Análisis de vulnerabilidades en sistemas biométricos dactilares en referencia a los ataques Timing y Hill-Climbing

Carlos Andrés Campos Leguízamo
Especialización en Seguridad Informática
Universidad Nacional Abierta y a Distancia, Colombia
carloscl06@gmail.com

Resumen – Por medio del documento realizado, se identificó las características, componentes tecnológicos y soluciones que brindan los sistemas biométricos dactilares en diferentes entornos de negocio. Con lo anterior, se realizó una investigación 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).

Por medio de lo desarrollado, se propone parámetros, recomendaciones, metodologías, normativas y estándares que llevan a considerar, junto a la implementación de está tecnología, buenas prácticas, lo anterior, bajo criterios de elección de sistemas considerando pruebas de concepto (PoC). Adicionalmente, se propone controles de mitigación de riesgos posterior a las vulnerabilidades identificadas, las cuales, se logran obtener por resultados con base en desarrollos experimentales ejecutados por autores investigados, que involucraron diferentes escenarios y condiciones.

Palabras clave— biometría estática, vulnerabilidades, estándar, mitigación de riesgos.

I. MÉTODOS

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 y esquematizados (Ver Figura 1), para el tratamiento de la información, involucran una parte del sistema que puede llegar a ser vulnerable y afectada por un atacante.

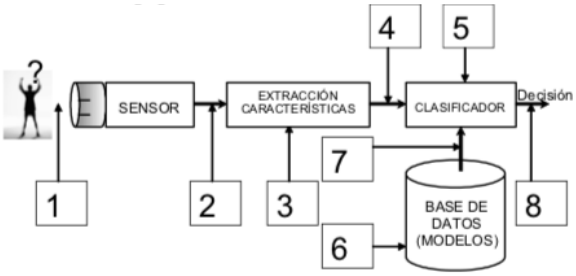

Figura 1. Puntos vulnerables sistema reconocimiento biométrico.

Las principales vulnerabilidades a destacar: en el proceso de transmisión entre el sensor y el extractor de características, se puede presentar ataques de inyección de datos biométricos, almacenados previamente en repositorios remotos que hacen uso de internet; además, el sensor puede presentar vulnerabilidades conforme biometría intrusiva, que consiste en burlar por medio de software e imágenes sintéticas, la identidad de un usuario. En el extractor de

características, un atacante puede vulnerar el sistema para alojar valores escogidos y convenientes, presentándose el escenario en el que se inserta un programa que reemplaza un extractor legítimo. En el proceso de transmisión de las características, se puede presentar un ataque que busca reemplazar las muestras originales por muestras falsas. Por último, en el proceso de decisión, se presentan ataques que omiten todo el sistema biométrico; alli, es posible generar cambios de decisión afectando de manera puntual el resultado, de esta manera, se materializa 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.

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 en el mercado que crece como solución de seguridad a organizaciones en ecosistemas disruptivos. La aplicabilidad de los sistemas biométricos dactilares, involucra diferentes dispositivos en los cuales se genera la toma de muestras dactilares, los casos de uso, entre otros, sector bancario, *retail*, sector transaccional, aplicaciones.

Los ataques de tipo *Hill-climbing*, consisten en generar una modificación sucesiva a un patrón específico de características; las modificaciones involucran una alteración estructurada 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 de acuerdo al objetivo:

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.

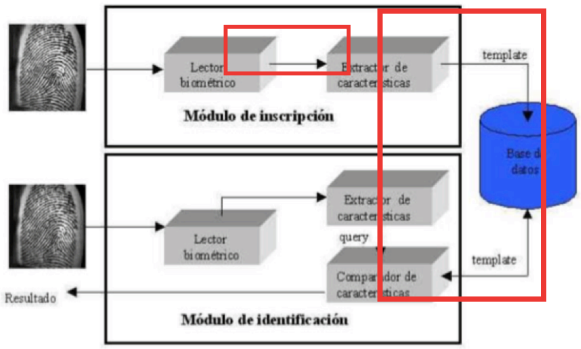

Figura 2. Puntos vulnerables ataque Hill - Climbing sistema reconocimiento biométrico.

Los ataques de tipo Timming-attack, consisten en obtener los tiempos de respuesta del sistema dactilar tanto para patrones de huella legítimos como impostores. Por medio de la experimentación, es posible deducir que existe una relación directa entre tiempo y puntuación, siendo altamente viable un ataque *Hill-climbing,* logrando materializar el riesgo existente en los sistemas afectando la confidencialidad e integridad de la información.

Considerando los tipos de ataques expuestos, se ha establecido un propósito, para el desarrollo de métodos estandarizados de evaluación y pruebas a sistemas biométricos dactilares, lo anterior, con el fin de obtener resultados en referencia a la protección de la integridad, confidencialidad y disponibilidad de la información.

Inicialmente, hablamos de BEAT (Biometrics Evaluation and Testing), que es considerada una guía de evaluación de diferentes componentes y en general, de sistemas biométricos de acuerdo a criterios comunes establecidos. Proporciona cinco aspectos en los cuales, se establece el proceso de evaluación para los sistemas biométricos, estos a continuación dados a conocer:

1. 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.

