ANÁLISIS DE LA EFECTIVIDAD DE LOS MODELOS DE AUTENTICACIÓN 2FA Y MFA DE ACUERDO A LOS ALGORITMOS Y PROTOCOLOS APLICADOS EN LA SEGURIDAD DE CUENTAS DE SERVICIOS Y PLATAFORMAS ONLINE EN COLOMBIA.

JENNY CAROLINA SEPULVEDA MARIN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2022

ANÁLISIS DE LA EFECTIVIDAD DE LOS MODELOS DE AUTENTICACIÓN 2FA Y MFA DE ACUERDO A LOS ALGORITMOS Y PROTOCOLOS APLICADOS EN LA SEGURIDAD DE CUENTAS DE SERVICIOS Y PLATAFORMAS ONLINE EN COLOMBIA.

JENNY CAROLINA SEPULVEDA MARIN

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

DIRECTOR
YENNY STELLA NUNEZ ALVAREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

CONTENIDO

GLOSARIO

2FA Autenticación de dos pasos que combina dos factores o métodos para aumentar la seguridad en el ingreso.

AUTENTICACIÓN Procedimiento que permite validar la información e identidad de un usuario, para esto se utilizan diferentes factores o métodos que pueden permitir esto.

BIOMÉTRICO Es el reconocimiento de elementos físicos e intransferibles de las personas, por ejemplo, las huellas digitales, e reconocimiento facial, etc.

OTP'S Códigos o pines de ingreso de un solo uso, normalmente se envían a través de mensajes de texto o correo electrónico.

SEGURIDAD Ausencia o control del peligro o amenaza utilizándose sistemas, medios humanos u organizativos para eliminarlos o reducirlos.

RESUMEN

En las últimas décadas se ha observado una nueva tendencia de evolución en sistemas de autenticación (unifactor o multifactor), su meta es asegurar la información del usuario utilizando métodos de seguridad que respalden su identidad al momento de usar un sistema; sin embargo, esto ha ocasionado que varios perpetradores averigüen la manera de vulnerar dichas seguridades, aprovechando falencias aún no corregidas en los procesos de autentificación. Por esto, es de suma importancia determinar la efectividad de este tipo de sistemas en el momento de garantizar una protección al usuario. El objetivo principal de esta monografía se centra en encontrar, mediante una revisión bibliográfica, que tan efectiva es la autenticación de dos factores al momento de proteger los datos personales de los usuarios que utilizan cuentas en plataformas online en Colombia. Las principales fuentes de información utilizadas para el cumplimiento del objetivo son las publicaciones de artículos científicos extraídos de bases de datos y de buscadores en línea, permitiendo el debido análisis y comparación de resultados obtenidos a nivel internacional y local.

Palabras claves: 2FA, seguridad, biometría, MFA

ABSTRACT

In recent decades, a new evolution trend has been observed in authentication systems (unifactor or multifactor), its goal is to secure user information using security methods that support their identity when using a system; however, this has caused several perpetrators to find out how to violate said security, taking advantage of flaws not yet corrected in the authentication processes. For this reason, it is extremely important to determine the effectiveness of this type of system when guaranteeing user protection. The main objective of this monograph focuses on finding, through a bibliographic review, how effective two-factor authentication is when protecting the personal data of users who use accounts on online platforms in Colombia. The main sources of information used to fulfill the objective are the publications of scientific articles extracted from databases and online search engines, allowing due analysis and comparison of results obtained at an international and local level.

Keywords: 2FA, security, biometrics, MFA

INTRODUCCIÓN

En el desarrollo de la revisión bibliográfica se logró determinar la importancia de la aplicación de un modelo de autenticación de dos factores, tenido en cuenta los cambios que se han dado en las tecnologías y en cómo se ven afectadas las plataformas de servicios online. Dichos avances han permitido dar cuenta de la vulnerabilidad de la información a causa de las medidas de seguridad que se aplican en la cotidianidad y en las organizaciones, ya que el uso constante de las redes y el acceso a diferentes sistemas de almacenamiento han contribuido a que los ataques cibernéticos o filtraciones ocurran con mayor frecuencia.

Sin embargo, dentro de los hallazgos más significativos de este desarrollo se encuentra que, entre los factores, existen ventajas y desventajas las cuales, dependiendo las características de la información que se desea proteger y el sistema al cual se va a ingresar, pueden determinar los factores de autenticación más adecuados a implementar. Por otra parte, con el desarrollo llevado a cabo se logró establecer que la eficiencia de la aplicación y ejecución de un sistema de autenticación de dos factores está determinada por las características individuales de cada uno de los elementos involucrados y ellos mismo son los que establecen cuál de los factores existentes es el más adecuado a implementar.

