (November 2020)

Fuente: GARTNER INC. Gartner Magic Quadrant for Access Management [en línea]. Okta Named a Leader for the 4th Consecutive Year. [Consultado 9 de diciembre 2020]. Disponible en: https://www.okta.com/resources/access-management-leader-gartner-magic-quadrant/

Se destaca en el cuadrante mágico de Gartner el *Access Managment,* que se relaciona directamente con las consideraciones en los sistemas biométricos anteriormente expuestas; en dicho cuadrante, se presenta el resultado de un análisis de funcionalidades, tecnologías y tendencias de uso, brindando orientación hacía un proveedor teniendo implícitos aspectos en cuánto a requisitos básicos, metodologías y precios comerciales. [141]

[141] GARTNER INC. Gartner Magic Quadrant for Access Management [en línea]. Okta Named a Leader for the 4th Consecutive Year. [Consultado 9 de diciembre 2020]. Disponible en: https://www.okta.com/resources/access-management-leader-gartner-magic-quadrant/

CONCLUSIONES

Reconociendo las características y estructuras de los sistemas biométricos dactilares, así mismo, los procesos a nivel sensorial, extracción de características, comparador, y con ello, procesos implícitos, se identificó y analizó los aspectos relevantes a considerar relacionados a vulnerabilidades en el sistema que afectan la integridad, confidencialidad y disponibilidad, teniendo en cuenta la información directamente relacionada en cuánto a protección de datos personales.

Se identificó y analizó a detalle los ataques tipo *Timing y Hill-climbing* en los sistemas biométricos dactilares, reconociendo las metodologías de ataque en referencia al análisis del tiempo y los riesgos materializados, generando un análisis puntual y particular a los indicadores de compromiso implícitos en los eventos de penetración, entre ellos, la tasa de falso rechazo FR, la tasa falsa de aceptación FAR y la tasa de compensación de errores DET; los anteriores índices, permiten reconocer los aspectos a fortalecer y considerar en el proceso de implementación de sistemas biométricos dactilares en un ambiente de producción.

Es necesario analizar y distinguir que tasas de error se consideran relevantes para un tipo de sistema biométrico en un entorno y contexto de negocio particular. Existe en la actualidad parámetros, estándares, buenas prácticas y criterios que determinan aspectos relevantes a considerar para la evaluación de los sistemas biométricos dactilares, permitiendo establecer ideas concluyentes en referencia a la implementación, puesta en marcha y seguimiento de estos sistemas en un entorno productivo (trabajo a futuro).

Se realiza un análisis de dos sistemas en particular en cuánto a biométricos dactilares, con ello, se realiza una investigación de los procesos de evaluación BEAT y KBOC reconociendo aspectos relevantes en cuánto a las pruebas realizadas en dichos eventos de reconocimiento internacional; por medio de éste análisis, se logra reconocer la importancia de los indicadores anteriormente mencionados, dado que su análisis y verificación permiten generar ideas

concluyentes en cuánto a la efectividad y seguridad de los sistemas biométricos dactilares.

En la actualidad, existen normativas de carácter internacional que definen controles, metodologías y buenas prácticas, tanto para los procesos de implementación como de seguimiento y evaluación de los sistemas biométricos dactilares. La normatividad actual, se articula con sector Gobierno y privado que fortalecen los criterios y controles buscando estar a la altura de las nuevas tecnologías, como también, del respaldo de la información personal en referencia a la creciente demanda exponencial de los sistemas biométricos en el mundo.

Todos los sistemas de biometría dactilar, sin excepción, deben contar con la capacidad de detección de ataques PAD (Presentation Attack Detection). Ante la demanda comercial que crece de manera exponencial, estos controles que son considerados conforme la estandarización internacional, deben ser imprescindibles en los diferentes entornos de producción.

Se establece un *Common Criteria* como guía base para evaluar las propiedades y características de los sistemas biométricos dactilares, reconociendo los siete niveles de evaluación (*Evaluation Assurance Level*) que involucran la protección, el objeto de evaluación y el nivel de seguridad, otorgando un conjunto de requisitos que satisfacen las necesidades de cara al consumidor. Así mismo, el modelo Gartner, considera relevante establecer controles en cuánto a la seguridad y la protección de los datos, que serán evaluados, dando a conocer resultados en cuánto a funcionalidad, tecnología y comportamiento en entornos productivos.

Nuevos desafíos llegan de manera paralela a las nuevas tecnologías, es por esta razón, que los criterios y parámetros conforme las normativas existentes deben aplicarse de manera gradual y sistemática en los diferentes entornos de negocio, que hacen uso de las tecnologías de biometría dactilar, pues la información, como recurso tangible y de gran valor, debe ser protegida en cuánto a su confidencialidad, integridad y disponibilidad.

