INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 42-51 https://doi.org/10.33936/isrtic.v4i1.2347 | ISSN 2550-6730

Recibido: 02/04/2020
Aceptado: 15/04/2020

La importancia de la autenticación multifactor para el usuario final en un entorno financiero.

Alex Mendoza Arteaga [1] Francisco Bolaños Burgos [1] Cristhian Cedeño Sarmiento [1] Wilton Rafael Saltos Rivas [2]

[1]Universidad Espíritu Santo – Ecuador.,
[2]Universidad Técnica de Manabí – Ecuador.
alexmendoza@uees.edu.ec, fcobolanos@uees.edu.ec, cfcedeno@uees.edu.ec,
w.saltos@utm.edu.ec

RESUMEN
En la actualidad, encontrar sistemas de autenticación multifactor es común, en especial en los sitios web de las entidades financieras y las que se dedican al comercio electrónico, en el presente artículo se revisó apartados, reportes e informes para analizar la importancia de la autenticación multifactor para el usuario final en un entorno financiero. Para alcanzar este objetivo se analizan los ataques a los sistemas de autenticación, así como los métodos y su clasificación, también la forma óptima de implementar los sistemas de multifactor de autenticación considerando costo, complejidad e interacción con el usuario final. Por lo consiguiente se concluye, que el uso de los sistemas de multifactor de autentificación en los sitios web de las empresas dentro del entorno financiero, se convirtió en una necesidad para garantizar a sus clientes la seguridad de su información y evitar el robo de dinero.
Palabras-clave: Autenticación; Multifactor; doble factor; financiero.

ABSTRACT
Currently finding multifactor authentication systems is common in particular in the websites of financial institutions and those engaged in electronic commerce, in this article articles, reports and reports were reviewed to analyze the importance of multifactor authentication for the end user in a financial environment. To achieve this goal, we analyze attacks on authentication systems, as well as methods and their classification, as well as the optimal way to implement multifactor authentication systems considering cost, complexity and interaction with the end user. As a result, it is concluded that the use of multifactor authentication systems in companies' websites within the financial environment became a necessity to guarantee their clients the security of their information and avoid the theft of money.
KEYWORDS: Authentication; Multifactor; double factor; financial.

1. Introducción

Actualmente los principales ataques cibernéticos en el área financiera son los phishing y códigos maliciosos o malware, incluyendo ataques a bancas virtuales, dispositivos móviles y cajeros automáticos, información basada en las estadísticas y datos de [1], también en los informes de tendencias emitidos por [2] muestran que en el segundo trimestre del año el 46,23 % de los ataques de phishing son al sector financiero, distribuidos en los ámbitos de comercio electrónico con el 20,3 %, sistemas de pagos en línea 24,7 % y bancos con el 55,00 %, asimismo encontramos que del total de personas que han recibido ataques de malware, el 4,8 % esta relacionados con amenaza financiera. De igual manera, ESET (2016) en los datos obtenidos por sus productos en Latinoamérica muestran que los primeros lugares de ataques cibernéticos son los relacionados con malware con el 40 % y el phishing 16 %, independientemente del tipo de empresas analizadas.

Con respecto a las técnicas de ataque mencionadas, [3][4] señalan que el phishing se refiere a un ataque mediante el cual se engaña a la víctima por medio de un correo electrónico, haciéndole creer que ha sido enviado por algún banco o entidad financiera del cual es cliente, incitándolo a que, mediante mensajes , el usuario acceda a sitios web falsos, provocando que divulguen su información personal o en otros casos instalen un malware en el equipo, lo que permite al atacante espiar las comunicaciones de los sitios web que visita, obteniendo así información de las cuentas personales.

Según [5], la propagación de los fraudes a distancias, mediante el uso de plataformas tecnológicas, ha generado mayor atención en los procesos de autenticación e identificación. [6][7] mencionan que el proceso dominante en el control de acceso, es el uso de contraseñas; este proceso fue tan exitoso, que la mayoría de sitios web empezaron a usarlo y se convirtió en blanco de una enorme variedad de ataques a cuentas de correo electrónicos, sistemas bancarios, médicos y redes sociales. [8] indica que las contraseñas no son nada seguras y expresa que por más extensa y compleja que sea, los criminales cibernéticos pueden robarla tanto mediante un malware, como por medio de phishing.