De igual manera, se tuvo en cuenta la normatividad que rige los derechos de autor y propiedad intelectual, citando y referenciando a los autores de cada uno de los documentos de los cuales se extrajo la información necesaria para la construcción de este documento.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La efectividad de la autenticación de dos factores (2FA) aplicados en la seguridad de cuentas de servicios y plataformas online en Colombia contra el ataque y robo de datos se ha evaluado ampliamente[1]. Si bien la autenticación 2FA tiene como objeto mejorar la resistencia o protección de los sistemas de seguridad convencionalmente conocidos (contraseñas o claves de acceso) aún se presentan casos de personas del común e incluso grandes empresarios que teniendo como método adicional de seguridad la autenticación de 2FA han sido vulnerados y hackeados, robándoles tanto información financiera como datos o cuentas personales[2]. Las nuevas tecnologías y el uso cada vez más frecuentes de dispositivos móviles por parte de grandes y pequeñas compañías (bancarias, de servicios o de entretenimiento) para extender y facilitar la prestación de sus servicios, ha llevado casi inevitablemente a toda la población conectada a una red eléctrica, a tener un dispositivo móvil y a desarrollar en este gran parte de las operaciones bancarias, manejo de información o uso de sus redes sociales; donde claramente se desea navegar de manera segura y tranquila al realizar cualquier actividad dentro de las plataformas online. Sin embargo es preciso tener en cuenta la inversión que implica la aplicación de nuevos métodos para combatir problemas relacionados con el robo de información.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuál es el nivel de efectividad de los modelos de autenticación 2FA Y MFA de acuerdo a los algoritmos y protocolos aplicados para garantizar la seguridad de la información al momento de efectuar diferentes transacciones a través de cuentas de servicios y plataformas online en Colombia?

[1] ANDRADE CHÁVEZ, Juan Carlos. Diseño De Un Sistema De Triple Factor De Autenticación Basado En Reconocimiento De Similitud De Imágenes, Tesis de Maestría. Universidad Internacional Sek. Facultad deIngeniería, 2019, 26 p.

[2] VELÁSQUEZ LAGOS, Ignacio Andrés. Framework para la Comparación y Selección de Esquemas para la Autenticación Multi-Factor. Tesis de Maestría. Universidad del Bio-Bio.Facultad de Ingeniería, 2017, 23 p.

2 JUSTIFICACIÓN

Hoy en día la digitalización y las nuevas tecnologías se infiltran de manera decisiva en las sociedades modernas. Uno de los métodos o sistemas de seguridad que han sido claves en los últimos años son los sistemas de autenticación múltiple; estos cubren gran variedad de áreas en un mundo hiperconectado, tales como pagos en línea, comunicaciones, redes sociales, manejo de datos, etc. En particular el método de autenticación de dos factores ha tenido gran relevancia en los últimos años y ha influido de manera positiva en la seguridad de datos; sin embargo, los piratas informáticos o hackers han desarrollado de igual manera métodos o sistemas para vulnerar estos sistemas de protección adicional[3]. Es por esta razón que se hace necesario investigar, analizar y evaluar cuan efectivo es este método de seguridad adicional y, de igual manera, intentar establecer algunas bases para una posible mejora de este o ratificar la eficacia de la 2FA adicional en protección de nuestros datos.

Por tanto, es de suma importancia conocer que tan eficientes son estos métodos, no solo desde el punto de vista académico, si no desde la percepción de los usuarios de este tipo de dispositivos, ya que con base en su experiencia es posible sugerir algunas mejoras en la efectividad de los métodos de 2 factores para proteger la información personal.

Es así como en este trabajo se busca determinar la efectividad de la 2AF desde la perspectiva académica y científica analizando los aportes de diversos autores en artículos extraído de bases de datos. Y, con base en esta información, se espera establecer algunas sugerencias y mejoras que las personas y aplicaciones Android puedan tener al momento de desarrollar este tipo de sistemas múltiple factor.

[3] BONNEAU, Joseph, *et a*l.The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. En: 2012 IEEE Symposium on Security and Privacy, 2012, p. 55

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar la efectividad de los modelos de autenticación 2FA Y MFA en relación a los protocolos aplicados en la seguridad de cuentas de servicios y plataformas online en Colombia, estableciendo los ciberataques que pueden vulnerar al sistema y cómo prevenirlos.

3.2 OBJETIVOS ESPECÍFICOS

- Diseñar comparativa sobre los modelos de autentificación 2FA y MFA para identificar factores y pautas con el fin de diseñar estrategias que mejoren el uso de las plataformas online.
- Analizar los métodos y protocolos de autenticación 2FA y MFA en plataformas online, teniendo en cuenta cuáles son sus posibles riesgos y determinar el manejo inadecuado de los mismos.
- Identificar las vulnerabilidades de los modelos de autenticación 2FA y MFA, a través de los diferentes mecanismos de protección de la información para validar el nivel de seguridad en el manejo de las plataformas en Colombia.

4 MARCO REFERNCIAL

4.1 MARCO TEÓRICO

Andress[4] en su estudio concluyó que implementar un sistema de autenticación de un solo factor como las contraseñas con mayor combinación de elementos posible es un permite una protección más fuerte de los datos e información de los usuarios, sin embargo, el utilizar contraseñas fuerza a las personas a guardarlas o apuntarlas en algún lugar asequible para disminuir el riesgo de olvidarlas y tener que realizar la creación constante de nuevas. Este hecho llega a representar un peligro ya que la contraseña queda al acceso de terceros y como consecuencia queda anulado su alto nivel de seguridad.