RECOMENDACIONES

Los sistemas biométricos dactilares, deben ser verificados, analizados y puestos a prueba por medio de pruebas de concepto (POC), estándares, recomendaciones, entre otros. Los anteriores procesos deben considerarse imprescinbibles, pues en escenarios de acceso a sistemas de información que implican un grado de criticidad a nivel gobierno, sector privado y en las personas naturales, cualquier tipo de error o ataque informático, como los descritos en la presente monografía, puede materializar riesgos catastróficos generando afectaciones incalculables.

A nivel normativo y de disposición legal, a considerar: como referente de carácter internacional, se tiene la ley de protección de datos francesa de 1978 titulada “ley de tecnología de la información, archivos y libertades civiles”, que establece requisitos particulares para con el tratamiento de los datos biométricos; así mismo, el convenio para la protección de las personas con respecto al tratamiento automatizado de los datos personalea, del año 1981, la Directiva europea sobre la protección de las personas con respecto al tratamiento de los datos personales y la libre circulación de estos datos, del año 1995, la Resolución de las Naciones Unidas del 14 de diciembre de 1990, y por último, el proyecto Reglamento General de Protección de Datos, adoptado por el parlamento europeo, que establece disposiciones que son relativas a los datos personales y son viables para adoptar a los sitemas biométricos dactilares.

Así mismo, es importante considerar el cuadrante mágico de Gartner en su apartado *Access Managment,* que se relaciona directamente con las consideraciones en los sistemas biométricos; en dicho cuadrante, se presenta el resultado de un análisis de funcionalidades, tecnologías y tendencias de uso, brindando orientación hacía un proveedor teniendo implícitos aspectos en cuánto a requisitos básicos, metodologías y precios comerciales.

En referencia a la Organización Internacional de Normalización ISO/IEC, se debe considerar lo establecido en la ISO/IEC 19785-4:2010, en la cual, se establece

un marco de trabajo que específica aspectos conforme un bloque de seguridad; allí se hace hincapié en referencia a la integridad y confidencialidad de la información por medio del cifrado de mensajes, bajo el estándar promovido por la IETF (RFC 3852), proponiendo configuraciones necesarias en cuánto al transporte, cifrado, firma y autenticación de los datos biométricos.

La norma ISO/IEC 30107 establece un marco de trabajo que define diferentes parámetros y consideraciones para con los tipos de ataques cibernéticos relacionados a los sistemas biométricos, específicamente, sobre la etapa de presentación y recopilación de información del sistema. Se considera la técnica automatizada PAD (Detección de ataques de presentación), que permite visibilizar eventos y por medio de su correlación y categoriazación, identificar registros que se relacionen a ataques sobre la información.

Así mismo, la norma ISO/IEC 19795, establece un marco de referencia para la evaluación del desempeño de los sistemas biométricos; allí se expone una metodología de pruebas, un escenario de evaluación, rendimiento e interoperabilidad, control de acceso y un esquema de calificación. Complementando esto, la ISO/IEC 15408, establece una guía de criterio de siete niveles de evaluación que buscan validar la funcionalidad, la estructura, pruebas de caja gris (grey box), criterios de diposición comercial y análisis de vulnerabilidades por medio de caja blanca (White-box), que no deben pasar por alto al momento de considerar las tecnologías de biometría dactilar.

TRABAJO A FUTURO

Considerando el precedente en relación a que si bien, existe tasas de error que se consideran relevantes para un tipo de sistema biométrico, es necesario continuar analizando los parámetros existentes y no existentes, articulados con estándares, buenas prácticas y criterios que determinen aspectos relevantes para la evaluación de sistemas biométricos dactilares, lo anterior, en entornos de laboratorio que permitan simular los diferentes escenarios de investigación, involucrando tecnologías disruptivas en un mundo interconectado.

BIBLIOGRAFÍA

A. MORALES, J. FIERREZ, M. GOMEZ-BARRERO, J. ORTEGA-GARCIA, R. DAZA, J.V. MONACO, J. MONTALVÃO, J. CANUTO, A. GEORGE, "KBOC: Keystroke Biometrics OnGoing Competition", Proc. 8th IEEE International Conference on Biometrics: Theory, Applications, and Systems, Buffalo, USA, pp. 1-6, 2016. Disponible en: https://sites.google.com/site/btas16kboc/home

ASATAÑO ESPAÑA, Julio y ROSALES DIAZ, Estela. La biometría dactilar como una opción para la seguridad informática [en línea]. 2011, agosto–diciembre, nro. 97. [Consultad: 25 de abril 2020]. Disponible en: http://pistaseducativas.itc.mx/wp-content/uploads/2012/02/3-ASATO-PE-97-44-58.pdf. ISSN: 1405-1249

BBC NEWS. Red de hackers afirma que clonó huella dactilar de ministra alemana. En: BBC NEWS Mundo. [sitio web]. Reino Unido. [Consulta 18 de mayo 2020]. Disponible en: https://www.bbc.com/mundo/ultimas_noticias/2014/12/141229_ultnot_hackeo_huella_dactilar_ministra_alemana_men