Para reducir este tipo de ataques, un solo factor de autenticación no es seguro, por lo que en la actualidad la autenticación multifactor es la tendencia para asegurar que los usuarios sean legítimos[9]. El principal objetivo de este artículo es demostrar al usuario final la importancia de la autenticación multifactor para reducir el riesgo de robo de información y dinero con una revisión de seis métodos de autenticación y su clasificación.

2. Marco Teórico

Ataques Informáticos

Según [10] un ataque informático radica en aprovechar la vulnerabilidad en el hardware, en el software, e incluso en los usuarios que forman parte de un entorno informático con la finalidad de obtener un beneficio, la mayoría de veces de índole económico, causando un efecto negativo para las personas y empresas.

Los ataques informáticos más comunes al área financiera son el phishing y malware según estadística de[1][2], ESET (2015) y ESET (2016), en general para que estos ataques tengan el éxito deseado por los cibercriminales, son acompañados de otra técnica conocida como ingeniería social, que analiza el comportamiento humano para encontrar sus vulnerabilidades y llegar de esa forma a la información deseada [11][12]

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 42-51 https://doi.org/10.33936/isrtic.v4i1.2347 | ISSN 2550-6730

Códigos Maliciosos (Malware)

El malware es un término que se le da a los códigos o programas maliciosos que afectan al computador, convirtiéndose actualmente en una de las principales amenazas para los sistemas informáticos.

Con el paso del tiempo, el malware se ha vuelto cada vez más sofisticado, al punto en que varias soluciones de prevención como los sistemas antispyware y antivirus se ven superadas, lo que permite que los virus aprovechen estas ventajas de la tecnología para ser rápidos, nocivos y sutiles y engañar así a sus víctimas[11].

La ventaja que posee el malware con otras sofisticadas técnicas de ataque, es que en la mayoría de las ocasiones aprovecha la inocencia de las personas; es decir, los creadores de malware utilizan técnicas como ingeniería social para engañar y abusar de sus víctimas, aunque hay que tener en cuenta que los cibercriminales desarrollan los malware a margen de la tecnología y evolucionan de manera permanente [10].

Phishing

Hoy por hoy existen muchos métodos de atentar contra la seguridad de la información.

Dentro de las estafas cibernéticas encontramos como uno de los delitos más comunes el Phishing, delito que va acompañado de la ingeniería social para lograr su objetivo y adquirir información de forma fraudulenta [12].

[12][3][4] describen el phishing como el proceso mediante el cual el estafador se hace pasar por una empresa o persona de confianza y por medio de llamadas telefónicas o correos electrónicos intenta obtener los datos que desea. Cuando el estafador realiza estas comunicaciones, en la mayoría de los casos ha estudiado a su víctima mediante técnicas de ingeniería social.

Autenticación y Autorización

La autenticación es el mecanismo principal de un modelo estándar de seguridad, es importante diferenciar entre la autenticación y la autorización, siendo la autorización otro elemento importante en una estrategia de seguridad de la información. La autenticación prueba la identidad de un usuario, luego la autorización verifica los privilegios del usuario y que tenga los permisos correspondientes a los recursos o lugares donde se pretende acceder[13].

Multifactor de Autenticación

Actualmente, la autenticación de factor único, usuario y contraseñas, ya no se considera seguro en el mundo de Internet, especialmente en el sector financiero. Las contraseñas comunes que son en la mayoría de los casos las más usadas, como los nombres y la edad, son fácilmente descubiertas por los ataques con técnicas como diccionario y de fuerza bruta.[14] Sin tomar en cuenta que cuando los usuarios son víctimas de phishing y malware como indica [8], por más robusta y compleja que sea la contraseña son blanco fácil de los cibercriminales.

Los métodos de autenticación han evolucionado con el paso del tiempo, en la actualidad las tendencias se basan en autenticación multifactor para identificar a los usuarios de forma correcta. La técnica multifactor parte de combinar métodos de autenticación, llevándola más allá de un simple factor como un usuario y una contraseña[15][9]).

Métodos de autenticación

Para el presente artículo realizaremos una revisión de algunos métodos de autenticación, tomando en cuenta que toda forma de la misma se basa en la validación de uno de estos tres elementos: Algo que sabes, Algo que tienes, Algo que eres [15][16][17]. Algo que sabe, es un secreto que solo el usuario conoce, como una contraseña, que puede generarse en cualquier instante para el sistema de autenticación. Algo que tienes, es cualquier dispositivo físico que el usuario lo posea en el momento de la autenticación. Algo que eres es el análisis de algún rasgo físico o conducta sobre un usuario que normalmente nunca cambiará, también conocido como biometría humana [15][17].