Por dicha razón, se recomienda un segundo y tercer factor de autenticación, en el segundo caso se recomienda utilizar elementos de carácter biométrico, entendido como algo que es propio del usuario, como por ejemplo las huellas dactilares, la composición de la retina, la voz o el patrón en los intervalos de pulsación de teclas, etc[5]. En cuanto al tercer factor este estaría relacionado a algo que el usuario tiene en posesión en un medio físico, siendo algunas ejemplificaciones las tarjetas de identidad, tokens físicos o de software[6].

De igual manera, en el estudio llevado a cabo por Ñique[7] se recomienda la adopción de un modelo de defensa en profundidad, que permita la organización y protección de cada recurso de información. En este sentido, se establece la insuficiencia de aplicar un método de autenticación tradicional caracterizado por el uso exclusivo de un usuario y una contraseña o pin fijo, razón por la cual es necesario implementar métodos de autenticación de doble factor, como por ejemplo utilizar el usuario y contraseña fija más mensaje de texto o correo de verificación, preguntas de seguridad, entre otros[8].
La aplicación y configuración de este método de doble factor permite un mayor control de seguridad y validación de los usuarios que acceden a los recursos de información, permitiendo verificar que estos sean únicamente los autorizados para ello.

[4] ANDRESS, Jason. The basics of information security: understanding the fundamentals of InfoSec in theoryand practice, Syngress Publishing, 2011, p 240.
[5] MANTOVANI, Valentino, Autenticación de Múltiples factores (MFA). Trabajo de grado. Universidad de Buenos Aires, Facultad de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería, 2019, 7p.
[6] MANTOVAN, Op. cit., p 8
[7] ÑIQUE, Víctor, Implementación De Solución De Autenticación Segura Basada En Doble Factor En UnaEntidad Del Estado. Trabajo de grado. Universidad San Ignacio de Loyola, Facultad de Ingeniería, 2016,77p.
[8] Ñique, Op. cit., p 77.

En el estudio bibliográfico realizado por Velásquez[9], dentro de los hallazgos más significativos se encuentra que la combinación de los factores de conocimiento y posesión es muy predominante entre los métodos de autenticación multifactorial, especialmente el uso de contraseñas de texto y tarjetas inteligentes. De igual manera se determinó que la autenticación de tres factores, aunque parece ser que es la metodología menos aplicada, es la segunda combinación de factores más investigada.

4.2 MARCO CONCEPTUAL

4.2.1 Seguridad informática.

Es conocida como esas medidas que se implementan para impedir la realización de operaciones no autorizadas en un sistema o red informática, evitando los daños que puedan ocasionarse sobre la confidencialidad y autenticidad de la información de los usuarios y que disminuye el interfiere en el rendimiento del sistema[10]. De igual manera, la seguridad informática salvaguarda la integridad de los datos del usuario y es capaz de mantener la disponibilidad del sistema de información y la autentificación de identidades. Esta última es esencial para garantizar que los usuarios protejan su información en cada aplicación que utilizan[10].

4.2.2 Autentificación.

Es el proceso donde el sistema verifica identidad digital del usuario utilizando un canal de comunicación por medio del cual realiza una petición para conectarse a un sistema, es así como, una vez confirmada la identidad se otorga la autorización, con la cual se establecen y delimitan los recursos a los que puede acceder el usuario[11].

4.2.3 Sistemas de autentificación.

A continuación, se describen los sistemas de autentificación utilizados en las aplicaciones móviles[12]:

- **Biométricos (Inherencia):** Este sistema utiliza las características físicas del usuario y una la inteligencia artificial o el reconocimiento de formas para verificar la identidad

[9] VELÁSQUEZ LAGOS, Ignacio Andrés. Framework para la Comparación y Selección de Esquemas para la Autenticación Multi-Factor. Tesis de Maestría. Universidad del Bio-Bio.Facultad de Ingeniería, 2017, 87 p.
[10] VIEITES, Álvaro. Enciclopedia de la Seguridad Informática. 2 a edición. Grupo Editorial RA-MA, 2011, p.49
[11] ANDRADE CHÁVEZ, Juan Carlos. Diseño De Un Sistema De Triple Factor De Autenticación Basado En Reconocimiento De Similitud De Imágenes, Tesis de Maestría. Universidad Internacional Sek. Facultad de Ingeniería, 2019, p. 40.
[12] VELÁSQUEZ LAGOS, Ignacio Andrés. Framework para la Comparación y Selección de Esquemas para la Autenticación Multi-Factor. Tesis de Maestría. Universidad del Bio-Bio.Facultad de Ingeniería, 2017, p 40-45.

del usuario. Las características que más se implementan en la actualidad son: iris, retina, huellas dactilares, geometría de la mano, escritura o voz del usuario[13].