BEISNER MUÑOZ, Alicia. Ataques tipo “Side-Channel” a sistemas biométricos de reconocimiento de huella dactilar [en línea]. Título de Ingeniero Informático. Universidad Autónoma de Madrid, 2010. [Consultado 16 de Abril 2020]. Disponible en: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20100426AliciaBeisnerMunoz.pdf

CARBALLO DOMÍNGUEZ, Sara. Ataques indirectos a sistemas de reconocimiento de huella dactilar basados en los tiempos de comparación algorítmica [en línea]. Proyecto fin de carrera. Madrid: Escuela Politécnica Superior, 2009. [Consultado 28 de marzo 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/9991/51301_20090522SaraCarballo.pdf?sequence=1&isAllowed=y

CATAÑO RIVAS, Faiber. Mejoramiento en el procedimiento de seguridad de registro biométrico y carnetización en la compañía Frontera Energy de la ciudad de Bogotá [en línea]. Trabajo de grado para optar por el titulo de Administración de Empresas. Universidad Minuto de Dios, 2018. [Consultado 28 de marzo 2020]. Disponible en: https://repository.uniminuto.edu/handle/10656/6831?show= full

CENTRO EUROPEO DE POSTGRADO. ¿Qué es el cuadrante mágico de Gartner? [blog]. España. [Cosultado 17 de mayo 2020]. Disponible en: https://www.ceupe.com/blog/que-es-el-cuadrante-magico-de-gartner.html

CNIL - COMISSION NATIONALE DE l’INFORMATIQUE ET DES LIBERTÉS. Act Nº78-17 6 de enero de 1978. On Information Technology, Data Files and Civil Liberties [en línea]. Derecho y libertades informáticas – República de Francia,

1978. 45 p. [Consultado 3 de diciembre de 2020]. Disponible en: https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527 de 1999. (21, agosto, 1999). Reglamentos de acceso y uso de mensajes de datos. En: Diario oficial de Congreso de Colombia. Bogotá D.C., 1999.

COLOMBIA. CORTE CONSITUCIONAL. Sentencia C-1011 de 2008. (31, diciembre, 2008). Habeas data y regulación del manejo de la información. En: Gaceta de la Corte Constitucional. Bogotá D.C. Corte Constitucional y consejo de la judicatura, 2008.

COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1273 de 2009. (5, enero, 2009). De la protección de la información y los datos. En: MinTIC. Bogotá D.C, 2009.

CONSEIL DE L'EUROPE - CONSEJO EUROPEO. Convenio para la protección de las personas con respecto al tratamiento automático de datos personales [en línea]. Conseil de l'Europe, 1981. 1 p. Consultado 3 de diciembre de 2020]. Disponible en: https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108

CSRC NIST. ISO/IEC JTC 1/SC 27 "IT Security Techniques [en línea]. NIS. p. 1 [Consultado 9 de diciembre 2020]. Disponible en: https://csrc.nist.gov/csrc/media/publications/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999/documents/papers/o24.pdf

DAWSON, F. Creating Privacy Considerations for W3C Technical Specifications [sitio web]. 2013. [Consultado 9 de diciembre 2020]. Disponible en: https://yrlesru.github.io/SPA/

EUROPEAN COMMISION. Biometrics Evaluation and System. Londres. Seventh Framework Programme. 2012. [Consultado 17 de mayo de 2020]. Disponible en: https://cordis.europa.eu/project/id/284989

FAÚNDES ZANUY, Marcos. Experimentos prácticos sobre la vulnerabilidad de sistemas biométricos [en línea]. 2016. [Consultado 28 de marzo 2020]. Disponible en: https://docplayer.es/10065843-Experimentos-practicos-sobre-la-vulnerabilidad-de-sistemas-biometricos.html

GALBALLY, Javier, *et al.* On the Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks [en línea]. Trabajo de grado para optar por el titulo de Ingeniero Informático. Universidad Autónoma de Madrid, 2009. [Consultado 30 de marzo 2020]. Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.206.1024&rep=rep1&type=pdf

GALBALLY, Javier; FIERREZ, Julián y ORTEGA, Javier. Análisis temporal de vulnerabilidades de los sistemas basados en huella dactilar [en línea]. Universidad Autónoma de Madrid, 2009. [Consultado 30 de marzo 2020]. Disponible en: http://atvs.ii.uam.es/atvs/files/2010_JRBP_Galbally.pdf

GARTNER INC. Gartner Magic Quadrant for Access Management [en línea]. Okta Named a Leader for the 4th Consecutive Year. [Consultado 9 de diciembre 2020]. Disponible en: https://www.okta.com/resources/access-management-leader-gartner-magic-quadrant/

GOMEZ RAMIREZ, Diana y GIRALDO GIRALDO, Andrea. Estado del arte de la seguridad en sistemas biométricos [en línea]. Proyecto de Grado Monografía para Optar por el Título de Especialista en Seguridad Informática. Bogotá (Colombia): Universidad Nacional Abierta y a Distancia – UNAD, 2017. [Consultado 28 de marzo 2020]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14348/1/52752700.pdf