Contraseña

El usuario y la contraseña es el método de autenticación más conocido y más utilizado en la mayoría de sitios web, se encuentra dentro del grupo del elemento algo que sabes, siendo su mayor defecto que el nivel de seguridad depende directamente del usuario final, la complejidad de la contraseña, siempre es escasa, y las contraseñas demasiado complejas conducen a los usuarios a aplicar estrategias no siempre correctas para recordarlas, como anotarlas en el teléfono celular, en un archivo de Excel en el computador y hasta en una nota pegada al monitor del ordenador, dentro de sus ventajas encontramos que es un método fácil de utilizar e implementar y de muy bajo costo [16][18][6].

One-Time Password(OTP)

Otro método del grupo del elemento algo que sabes es el OTP el cual asegura el uso de la contraseña, en efecto, con un sistema OTP el usuario posee una contraseña por un tiempo determinado y para un uso específico. Esta solución es usada en general para el proceso de autenticación de inicio para los accesos externos, los cuales se realizan mediante P/VPN[19].

Tarjeta inteligente

Pertenece al grupo del elemento algo que tiene, el uso de tarjetas inteligentes que es cada vez más frecuente, ya que suministran información específica a un usuario en distintos escenarios, como por ejemplos, en el comercio electrónico, control de acceso y en la actualidad algunos países la han incorporado como documento de identidad. Para que un sistema que utiliza tarjetas inteligentes trabaje, debe estar compuesto por dos componentes fundamentales, las tarjetas inteligentes y un dispositivo de interfaz, frecuentemente conocido como un lector. Las tarjetas inteligentes son de uso personal de los usuarios del sistema, por lo que debe ser transportada dentro de sus bienes personales[20][21][22].
Con el paso del tiempo las tarjetas inteligentes han ido evolucionando considerablemente, estas incluyen memoria que almacena la información que es pertinente a la interacción del usuario con el sistema. En un sistema de comercio electrónico, cada tarjeta inteligente puede contener el saldo de una cuenta, así como los detalles de las transacciones, en la actualidad las tarjetas inteligentes también incluyen microprocesadores, por lo cual mejora su flexibilidad, facilita el almacenamiento de los programas ejecutables y proporciona amplias funcionalidades [20][21][22].

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 42-51 https://doi.org/10.33936/isrtic.v4i1.2347 | ISSN 2550-6730

Token

Un token es otro de los métodos de autenticación del grupo del elemento algo que tiene, es un dispositivo electrónico que posee la autorización de un servicio computarizado para un usuario específico a fin de facilitar el proceso de autenticación. El token es el dispositivo de seguridad utilizado para firmar digitalmente y cifrar mensajes, es un nivel de seguridad alto, con el cual se puede acceder a servicios que demandan certificados digitales y por el cual el usuario que posee esta llave puede acceder. Este dispositivo combina las funcionalidades de una tarjeta inteligente y su lectora en un solo hardware, siendo de fácil uso y manipulación, el usuario lo puede trasladar a cualquier parte del mundo. Existe más de una clase de token, como los conocidos generadores de contraseñas dinámicas OTP y la que comúnmente denominamos tokens USB los cuales no solo permiten almacenar contraseñas y certificados, sino que también almacenan la identidad digital de la persona [23].

En conclusión y en el contexto de la autentificación electrónica, un token es un dispositivo de almacenamiento que contiene una llave secreta para ser utilizado en el proceso de autenticación, la información que posee el dispositivo es certificada por una entidad que valida la autenticidad del mismo [24].

Biometría

Biometría es la autentificación de un individuo por medio de sus características físicas: forma de su rostro, huellas dactilares, estructura y forma de su voz, patrón de iris y otras características únicas de cada ser vivo. También se puede considerar a la biometría como una ciencia que mide las propiedades físicas en los seres vivos, por lo tanto aprovechando las características únicas del cuerpo se crean los sistemas biométricos y con éstos se permite la identificación tecnológica de una persona automáticamente utilizando características físicas de sí mismo [25].
De esta manera los sistemas biométricos se caracterizan por el reconocimiento de patrones que identifican a las personas de una forma automática, a partir de su comportamiento o características físicas, excluyendo de esta a los sistemas no automáticos como los procedimientos y métodos utilizados en la medicina forense. Por lo tanto el reconocimiento biométrico consiste en almacenar, medir y comparar las características de una persona, y ya que la dimensión de la identificación biométrica es muy amplia, nos remitimos a uno de ellos: el reconocimiento facial [26][27].