- **Dispositivos (Posesión):** Son elementos o dispositivos físicos que se le otorgan al usuario donde se almacenan los datos de autenticación, por ejemplo, tarjetas, dispositivos USB, tarjetas de coordenadas, etc[14].
- **Contraseñas (Conocimiento):** Es el método de autenticación más común utilizado en la actualidad y se basa en el uso de información secreta que solo el usuario dispone[15].

4.2.4 Multi-factor de autentificación

Cuando se unifican dos o más sistemas de autentificación se crea un sistema multi-factor en donde se crea una protección por capas para la mayor seguridad del usuario[16].
Actualmente, gracias al avance de los dispositivos móviles, se utiliza un sistema de fichas de seguridad, el cual es un sistema de autentificación multifactor en el que se usa el Hardware, como por ejemplo un teléfono móvil, para generar tokens sincronizados en el tiempo basados en una clave compartida con un servicio de autenticación, permitiendo que estos dispositivos pueden interactuar directamente con los servicios de autenticación, no obstante, en ocasiones este modelo permite la creación de una contraseña única sincronizada en el tiempo para que los usuarios la ingresen[17].
De igual manera, gracias a los avances tecnológicos algunos dispositivos móviles permiten que los usuarios combinen el uso de una contraseña con un factor biométrico como el escaneo de huellas dactilares o el reconocimiento facial[18].

4.2.5 Autenticación de dos factores

El proceso de autenticación de dos factores es conocido también como la autenticación de dos fases o 2FA, por sus siglas en inglés y es definido como empleo de dos sistemas de autenticación en el ingreso a un sistema para comprobar y validar la identificación del usuario, esto dado la insuficiencia del uso de un único factor en el mecanismo de seguridad[19] llevando a los investigadores y expertos a buscar otras alternativas que le

[13] MANTOVAN, Op. cit., p 8.
[14] GUERRERO RAMÍREZ, Javier. Autenticación de doble factor mediante OTPs.Tesis Maestría. Universitat Oberta de Catalunya, 2019, 6p.
[15] 15BONNEAU, Joseph, et al.The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. En: 2012 IEEE Symposium on Security and Privacy, 2012, p. 320-350.
[16] DEO Shaneel y FARIK Mohamed. Information Security - Recent Attacks in Fiji Techtarget. En: International Journal of Scientific & Technology Research, 2016, Vol 55.
[17] ANDRADE, Op. cit., p 42.
[18] ANDRADE, Op. cit., p 42
[19] GUERRERO, Op. cit., p7-9

permitan al usuario identificarse de forma rápida u segura razón por la cual se ha popularizado el uso de distintos factores de autenticación. Tradicionalmente, el proceso de autenticación de un único factor involucra únicamente la creación y uso de una contraseña fija y un usuario, sin embargo, este aspecto en la actualidad ha demostrado ser vulnerable e insuficiente para proteger a los usuarios de ataques cibernéticos que filtran, roban o destruyen su información personal. Esto ha llevado a que se recomiende la combinación de este mecanismo tradicional y uno complementario, aunque hay estudios que se decantan más por la implementación de tres o más factores, utilizándose pines, huellas dactilares, reconocimiento facial, de tarjetas u OTPs, que hacen referencia a esos pines so códigos de corta duración[20].

Empero, a pesar de que se utilice otro factor de autenticación, desde la creación de se ha encontrado que las contraseñas tienen un bajo nivel de seguridad esto a causa de que los usuarios normalmente repiten una misma contraseña en diversos sistemas informáticos, esto anudado a que, para evitar los olvidos, los usuarios prefieren anotarlas en sitios visibles o revelarla a amistades o familiares, exponiendo la información a riesgo de filtraciones o que terceros puedan acceder a ella[21].

Esta ha sido una de las razones por las que se recomienda implementar y mejorar los procesos de autenticación, además se debe tener en cuenta que los factores de autenticación no son 100% seguros ya que todos presentan un porcentaje de vulnerabilidad. Por ejemplo, en el uso de contraseñas débiles o la divulgación de ellas es la principal debilidad de este factor, mientras que se cree que los aspectos biométricos no pueden ser “robados”, en la actualidad si es posible, aclarando que en esto influencia la calidad de la fotografía y del sensor, a esto se le conoce como *biohacking*[22], en este factor también influye desfavorablemente el hecho de que no puede ser renovado o cambiado, aunque este último aspecto también puede ser considerado una ventaja frente a los otros factores todo está sujeto a la calidad de los elementos necesarios para realizar la identificación[23] . Así mismo, al implementar las tarjetas de identificación o dispositivos USB se encuentra que la principal desventaja que se presenta es el riego de que lleguen a manos de terceros y agentes no autorizados, afectando la seguridad del sistema[24].

[20] Ibid. p 8-9.
[21] Ibid. p 10-11.
[22] CIFUENTES DÍAZ, Erick Fabricio y MARTÍNEZ VÁSQUEZ, Maikol Estiven. Biohacking para la protección de los activos de información en las pymes por medio de un sistema de doble factor de autenticación. Tesis de especialización. Universidad Católica de Colombia, 2019, p12.
[23] MANTOVANI, Op. cit., p29-31.
[24] GONZÁLEZ ARRIETA, Angélica, et al. Llaves FIDO (Fast IDentify Online) como segundo factor de autenticación en la gestión on-line de los procesos de enseñanza y aprendizaje. 2018.