GONZALÉZ, Juan Carlos; CONTRERAS, Walter y YAÑEZ, Carlos. Tecnologías Biométricas aplicadas a la seguridad en las organizaciones [en línea]. Lima (Perú): Universidad Nacional Mayor de San Marcos. 2016. [Consultado 28 de marzo 2020]. Disponible en: https://revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/view/3336/2765

GRUPO NOVELEC. ¿Cómo funciona un sensor biométrico? [blog]. España. [Consultado 17 de mayo 2020]. Disponible en: https://blog.gruponovelec.com/redes-vdi/como-funciona-sensor-biometrico/

GUAMAN POMA, Cindy. Universidad Técnica de Machala. Facultad de Ciencias Empresariales. Auditoría Informática De La Seguridad Física Y Lógica De Las Computadoras Del Centro De Educación Continua De La Utmach. Ecuador. 2019. [Consultado: 30 de marzo de 2020]. Disponible en: http://repositorio.utmachala.edu.ec/bitstream/48000/14931/1/E-11255_GUAMAN%20POMA%20CINDY%20ABIGAIL.pdf

GUTIERRES RICARDO, Jorge. Estudio de factibilidad para el control de acceso biométrico, en una empresa empleando lectores de huella digital [en línea]. Trabajo de grado para optar por el titulo de Especialista en gerencia de proyectos. Universidad de la Salle, 2007. [Consultado 30 de marzo 2020]. Disponible en: https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1017&context=esp_gerencia_proyectos

HADID, Abdenour. Face Biometrics Under Spoofing Attacks: Vulnerabilities, Countermeasures, Open Issues, and Research Directions [en línea]. IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, 2014. [Consultado 17 de mayo 2020]. Disponible en: https://www.researchgate.net/publication/286732400_Face_Biometrics_Under_

Spoofing_Attacks_Vulnerabilities_Countermeasures_Open_Issues_and_Research_Directions/citation/download

HERNANDEZ PAZ, Carlos. Estudio del rendimiento biométrico de dispositivos de huella dactilar. Análisis de la influencia del tamaño de la muestra [en línea]. Grado Ingeniería electrónica Industrial. Universidad Carlos III de Madrid, 2015. [Consultado 30 de marzo 2020].

IBM. Las contraseñas son el pasado: los jóvenes prefieren usar la huella dactilar, citado por EL MUNDO España. Madrid: 2018. [Consulta 17 de mayo 2020]. Disponible en: https://www.elmundo.es/tecnologia/2018/01/29/5a6f0791e2704eee408b4600.html

INCENCIO PIÑEIRO, Grettel. Sistema informático para la evaluación de atributos de calidad en componentes biométricos. [en línea]. Cuba: Universidad de Granma, 2014. Nro 8. [Consultado 2 de mayo 2020]. Disponible en: https://www.3ciencias.com/wp-content/uploads/2014/03/SISTEMA-INFORMÁTICO-PARA-LA-EVALUACIÓN-DE-ATRIBUTOS-DE-CALIDAD-EN-COMPONENTES-BIOMÉTRICOS.pdf

INSTITUTO NACIONAL DE CIBERSEGURIDAD. Una guía de aproximación para el empresario. En: Tecnologías biométricas aplicadas a la ciberseguridad [sitio web]. Madrid: Gobierno de España. Ministerio de Energía, Turismo y Agenda Digital. 2016. [Consulta 1 de mayo 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. 19795-1:2006 Evaluación de desempeño biométrico y reporte [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/41447.html

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. 19795-2:2007 Metodologías de pruebas y escenario de evaluación [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/41448.html

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. 19795-3:2007 Pruebas conforme las diferentes modalidades de sistemas biométricos [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/41449.html

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. 19795-4:2007 Pruebas de rendimiento en interoperabilidad [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/46329.html

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. 19795-5:2007 Control de acceso y esquema de calificación [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/51768.html

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. 30107-1:2016 Biometric presentation attack detection — Part 1: Framework [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/53227.htm

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. 30107-3:2016 Biometric presentation attack detection — Part 3: Testing and reporting [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/51768.html

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 18013-3: 2017 - Especificaciones formato bloque de seguridad [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/70486.html

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 19785-4 2010 Especificaciones formato bloque de seguridad [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/50860.html

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC JTC 1/SC 17 Cards and security devices for personal identification [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/committee/45144/x/catalogue/p/0/u/1/w/0/d/0

ISO/IEC. Information security — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework [en línea]. ISO/IEC 19989-1. 2020. [Consultado 9 de diciembre 2020]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:19989:-1:ed-1:v1:en

ISO/IEC. Information security — Criteria and methodology for security evaluation of biometric systems — Part 2: Biometric recognition performance [en línea]. ISO/IEC 19989-2:2020. [Consultado 9 de diciembre 2020]. Disponible en: https://www.iso.org/standard/72403.html