Reconocimiento facial

El reconocimiento facial data del año 1871, año donde se realizó el primer intento de identificar a una persona comparando su rostro con un grupo de imágenes, más tarde en 1882, el criminólogo Alphonse Bertillon, de origen francés, usó un método que consistía en tomar medidas de todo los rastros posibles de la cara y con esto crear una base de datos de rasgos faciales, en resumidas cuentas el principio de reconocimiento facial parte en registrar las medidas de varios puntos característicos del rostro de un individuo, dado que en un rostro común se puede encontrar puntos significativos como: ojos, pupilas, boca, cejas entre otros. De manera que analizando y apoyándose en cada una de las distancias obtenidas de los puntos característicos del rostro se podía identificar caras iguales [28].
Por lo tanto, el reconocimiento facial pertenece al grupo del elemento algo que eres, el cual tiene la capacidad de reconocer a un individuo por sus características o rasgos faciales. En la actualidad existen algoritmos escritos en computadoras que se encargan de mapear los rasgos faciales de las personas y compararlas con bases de datos, realizándolo con alta precisión y con una respuesta rápida. Igualmente podemos decir que el reconocimiento facial parte de la detección del rostro, extraer las características y realizar el reconocimiento[29].
El rostro de los seres humanos nos brinda un sinnúmero de información proporcionada por rasgos característicos que ayudan a identificar y discernir de manera fácil a las personas, debido a que la cara contiene elementos que a su vez poseen sus propios rasgos característicos, como la nariz, boca, cejas,

orejas y que siempre se encuentran en las mismas posiciones dentro de la cara de cualquier ser humano, esto ayuda al desarrollo de sistemas de reconocimiento facial ya que podría comparar narices con narices, bocas con bocas y así sucesivamente hasta encontrar similitudes entre sí[30].

Huella dactilar

La autenticación por huella dactilar es otro método del grupo del elemento de algo que eres, se caracteriza por extraer particulares desde distintos sectores y ángulos de la yema del dedo y de guardarlas. Las huellas dactilares son imborrables a lo largo de la vida de un ser humano, pero en algunas situaciones, por eventos externos que producen lastimaduras y cicatrices pueden alterarlas. Se ha convertido en una de las tecnologías más empleadas y de las que se han desarrollado diferentes aplicaciones y dispositivos de bajo costo que permiten la implementación de la tecnología biométrica, como por ejemplo: en controles de accesos,control de asistencia y autenticación a sistemas computacionales.[31]

Una huella dactilar es la representación de la morfología superficial de la epidermis de un dedo, esta posee un conjunto de líneas que, en forma global, aparecen dispuestas en formas paralelas. Sin embargo, estas líneas se intersectan y a veces terminan en formas abruptas. Los puntos donde las líneas terminan o se bifurcan, se conocen como puntos característicos. Para concluir, para saber si dos huellas dactilares corresponden o no a una misma persona se realiza el procedimiento que comienza con la clasificación de la huella dactilar y se culmina con la comparación de los puntos característicos de ambas huellas.[32]

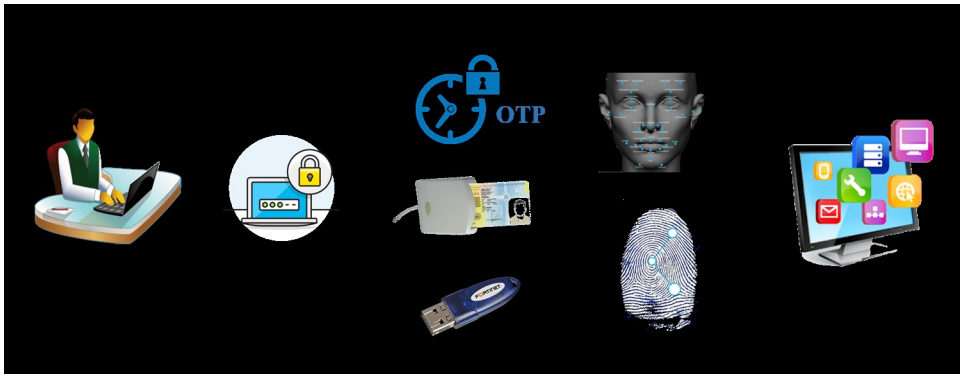

Figura 1: Factores de autenticación, según categoría.