En contra parte, durante la revisión de los documentos se halló que las ventajas de implementar esta combinación de factores de autenticación, además de intensificar los niveles de seguridad, es que le permite a la empresa o usuario tener cierto control e identificación sobre los casos de intento de ingreso ya que, de una forma u otra, el intento de ingreso necesita de algún elemento del individuo.

Adicionalmente, aunque existen desventajas en cada uno de los factores ellos también posen ventajas que, aunque pueden parecer muy obvias, facilitan la adopción e implementación de ellos. Como la autenticación utilizando elementos biométricos, en ella no se evidencia la necesidad de portar o utilizar otro elemento ya que son factores que se encuentran en el mismo individuo, aunque requiere la adquisición de une tecnología especializada, entre mejor sea su calidad, más riguroso será el proceso de autenticación y la implementación de los factores biométricos permite reducir la probabilidad de que personal no autorizado acceda a zonas o información restringida, como puede suceder en caso de robo o pérdida de credenciales o tarjetas de identificación[25].

Por otra parte, otro elemento que se ha implementado durante años son los OTPs, siendo conveniente su aplicación ya que, al enviarse, comúnmente, a los dispositivos móviles, el usuario siempre tendrá acceso a ellos mientras lo tenga consigo y puede no necesitar una conexión a internet, como es el en el caso de que los códigos sean enviados vía mensaje de texto o llamada telefónica[26]. Del mismo modo, al tener estos códigos una vida útil relativamente corta, disminuyen la posibilidad de robo y acceso de terceros. Teniendo en cuenta que las ventajas y desventajas de cada uno de los factores de autenticación que se implementan hoy en día son muchas, es necesario que los usuarios y las empresas realicen una evaluación de sus capacidades y la necesidad de la implementación de uno o más factores de autenticación, basándose en la información que se desea proteger y los recursos que se tengan a la mano.

4.3 MARCO HISTÓRICO

En las últimas décadas se ha visto un incremento exponencial en los avances tecnológicos, permitiendo que un mayor número de usuarios y empresas puedan almacenar su información de manera virtual. No obstante, el uso de las redes sociales, la creación de sucursales bancarias virtuales y la constante necesidad de vinculación de diferentes cuentas, que facilita el intercambio de información, han permitido que la información personal de los individuos se encuentre vulnerable al robo, pérdida o filtración, requiriendo que la creación de nuevos sistemas de autenticación y seguridad o

[25] MANTOVANI, Op. cit., p29.
[26] HUERRERO, Op. cit., p29.

la mejora y optimización de los mimos, buscando garantizar la privacidad y confidencialidad de la información. Teniendo en cuenta lo anterior, las aplicaciones móviles, y los equipos mismos, han avanzado, adoptándose e implementando diversos métodos de autenticación en vista de la débil protección que supone la implementación de un solo factor[27]. Siendo el esquema de las contraseñas de texto que combinan caracteres alfanuméricos el más usado hoy en día y, en los años más recientes, se ha aumentado implementación de los medios biométricos para los procesos de autenticación[28]. Sin embargo, aunque en ha sido un tema estudiado desde poco años antes de los años 2000, es a partir de 2015 que el número de investigaciones y publicaciones relacionadas al tema de los esquemas de autenticación[29]. No obstante, la cantidad de investigaciones desarrolladas y publicadas en cada año varía y, del mismo modo, los esquemas de autenticación que despiertan el interés de los investigadores son igual de variables, siendo más prevalentes desde el año 2010, hasta la actualidad, las investigaciones centradas en los sistemas biométricos[30]. Es así como, dentro de las investigaciones consultadas, se logra evidenciar que los escenarios de las investigaciones igualmente varían[31]. Esto se puede explicar teniendo en cuenta la postura que las empresas y las personas han tomado en cuanto a la información que se encuentra almacenada digitalmente, asimismo esto se ha originado a raíz del nuevo ambiente que diferentes sectores, como el bancario/financiero[32] y la salud[33], han implementado, creando grandes bancos de información que, de no implementar un sistema de protección adecuadamente.