ISO/IEC. Information security — Criteria and methodology for security evaluation of biometric systems — Part 3: Presentation attack detection [en línea]. ISO/IEC 19989-3:2020. [Consultado 9 de diciembre 2020]. Disponible en: https://www.iso.org/standard/73721.html

ISO/IEC. Information technology - Security techniques - Identity management and privacy technologies [sitio web]. ISO/IEC JTC 1/SC 27/WG 5, Alemania. [Consultado 9 de diciembre 2020]. Disponible en:

https://www.din.de/resource/blob/78926/97764df63cb1d7efa02a351c4f3b7b8e/sc27wg5-sd4-data.pdf

ISO/IEC. Information technology — Security techniques — Biometric information protection [en línea]. ISO/IEC 24745:2011. 2011. [Consultado 9 de diciembre 2020]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:24745:ed-1:v1:en

ISO/IEC. Standards Application against Advanced Cybersecurity Attacks [sitio web]. China, 2018. [Consultado 9 de diciembre 2020]. Disponible en: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180828/Documents/Jinghua%20Min.pdf

LANZ, Leonel. Que es la ciberseguridad. [sitio web]. España: OpenWebinars. [Consultado 01 mayo de 2020]. Disponible en: https://openwebinars.net/blog/que-es-la-ciberseguridad/

LINNARTZ, Jean-Paul y TUYLS, Pim. New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates [en línea]. Amsterdam (Holanda): Eindhoven University of Technology, Junio 2003. [Consultado 1 de mayo de 2020] Disponible en: https://www.researchgate.net/publication/221597796_New_Shielding_Functions_to_Enhance_Privacy_and_Prevent_Misuse_of_Biometric_Templates

LOVISS, Giulio, *et al.* Mobile Biometrics in Financial Services: A Five Factor Framework [en línea]. Estados Unidos de América: Universidad de Oxford. [Consultado 17 de mayo 2020]. Disponible en: http://www.cs.ox.ac.uk/files/9113/Mobile%20Biometrics%20in%20Financial%20Services.pdf

LUCIO, Cristina. El extraño caso de la familia sin huellas dactilares. En: EL MUNDO [sitio web]. Madrid. Serie “Estudi del ADN”. [Consulta 28 de abril 2020]. Disponible en: https://www.elmundo.es/elmundosalud/2011/08/04/pielsana/1312482983.html

MAYA VARGAS, Adriana. Sistema biométrico de reconocimiento de huella dactilar en control de acceso de entrada y salida. Sistema biométrico de huella dactilar 1 [en línea]. Bogotá (Colombia): Universidad Militar Nueva Granada, 2013. [Consultado 30 de marzo 2020]. Disponible: https://repository.unimilitar.edu.co/bitstream/handle/10654/11168/MayaVargasAdriana2013.pdf?sequence=1&isAllowed=y

MEDINA, Matias. ¿Qué es la biometría?. [sitio web]. [Consultado 27 de abril 2020]. Disponible en: https://www.mejoresvpn.pro/que-es-la-biometria/

MORAES, Alexandre Fernandes de. Método para avaliação da tecnologia biométrica na segurança de aeroportos [en línea]. Sao Paulo (Brasil): Universidade de São Paulo, marzo 2006. [Consultado 02 de mayo 2020]. Disponible en: https://repositorio.usp.br/item/001516079

MORALES MORENO, Aythami. Investigación reproducible: uso de la plataforma BEAT para la evaluación tecnológica de algoritmos de reconocimiento biométrico [en línea]. Trabajo fin de grado para optar por el título de Electrónica. Universidad Autónoma de Madrid, 2016. [Consultado 3 de mayo 2020]. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/674163/Daza_Garcia_Roberto_tfg.pdf?sequence=1&isAllowed=y

MORALES, Aythami, *et al.* Keystroke Biometrics Ongoing Competition [en línea]. 2016. [Consultado 17 de mayo 2020]. Disponible en: https://www.idiap.ch/~aanjos/papers/ieee-access-2016.pdf

N. Tekampe (TUViT), A. Merle, (CEA), J. Bringer (Mor- pho), M. Gomez-Barrero (UAM), J. Fierrez (UAM), J. Galbally (UAM). Biometrics Evaluation and Testing. [En línea]. beat-eu.org/, 2011. [Recuperado en 17 de octubre 2020]. Disponible en: https://www.beat-eu.org/project/deliverables-public/d6-5-toward-common-criteria-evaluations-of-biometric-systems

NACIONES UNIDAS. Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales [en línea], A/RES//45/95, 1990, 1 p. [Consultado: 3 de diciembre de 2020]. Disponible en: https://www.un.org/es/documents/ag/res/45/list45.htm

NARDI, Joel, *et al*. Análisis de Riesgos, vulnerabilidades y propuestas de auditoría sobre sistemas de voto electrónico [en línea]. Rosario (Argentina): Universidad Tecnológica Nacional, noviembre 2017. [Consultado 15 de abril 2020]. Disponible en: https://www.researchgate.net/publication/321183010_Analisis_de_Riesgos_Vulnerabilidades_y_Propuestas_de_Auditoria_sobre_Sistemas_de_Voto_Electronico