3. Conclusiones, Limitaciones y Trabajos Futuros

Luego de la revisión de artículos, informes, foros relacionados a la autenticación, los métodos y clasificación, se puede evidenciar que la autenticación de factor simple es la que ha liderado los sistemas de autenticación en la mayoría de sitios web, usando el método de contraseña como único factor en la autentificación para identificar al usuario. Los reportes e informes de las marcas de antivirus indican alto índice de ataques mediante las técnicas conocidas como phishing y malware, evidenciando que las contraseñas son blanco fácil de los cibercriminales, especialmente en los usuarios de bancos y comercio electrónico. Otros autores afirman que la complejidad de la contraseña no garantiza que no pueda ser vulnerada, ya que en la actualidad los ataques se inclinan más a robar los datos con engaños, antes de intentar descifrar las contraseñas.

Con estas debilidades que la mayoría de empresas en el entorno financiero han encontrado, los desarrolladores e investigadores de los sistemas de autenticación luchan por implementar nuevas formas de garantizar que los usuarios no sean víctimas de fraudes cibernéticos y evitar así que su información y dinero sean robados. Actualmente la tendencia en la autenticación de usuario se basa en multifactores

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES
Vol. 4, No. 1, (Enero-Junio 2020), 42-51 https://doi.org/10.33936/isrtic.v4i1.2347 | ISSN 2550-6730

que no es más que un conjunto de factores de autenticación (figura 1), tomando en cuenta los elementos de la misma: algo que sabe, algo que tiene y algo que es, para crear sistemas de autenticación multifactor complejos, pero a su vez se busca que sea de fácil uso para el usuario final. Aunque se ha evidenciado que la contraseña, por sí sola, no es un método seguro de autenticación, los procesos de autenticación multifactor en la mayoría de los casos la sigue implementando acompañada de un segundo factor que por costos es un token o tarjeta inteligente u objeto físico que el usuario siempre lleva con él, y que pertenece a uno de los métodos del grupo del elemento algo que se tiene.

En la revisión literaria podemos encontrar que el método más seguro para garantizar la identidad de un usuario, es la biometría del grupo del elemento algo que es, este tercer elemento de la autenticación que es casi imposible de suplantar ya que se realiza la identificación mediante un rasgo físico o del comportamiento de un individuo. En el presente trabajo se analizó 2 métodos de autenticación biométrica, el reconocimiento facial y el reconocimiento por huella dactilar, pero el costo de la implementación en los sistemas de autenticación es muy elevado.

Las limitaciones de la investigación se encontraron en la aplicación del tercer grupo del elemento algo que es, ya que por el costo de aplicación y su complejidad no se evidencia su uso en los sitios web, al contrario, se utiliza en la mayoría de los casos en controles de accesos y de asistencia, sin embargo existen artículos de autenticaciones que emplean biometría pero en aplicaciones locales, por lo cual se propone realizar trabajos futuros orientados a la biometría como método de autenticación multifactor y realizar análisis técnicos de las combinaciones idóneas para generar sistemas de autenticación seguros económicos y de fácil uso para los usuarios finales.

Referencias

[1] Kasperski. *Financial cyber threats in 2014: things changed | Securelist*. 2014. URL: https://securelist.com/financial-cyber-threats-in-2014-things-changed/68720/ (visitado 05-05-2020).

[2] Kasperski y Telefonica. *Ciberamenazas Sector Financiero Q2 2016*. es-ES. 2016. URL: https://www.elevenpaths.com/es/ciberamenazas-sector-financiero-q2-2016/ (visitado 05-05-2020).

[3] Jason Hong. "The state of phishing attacks". En: *Communications of the ACM* 55.1 (2012), págs. 74-81.

[4] Jason Milletary y CERT Coordination Center. "Technical trends in phishing attacks". En: *Retrieved December* 1.2007 (2005), págs. 3-3.

[5] Luis Gerardo Gabaldón y Wílmer Pereira. "Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico". En: *Sociologias* 20 (2008), págs. 164-190.

[6] Dinei Florêncio, Cormac Herley y Baris Coskun. "Do strong web passwords accomplish anything?" En: *HotSec* 7.6 (2007), pág. 159.

[7] L. C. F. Araújo y col. "Autentificación personal por dinámica de tecleo basada en lógica difusa". En: *IEEE LATIN AMERICA TRANSACTIONS* 2.1 (2004), pág. 69.

[8] C. Alonso. *Un informático en el lado del mal*. Obtenido de http://www. elladodelmal. com/2017/04/publicada-owasp-top-ten ...