Finalmente, con este aumento en las investigaciones se descubrió que solo en 2015[34] únicamente el 10% de las empresas realizaban los procesos de autenticación de doble factor mientras el 90% restante únicamente implementaba una autenticación simple de usuario y contraseña, registrándose en este mismo año vulneraciones sistemáticas en 41% de las empresas con este tipo de autenticación. Aunque se esperaría que los porcentajes de las empresas que aplican procesos de autenticación de doble factor o e tres factores hayan aumentado, conocer las cifras las cifras exactas y la calidad de estos

[27] VELÁSQUEZ. Op. cit., p 21
[28] Bonneau, J.; Herley, C.; Van Oorschot, P.C. y Stajano, F. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: 2012 IEEE Symposium on Security and Privacy, pp. 553-567. IEEE, 2012. Citado por: VELÁSQUEZ LAGOS, Ignacio Andrés. Framework para la Comparación y Selección de Esquemas para la Autenticación Multi-Factor. Tesis de Maestría. Universidad del Bio-Bio.Facultad de Ingeniería, 2017, p 21.
[29] VELÁSQUEZ. Op. cit., p 21.
[30] VELÁSQUEZ. Op. cit., p 22.
[31] Ibid. p. 22
[32] CAMPO RUIZ, Asunción. La digitalización del sector bancario. Tesis de pregrado. Universidad de Cantabria, 2019.
[33] FORTUNY, Sabartés, et al. Digitalización de historias clínicas y seguridad del proceso. *Papeles médicos*, 2010, vol. 19, no 2, p. 4.
[34] ÑIQUE, Víctor, Implementación De Solución De Autenticación Segura Basada En Doble Factor En Una Entidad Del Estado. Trabajo de grado. Universidad San Ignacio de Loyola, Facultad de Ingenieria,2016, p 11

es una tarea difícil ya que se existen diversas variables, tanto internas como externas, que influyen en la determinación y en el impacto de los factores de autenticación.
Sin embargo, considerando el número de investigaciones realizadas la perspectiva de que en estos años la aplicación de dos factores de autenticación es más común que antaño, lográndose evidenciar en la cotidianidad esto, puesto que los dispositivos móviles ya integran el uso de elementos biométricos como la lectura dactilar, siendo la más usada, con la integración de lectores de huellas en sus diseños, y el reconocimiento facial, gracias al aumento en la calidad de las imágenes que proporcionan las cámaras de estos dispositivos. Además, se mantiene el uso de códigos alfanuméricos, considerándose este el mecanismo de acceso al dispositivo.

4.4 MARCO LEGAL

Para el desarrollo de esta investigación se tuvo en cuenta la siguiente normatividad:

- **COLOMBIA. CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 23 (28 de enero de 1984)[35]. Sobre derechos de autor [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 1984. Nro. 35.949.**
- **COMUNIDAD ANDINA. LA COMISIÓN DEL ACUERDO DE CARTAGENA. Decisión Andina 351 (17 de diciembre de 1993)[36]. Se decide aprobar el régimen común sobre derecho de autor y derechos conexos [en línea].**
- **INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC)[37]. ICONTEC. documentación, presentación de tesis, trabajos de grado y otros trabajos de investigación, NTC-1486 [En línea]. Bogotá D.C: El Instituto. 2008.**
- **INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC)[38]. Referencias bibliográficas. Contenido, forma y estructura, NTC 6166 [En línea]. Bogotá D.C: Instituto colombiano de normas técnicas y certificación (Icontec). 2016.**

[35] COLOMBIA. CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 23 (28 de enero de 1984). Sobre derechos de autor [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 1984. Nro. 35.949.
[36] COMUNIDAD ANDINA. LA COMISIÓN DEL ACUERDO DE CARTAGENA. Decisión Andina 351 (17 de diciembre de 1993). Se decide aprobar el régimen común sobre derecho de autor y derechos conexos [en línea
[37] NSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). ICONTEC. Documentación, presentación de tesis, trabajos de grado y otros trabajos de investigación, NTC-1486 [En línea]. Bogotá D.C: El Instituto. 2008.
[38] NSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Referencias bibliográficas. Contenido, forma y estructura, NTC 6166 [En línea]. Bogotá D.C: Instituto colombiano de normas técnicas y certificación (Icontec). 2016.

5 MODELOS DE AUTENTICACIÓN 2FA Y MFA DE ACUERDO A LOS ALGORITMOS Y PROTOCOLOS APLICADOS EN LOS MÉTODOS DE SEGURIDAD DE CUENTAS DE SERVICIOS Y PLATAFORMAS ONLINE EN COLOMBIA

5.1 CRITERIOS DE SELECCIÓN Y DIFERENCIACIÓN DE LOS MÉTODOS DE AUTENTICACIÓN 2FA Y MFA

La diferencia entre MFA y 2FA se basa en que la autenticación de dos factores siempre usa dos de estos factores para verificar la identidad de un usuario, mientras que la autenticación de múltiples factores puede involucrar dos o tres de estos factores.

Ya sea que un usuario esté accediendo a su correo electrónico o al archivo de nómina de una empresa, debe verificar su identidad antes de que se le otorgue el acceso. Hay tres formas para que los usuarios verifiquen que son ellos mismos. Puede hacerlo desde:

• Datos conocidos: los usuarios brindan información que solo ellos conocen, como una contraseña o una respuesta a una pregunta en específico.

• Datos privados: los usuarios proporcionan algo propio, como un token o una contraseña de un solo uso.

• Reconocimiento: los usuarios confían en una característica única, como las huellas dactilares, el escaneo de retina o el reconocimiento de voz.