OCAÑA DIEZ DE LA TORRE, Manuel. Algoritmos de Matching entre huellas dactilares [en línea]. Trabajo de grado para optar por el título de Ingeniería electrónica y automática industrial. Universidad Politécnica de Madrid, 2017. 100 p. [Consultado 17 de mayo 2020]. Disponible en: http://oa.upm.es/47958/1/TFG_MANUEL_OCANA_DIEZ_DE_LA_TORRE.pdf

ORTEGA GARCIA, Javier. Biometría y seguridad. Madrid: Fundación Rogelio Segovia para el desarrollo de las Telecomunicaciones, 2008. 59 p. ISBN 978-84-7402-350-3.

PARADA SOLÓRZANO, Carlos. Propuesta de Metodología para implementar Token biométrico en la consulta de Clientes de las Compañías de Telecomunicaciones en la Policía Nacional de Colombia [en línea]. Titulo para optar como Especialización en Seguridad Informática. Universidad Piloto de Colombia, 2013. [Consultado: 26 de abril de 2020]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2611/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

PARLAMENTO EUROPEO NEWS. Data protection reform - Parliament approves new rules fit for the digital era 2016. En: News Parlamento Europeo [sitio web]. Reino Unido. [Consulta 4 de diciembre 2020]. Disponible en: https://www.europarl.europa.eu/news/en/press-room/20160407IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era

PARLAMENTO EUROPEOY DEL CONSEJO. Directiva 95/46/CE [en línea]. Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, 1995. 1 p. [Consultado: 3 de diciembre de 2020]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

PETROVSKA, Dijana y CHOLLET, Gerard. Biometric Reference Systems and Performance Evaluation. Estados Unidos de América: Springer, 2009. 389 p. ISBN 978-1-84800-292-0

RIFA, Helena y SIERRA, Jordy. Las cuatro brechas de la seguridad de la biometría. En: Cuadernos de seguridad [sitio web]. Madrid: Universitat Oberta de Catalunya (UOC). [Consulta 28 de Abril 2020]. Disponible en: https://cuadernosdeseguridad.com/2019/12/tecnologia-biometrica-expertos-uoc/

SHIMANUKI, Mario y ZANINI, Angelo. Vulnerabilidades em Sistemas Biométricos Baseados em Impresso˜es Digitais [en línea]. Brasil: Instituto Tecnológico de Aeronáutica. [Consultado 28 de abril 2020]. Disponible en: https://www.sige.ita.br/anais/VIIISIGE/GE/GE055.pdf

TECHNAVIO. Global Biometric PoS Terminals Market 2017-2021. En: Technavio [sitio web]. Reino Unido. [Consulta 18 de mayo 2020]. Disponible en: https://www.technavio.com/report/global-computing-devices-global-biometric-pos-market?tnplus

THALES Group. Biometría para identificación y autenticación [sitio web]. Francia. [Consulta 4 de diciembre 2020]. Disponible en: https://www.thalesgroup.com/es/countries/americas/latin-america/dis/gobierno/inspiracion/biometria

TRUJILLO TELLEZ, Fernando. Mitigación de riesgos. [sitio web]. Colombia. [Consultado 01 de mayo 2020]. Disponible en: http://riesgosyplanesdecontingencia.blogspot.com/2016/09/mitigacion-de-riesgos.html

ViewPost. La autenticación biométrica se impone entre los más jóvenes, citado por COMPUTERWORLD. Madrid: 2018. [Consulta 18 de mayo 2020]. Disponible en: https://cso.computerworld.es/seguridad-movil/la-autenticacion-biometrica-se-impone-entre-los-mas-jovenes

WADHWANI, Preeti y GANKAR, Saloni. Biometrics Market Size By Application. En: Global Market Insights [sitio web]. USA. [Consulta 18 de mayo 2020]. Disponible en: https://www.gminsights.com/industry-analysis/biometrics-market

WAYMAN, James. Biometric Evaluation Methodology Common Criteria Common Methodology for Information Technology [en línea]. 2002. [Consultado 01 de Abril 2020]. Disponible en: https://www.semanticscholar.org/paper/Biometric-Evaluation-Methodology-Common-Criteria-[-Stuart-Australia/e96c1dabba7775c9d029319ec2a769e59cf7d152#citing-papers

YOSHIDA, H. The overview of SC 27/WG 2 and lightweight cryptography [sitio web]. [Consulta 11 de diciembre 2020]. Disponible en: https://www.il-pib.pl/images/stories/FSC/pdf/7_Dr-Hirotaka-Yoshida_The-overview-of-SC-27WG-2-and-lightweight-cryptography_17092020.pdf