2. Como segundo aspecto de evaluación, se presenta los requisitos de desarrollo, proporcionando como referencia el tomar funcionalidades de los sistemas biométricos por medio de subsistemas y módulos.

3. Tercer aspecto de evaluación, los repositorios y documentación, que permiten establecer una preparación propia para la evaluación TOE, reconociendo las funcionalidades específicas del sistema biométrico a evaluar, definiendo requisitos para su uso, conforme los roles establecidos y el entorno de aplicabilidad.

4. 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 en referencia a los criterios a evaluar, permitiendo reconocer, entre otros aspectos, aquellos propios de ciberataques y su detección por medio de mecanismos de relación por firmas.

5. 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 hincapié 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 predecible.

Otro método de evaluación por su parte, es KBOC (Keystroke Biometrics OnGoing Competition), que permite establecer la autenticación de personas por medio de la biometría de pulsación de teclas. Este tipo de competencia ha sido desarrollado tomando como referencia el marco de evaluación BEAT, mencionado con anterioridad, involucrando un *benchmark* que contiene registros de pulsaciones de teclas de gran tamaño tanto para usuarios legítimos como para impostores.

Keystroke Biometrics OnGoing Competition ha sido un referente de evaluación biométrica dinámica, esto es demostrado por investigadores de la Universidad Autónoma de Madrid, quienes tomaron como referencia secuencias de pulsaciones de teclas de usuarios, obteniendo resultados que arrojan variables como el EER (Equal Error Rate) predescibles ante diferentes tipos de comportamiento, y esto, articulándolo ante modelos de evaluación como BEAT.

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 el presente documento, pueden materializar riesgos catastróficos generando afectaciones incalculables.

En referencia a disposiciones normativas, 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 referentes de carácter internacional, se tiene la Ley de Protección de Datos Francesa del año 1978 titulada “Ley de Tecnología de la Información, Archivos y Libertades Civiles” , que establece requisitos particulares en 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, 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, 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.

Igualmente a resaltar, estándares de la ISO (International Organization for Standardization), generados por diferentes subcomités, entre ellos:

- Sub-Comité 17 (SC17), en el cual se involucra marcos de trabajo enfocados en tarjetas de identificación, involucrando tecnologías biométricas en diferentes sectores: bancarios, comercio, telecomunicaciones y transporte.
- Subcomité 27 (SC27), en el cual 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.
- Sub-Comité 37 (SC37), en el cual se establece la importancia de la implementación de técnicas que busquen disminuir los riesgos con base en la autenticación del usuario.

II. RESULTADOS Y DISCUSIÓN

Además de los tipos de biometría existentes, existen coeficientes con el fin de generar procesos de evaluación (Ver Figura 3): FNMR (*False Non-Match Rate*), FMR (*False Match Rate*), FRR (*False Reject Rate*), FAR (*False Accept Rate*), EER (*Error Equal Rate*).

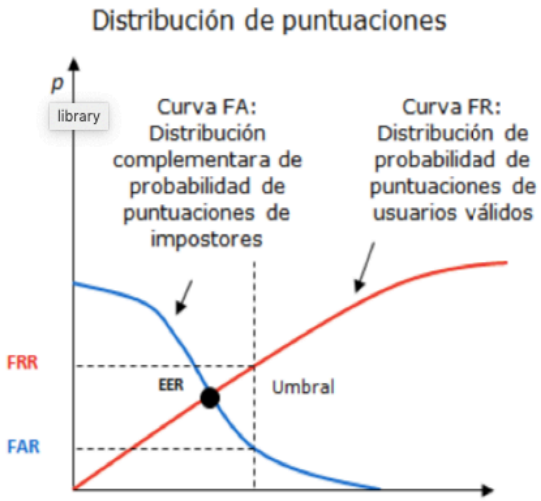

Figura 3. Puntos vulnerables ataque Hill - Climbing sistema reconocimiento biométrico.

La investigación realizada, permite generar diferentes procesos experimentales en dos sistemas de referencia: NFIS de la NIST, cuyo sistema de biometría dactilar esta alineado al sistema estándar, y por su parte, el sistema Match-On-Card, usualmente aplicado en plásticos de tarjetas de crédito que por medio de un chip, guardan información dactilar.

Los procesos experimentrales permiten reconocer el nivel de coincidencia conforme la puntuación de identidad y el tiempo de respuesta del sistema. Es posible identificar que para puntuaciones altas (línea color naranja), el sistema NFIS no tiene una respuesta predecible, por el contrario, para puntuaciones de identidad pequeñas (línea color negro), el sistema da a conocer una respuesta predecible (Ver Figura 4.)