En cuanto a la seguridad brindada el MFA resulta más beneficioso en comparación con el 2FA y esto es por los requerimientos de más factores de autenticación para el usuario.

La mayoría de los profesionales y usuarios de TI reconocen que las contraseñas pueden verse comprometidas fácilmente, sin embargo, es menos probable que un hacker pueda obtener la contraseña y el token o el dispositivo móvil del mismo usuario. La posibilidad de que el atacante también tenga la huella digital del usuario es mucho menor. Los atributos inherentes de una persona son difíciles de piratear o robar, y eso es lo que los hace valiosos como factor de autenticación.

La autenticación multifactor consiste en realizar dos o más pruebas diferentes a los usuarios para verificar que son quienes dicen ser, con el objetivo de agregar una capa más de seguridad al verificador. Estas pruebas pueden ser diferentes, como contraseñas, tener una subclave privada, certificados digitales instalados en la computadora, tokens,

etc. Es muy común (y cada vez más) considerar la autenticación de dos factores o 2FA, al menos como una opción para los usuarios que desean mejorar la autenticación de sus cuentas. Empresas como Mercado Libre, Google, Gmail, Apple, iCloud, Facebook y muchas entidades bancarias ya lo han hecho.

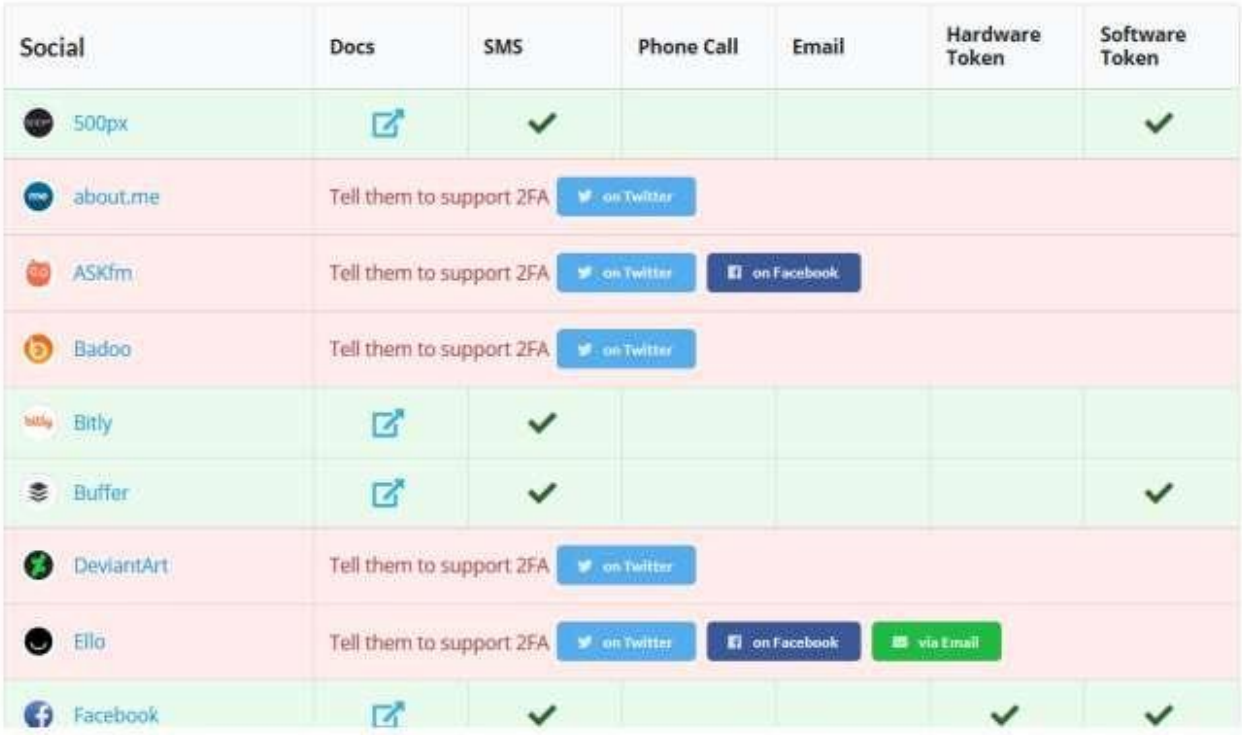

Ilustración 1. Autenticación 2FA y redes involucradas
Fuente: MANTOVANI, Valentino. *Autenticación de Múltiples factores (MFA). Disponible en: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1524_MantovaniV.pdf, 2019.*

La ilustración 1 presenta alguna de las redes sociales involucradas y los soportes de comunicación que soportan la seguridad en dos pasos En lugar de usar solo un factor para verificar su identidad, como una contraseña, usa dos: su contraseña y una contraseña de un solo uso (OTP) que se le envía a través de SMS o correo electrónico.