ZURITA BAJAÑA, Jhonn. Nivel de eficiencia de los lectores biométricos de los departamentos del Gad Municipal del Canton Baba [en línea]. Trabajo para obtener el título de Ingeniero de Sistemas. Ecuador: Universidad Técnica de Babahoyo, 2019. [Consultado 6 de abril 2020]. Disponible en: http://dspace.utb.edu.ec/bitstream/handle/49000/5526/-E-UTB-FAFI-SIST-000129.pdf?sequence=1&isAllowed=y

Estructura del documento para la estructura del Resumen Analítica Especializado -RAE

1. Información General	
Tema:	Investigación en referencia a los sistemas biométricos dactilares y con ello, sus vulnerabilidades ante ataques tipo Timing y Hill-Climbing considerando los sistemas NFIS y Match-On-Card que son objeto de investigación.
Titulo:	Análisis de vulnerabilidades en sistemas biométricos dactilares en referencia a los ataques Timing y Hill-Climbing
Autor:	Carlos Andrés Campos Leguízamo
Fuente bibliográfica:	Se referencia 73 fuentes bibliográficas, de ellas algunas que mencionan la temática principal: A. MORALES, J. FIERREZ, M. GOMEZ-BARRERO, J. ORTEGA-GARCIA, R. DAZA, J.V. MONACO, J. MONTALVÃO, J. CANUTO, A. GEORGE, "KBOC: Keystroke Biometrics OnGoing Competition", Proc. 8th IEEE International Conference on Biometrics: Theory, Applications, and Systems, Buffalo, USA, pp. 1-6, 2016. Disponible en: https://sites.google.com/site/btas16kboc/home CNIL - COMISSION NATIONALE DE l'INFORMATIQUE ET DES LIBERTÉS. Act Nº78-17 6 de enero de 1978. On Information Technology, Data Files and Civil Liberties [en línea]. Derecho y libertades informáticas – República de Francia, 1978. 45 p. [Consultado 3 de diciembre de 2020]. Disponible en: https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf HADID, Abdenour. Face Biometrics Under Spoofing Attacks: Vulnerabilities, Countermeasures, Open Issues, and Research Directions [en línea]. IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, 2014. [Consultado 17 de mayo 2020]. Disponible en: https://www.researchgate.net/publication/286732400_Face_Biometrics_Under_Spoofing_Attacks_Vulnerabilities_Countermeasures_Open_Issues_and_Research_Directions/citation/download INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 18013-3: 2017 - Especificaciones formato bloque de seguridad [sitio web]. Ginebra, Suiza. [Consulta 4 de diciembre 2020]. Disponible en: https://www.iso.org/standard/70486.html
Año:	2021
Resumen:	Por medio del documento realizado se identificó las características, componentes tecnológicos y soluciones que brinda los sistemas biométricos dactilares en diferentes entornos de negocio, entre otros, los implementados con el fin de adoptar lo establecido en la norma ISO27001:2013 (dominio de Seguridad física – objetivo áreas seguras – control físico de entradas) en soluciones orientadas a sistemas de votación electrónicos y en Organizaciones para procesos de autenticación y legitimidad. Con lo anterior, se realizó una validación de las vulnerabilidades respecto a los tipos de ataques Timing y Hill-climbing, considerando indicadores como EER (Coeficiente de eficiencia energética), FAR (False Acceptance Rate) y DET (Detection Error Tradeoff), en referencia a los sistemas NFIS y Match on Card, con base a los parámetros BEAT (Biometrics

	Evaluation and Testing) y KBOC (Keystroke Biometrics OnGoing Competition).
Palabras clave:	Ciberseguridad, vulnerabilidad, prueba de concepto (Poc), biométrico, mitigación, sensor, buenas prácticas.
Contenidos:	Introducción Definición del problema Justificación Objetivos Objetivo general Objetivos específicos Marco referencial Marco teórico Marco conceptual Marco legal Desarrollo de objetivos Desarrollo de objetivo 1 Desarollo de objetivo 2 Desarollo de objetivo 3 Desarollo de objetivo 4 Conclusiones Recomendaciones Trabajo a futuro Bibliografía

2. Descripción del problema de investigación

Los ataques tipo Timing en los sistemas biométricos consisten en el éxito de obtener una etiqueta de un paquete de datos válida por parte del atacante. Por medio del envío de mensajes, se genera comparaciones a nivel de Bytes, permitiendo al atacante medir los tiempos de respuesta en un servidor que revela su clave secreta permitiendo accesos no autorizados. Los ataques tipo Hill-climbing, fundamentan su acción en patrones sintéticos que elevan las puntuaciones sucesivas conforme los parámetros evaluados.

3. Objetivos

General:

Identificar las vulnerabilidades de los sistemas biométricos de huella digital en los ataques tipo Timing y Hill-climbing, analizando los parámetros establecidos por estándares internacionales que busquen la mitigación de posibles riesgos.

Específicos:

Describir el sistema biométrico de huella digital, con ello sus características, componentes Software – Hardware, tecnologías y aplicabilidad.