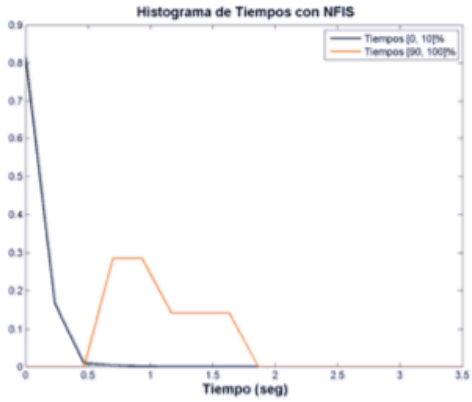

Figura 4. Evaluación experimental Timing Attack NFIS.

Por su parte, en el sistema MoC es posible identificar que para puntuaciones altas (línea color naranja), el sistema tiene una respuesta predecible, por el contrario, para puntuaciones de identidad pequeñas (línea color negro), el sistema no da a conocer una respuesta predecible (Ver Figura 5.)

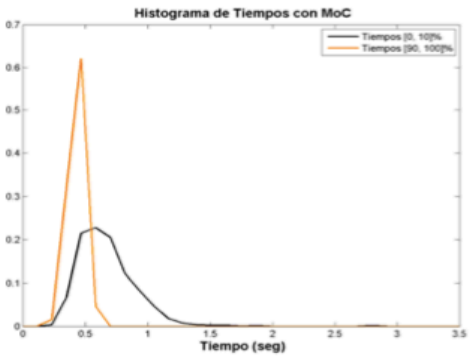

Figura 5. Evaluación experimental Timing Attack MoC.

En referencia al tipo de ataque Hill-Climbing, se toma como referencia nuevamente los sitemas NFIS y MoC. Conforme indicadores como el falso rechazo (FR) y la falsa aceptación (FA), es posible observar (Ver Figura 6), 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 (Ver Figura 7), 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, no obstante, con un porcentaje de error mayor.

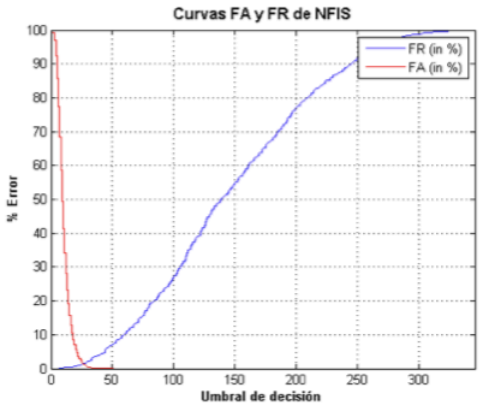

Figura 6. Evaluación experimental Hill Climbing NFIS.

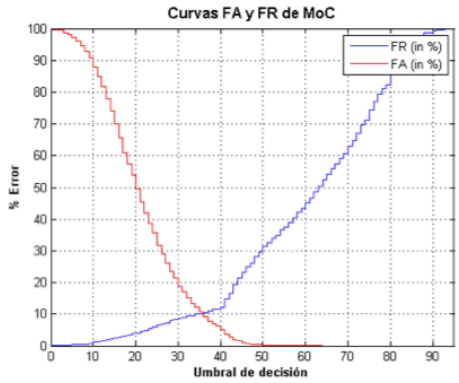

Figura 7. Evaluación experimental Hill Climbing MoC.

De acuerdo a los valores analizados con anterioridad, se realiza una evaluación de los sistemas de acuerdo al parámetro DET (Detection Error Tradeoff), 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% (Ver Figura 8).

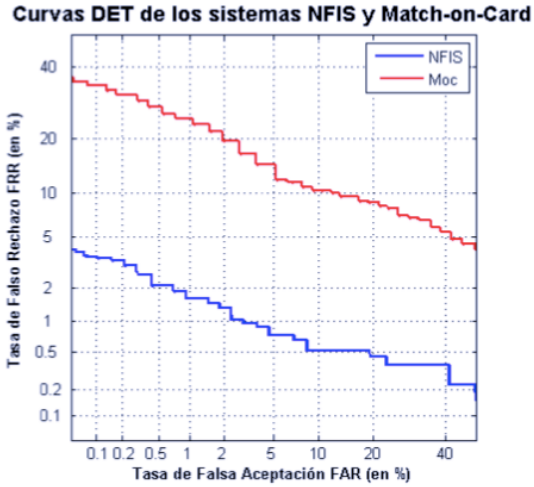

Figura 8. DET (Detection Error Tradeoff),

DET permite identificar que tan restrictivo es considerado el sistema, de manera que a menor tasa de falsa aceptación (verdadero positivo) mayor es la probabilidad del falso rechazo (falso positivo).

III. 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.

AGRADECIMIENTO

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.

REFERENCIAS

[1] 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

[2] 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

[3] 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

[4] 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

[5] 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

[6] 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

[7] 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

[8] CNIL - COMISSION NATIONALE DE I’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

[9] 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.

[10] 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.

[11] 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.

[12] 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

[13] 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

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

[15] 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

[16] 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

[17] 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

[18] 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
[19] 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/
[20] 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
[21] 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
[22] 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/
[23] 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
[24] 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
[25] 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
[26] 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
[27] 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
[28] 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
[29] 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
[30] 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
[31] 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
[32] 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
[33] 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