[9] Abhijit Kumar Nag y Dipankar Dasgupta. "An adaptive approach for continuous multi-factor authentication in an identity eco-system". En: *Proceedings of the 9th Annual Cyber and Information Security Research Conference*. 2014, págs. 65-68.

[10] Jorge Mieres. "Ataques informáticos: Debilidades de seguridad comúnmente explotadas". En: *ene-2009* (2009).

[11] Luis Fernando Fuentes Serrano. "Malware: una amenaza de Internet". En: (2008).

[12] Milagros Infante Montero. "Criptografía y psicología de la contraseña: generando una contraseña fuerte para diferentes servicios". En: *Apuntes de Ciencia & Sociedad* 3.1 (2013).

[13] Fatima Moumtadi y Luis Alfonso García Vázquez. "Autenticación multifactor con el uso de un sensor kinect". En: *ITECKNE: Innovación e Investigación en Ingeniería* 13.1 (2016), págs. 23-35.

[14] Fadi Aloul, Syed Zahidi y Wassim El-Hajj. "Two factor authentication using mobile phones". En: *2009 IEEE/ACS International Conference on Computer Systems and Applications*. IEEE, 2009, págs. 641-644.

[15] Hisham Al-Assam, Harin Sellahewa y Sabah Jassim. "Multi-factor biometrics for authentication: A false sense of security". En: *Proceedings of the 12th ACM Workshop on Multimedia and Security*. 2010, págs. 81-88.

[16] Mark Burnett. *Perfect password: Selection, protection, authentication*. Elsevier, 2006.

[17] Igor Ruiz-Agundez y Pablo G. Bringas. "Service authentication via electronic identification cards: voip service authentication through the DNIe". En: *2012 Annual SRII Global Conference*. IEEE, 2012, págs. 602-607.

[18] Niklas Auerbach. "Anonymous digital identity in e-government". PhD Thesis. University of Zurich, 2004.

[19] Neil Haller y col. "A one-time password system". En: *Network Working Group Request for Comments* 2289 (1998).

[20] William Reid Carlisle y col. "Smart card with multiple charge accounts and product item tables designating the account to debit". Jul. de 1997.

INFORMÁTICA Y SISTEMAS
REVISTA DE TECNOLOGÍAS DE LA INFORMÁTICA Y LAS TELECOMUNICACIONES

Vol. 4, No. 1, (Enero-Junio 2020), 42-51 https://doi.org/10.33936/isrtic.v4i1.2347 | ISSN 2550-6730

[21] Raúl Sánchez Reillo. "Mecanismos de autenticación biométrica mediante tarjeta inteligente". En: *Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingenieros de Telecomunicación* (2000).

[22] Jean-Marc Sarat. *Smart card which operates with the USB protocol*. Google Patents, jun. de 2003.

[23] Keitling Daysi Salinas Hinojosa. "TOKENS DE SEGURIDAD". En: *Revista de Información, Tecnología y Sociedad* (2013), pág. 59.

[24] William Burr, Donna Dodson y W. Polk. *Electronic authentication guideline*. Inf. téc. National Institute of Standards y Technology, 2004.

[25] Javier Areitio Bertolín y María Teresa Areitio Bertolín. "Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación". En: *Revista española de electrónica* 630 (2007), págs. 52-67.

[26] Virginia Espinosa Duró. "Evaluación de sistemas de reconocimiento biométrico". En: *Departamento de Electrónica y Automática. Escuela Universitaria Politécnica de Mataró* (2001).

[27] Ana Belén Moreno Díaz. "Reconocimiento facial automático mediante técnicas de visión tridimensional". PhD Thesis. Informatica, 2004.

[28] Maya Binetskaya. "Reconocimiento Facial en el ámbito Forense". B.S. thesis. 2013.

[29] Nicolas Lopez Perez, JJ Toro Agudelo y CIENCIAS DE LA COMPUTACION. "Técnicas de biometría basadas en patrones faciales del ser humano". PhD Thesis. Universidad Tecnológica de Pereira. Facultad de Ingenierías Eléctrica . . ., 2012.

[30] Javier Eslava Ríos. "Reconocimiento facial en tiempo real". B.S. thesis. 2013.

[31] José I. Carri y col. "Reconocimiento biométrico en aplicaciones de E-Government". En: *Congreso Argentino de Ciencias de la Computación*. Vol. 13. 2007.

[32] A. Arrieta y col. "Gestión y Reconocimiento Óptico de los Puntos Característicos de Imágenes de Huellas Dactilares". En: *Universidad de Salamanca* (2016).