Considerar las vulnerabilidades relacionadas al sistema biométrico de huella digital respecto a ataques Timing y Hill-climbing, analizando indicadores como EER (Equal Error Rate), FAR (False Acceptance Rate) y DET (Detection Error Tradeoff).

Generar un análisis de los sistemas NFIS y Match On Card con base en parámetros BEAT (Biometrics Evaluation and Testing) y KBOC (Keystroke Biometrics OnGoing Competition).

Proponer parámetros, recomendaciones y metodologías conforme buenas prácticas y criterios de elección (modelo Gartner) para las organizaciones en cuánto a dispositivos biométricos dactilares.

4. Metodología

Se establece cuatro aspectos principales con el fin de identificar, analizar y destacar aspectos importantes en relación a los tipos de ataque Timing y Hill-Climbing que buscan vulnerar los sistemas biométricos dactilares:

Los sistema biométrico de huella digital, con ello sus características, componentes Software – Hardware, tecnologías y aplicabilidad.

Vulnerabilidades relacionadas al sistema biométrico de huella digital respecto a ataques Timing y Hill-climbing, analizando indicadores como EER (Equal Error Rate), FAR (False Acceptance Rate) y DET (Detection Error Tradeoff).

Análisis de los sistemas NFIS y Match On Card con base en parámetros BEAT (Biometrics Evaluation and Testing) y KBOC (Keystroke Biometrics OnGoing Competition).

Parámetros, recomendaciones y metodologías conforme buenas prácticas y criterios de elección (modelo Gartner) para las organizaciones en cuánto a dispositivos biométricos dactilares.

5. Referentes teóricos

Se consulta diferentes fuentes considerando importante pruebas de laboratorio realizadas, con fines de análisis cualitativo y cuantitativo en relación a los ataques objeto de estudio en sistemas biométricos dactilares. Se toma como referencia principalmente la ISO (Organización Internacional de Normalización), para relacionar estándares y normativas directamente relacionados a la seguridad de los sistemas biométricos dactilares.

6. Referentes conceptuales

Se toma como referencia conocimientos en referencia al sistema de biometría dactilar, su estructura lógica y fisica, estudio del comportamiento y vector de ataque de las vulnerabilidades objeto de estudio, así como también pruebas de concepto realizadas y articuladas con estándares internacionales.

7. Resultados

Los sistemas biométricos dactilares, deben ser verificados, analizados y puestos a prueba por medio de pruebas de concepto (POC), estándares, recomendaciones, entre otros. Los anteriores procesos deben considerarse imprescinbibles, pues en escenarios de acceso a sistemas de información que implican un grado de criticidad a nivel gobierno, sector privado y en las personas naturales, cualquier tipo de error o ataque informático, como los descritos en la presente monografía, puede materializar riesgos catastróficos generando afectaciones incalculables.

A nivel normativo y de disposición legal, a considerar: como referente de carácter internacional, se tiene la ley de protección de datos francesa de 1978 titulada “ley de tecnología de la información, archivos y libertades civiles”, que establece requisitos particulares para con el tratamiento de los datos biométricos; así mismo, el convenio para la protección de las personas con respecto al tratamiento automatizado de los datos personalea, del año 1981, la Directiva europea sobre la protección de las personas con respecto al tratamiento de los datos personales y la libre circulación de estos datos, del año 1995, la Resolución de las Naciones Unidas del 14 de diciembre de 1990, y por último, el proyecto Reglamento General de Protección de Datos, adoptado por el parlamento europeo, que establece disposiciones que son relativas a los datos personales y son viables para adoptar a los sitemas biométricos dactilares.

Así mismo, es importante considerar el cuadrante mágico de Gartner en su apartado Access Managment, que se relaciona directamente con las consideraciones en los sistemas biométricos; en dicho cuadrante, se presenta el resultado de un análisis de funcionalidades, tecnologías y tendencias de uso, brindando orientación hacía un proveedor teniendo implícitos aspectos en cuánto a requisitos básicos, metodologías y precios comerciales.

8. Conclusiones

Reconociendo las características y estructuras de los sistemas biométricos dactilares, así mismo, los procesos a nivel sensorial, extracción de características, comparador, y con ello, procesos implícitos, se identificó y analizó los aspectos relevantes a considerar relacionados a vulnerabilidades en el sistema que afectan la integridad, confidencialidad y disponibilidad, teniendo en cuenta la información directamente relacionada en cuánto a protección de datos personales.

Se identificó y analizó a detalle los ataques tipo Timing y Hill-climbing en los sistemas biométricos dactilares, reconociendo las metodologías de ataque en referencia al análisis del tiempo y los riesgos materializados, generando un análisis puntual y particular a los indicadores de compromiso implícitos en los eventos de penetración, entre ellos, la tasa de falso rechazo FR, la tasa falsa de aceptación FAR y la tasa de compensación de errores DET; los anteriores índices, permiten reconocer los aspectos a fortalecer y considerar en el proceso de implementación de sistemas biométricos dactilares en un ambiente de producción.