Los MFA utilizan pruebas para poder validar correctamente la transacción solicitada, estas pruebas son agrupadas en factores de distintos tipos y clasificadas para poder armar una definición más clara de los requerimientos que debe tener un verificador para poder realizar un autenticado de múltiples factores, uno de ellos es el factor de conocimiento, el cual está basado en que ya se conoce, es decir, los factores de conocimiento son la forma más común de autenticación. El usuario necesita demostrar que conoce un secreto para poder autenticarse, como por ejemplo un ping, una contraseña, fechas de nacimiento, el nombre de su primera mascota, etc. Dentro de los factores físicos, estos son basados en algo que ya se posee, los factores físicos han

estado en uso desde que se tiene conocimiento, el ejemplo más básico es el de la llave de una cerradura y por último los factores inherentes, estos son factores que están asociados al usuario, y generalmente son métodos biométricos, como los lectores de huellas, de retina o reconocimiento de voz.

La autenticación de dos pasos muchas veces se suele confundir con 2SV ya que parecen ser lo mismo, pero no lo son. Se dice que la autenticación de dos pasos es una expansión de la autenticación simple y es muy utilizada en los inicios de sesión de algunos sitios web.

Ilustración 2. Autenticación en dos pasos.
Fuente: MANTOVANI, V. *Autenticación de Múltiples factores (MFA). Disponible en: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1524_MantovaniV.pdf. 2019.*

La información que los usuarios o empresas depositan en páginas o servidores informativos ha cobrado mayor importancia en los últimos años, es por esto por lo que las garantías o métodos que se implementen para garantizar la seguridad y protección de ella empiezan a cobrar mayor protagonismo y las empresas destinan mayores presupuestos para poder obtener una interfaz más segura para ellos y para sus empleados.

No obstante, en la actualidad no únicamente las páginas o servidores internos de las empresas han aumentado su seguridad ya que los ataques cibernéticos han evidenciado la vulnerabilidad de la información personal que fácilmente se proporciona en los diferentes espacios cibernéticos, es por esto que las redes sociales, los servicios de mensajería electrónica y demás espacios han decidido reforzar la seguridad que le ofrecen a sus usuarios implementando un modelo multifactorial de autenticación,

permitiéndose garantizar la veracidad de la información proporcionada y reduciendo los riesgos de accesos no autorizados a ellas.

Teniendo en cuenta lo anterior, el hecho de descartar y elegir los métodos más eficaces para garantizar la seguridad se encuentra ligado a las propiedades de la información o sistema a proteger y las características de la población que harán uso y manejo de esa interfaz diseñada.
Ahora, en los últimos años, estas no han sido las únicas consideraciones que se han tenido en cuenta para realizar la selección de los factores de autenticación dado que también se deben estudiar y analizar las vulnerabilidades detectadas en los sistemas, lo que permitirá el establecimiento de uno o varios métodos de autenticación de tal manera que proporcionen una mayor seguridad[39] a los usuarios y permitan dar una mejor solución a los problemas identificados.

De igual manera, otro criterio que es utilizado para determinar qué método de autenticación es el más adecuado, se encuentra relacionado a los costos de la implementación y diseño del método escogido[40]. Esto hace referencia al presupuesto que las empresas deben establecer para la creación o modificación de una interfaz más segura, sin embargo, para lograr una mayor seguridad las empresas, normalmente, deben realizar mayores inversiones y aumentar presupuestos para lograrlo, lo cual puede, en muchas ocasiones, dificultar la adquisición de nuevos y más actualizados protocolos de seguridad ya que elegir un sistema de autenticación más complejo suele significar un aumento en los costoso y se es necesario que la empresa tenga una participación activa en el mercado para justificar los costos ocasionados por él[41].

Por otro lado, para determinar qué método de autenticación tiene mayor pertinencia se suelen tener en cuenta las tendencias futuras, la privacidad y el tipo de recursos que debe utilizar el usuario para poder implementarlo[42,] esto teniendo en cuenta el acelerado avance que experimentan las tecnologías en la actualidad y las exigencias que este plantea tanto para los usuarios como para las empresas desarrolladoras. Lo anterior se encuentra enlazado con el contexto, debido a que es una de las variables más importantes a la hora de determinar o considerar un modelo de autenticación multi-factor, puesto que cada para ambientes posee unas características, funcionamiento y

[39] ODRIGUEZ VALDES, Osviel; LEGON, C.M y SOCORRO LLANES, Raisa. Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica. *Rev cuba cienc informat* [online]. 2018, vol.12, suppl.1, pp.13-27. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992018000500002&lng=es&nrm=iso
[40] VELÁSQUEZ. Op. cit., p25.
[41] ALTINKEMER, Kemal; WANG, Tawei. Cost and benefit analysis of authentication systems. Decision Support Systems, 2011, vol. 51, no 3, p. 394-404.
[42] Ibid. p 25.

necesidades especiales, elementos que determinan las características y la rigurosidad de los factores a implementar[43]. Es decir, ambientes como la banca y el comercio poseen una información y un procesamiento que requieren un manejo y procesamiento diferente al que se realiza en las redes sociales o en aplicaciones web, esto ya que son ambientes más exigentes y requieren un sistema que les garantice la validez de la información y que, a su vez, les otorgue mejores garantías en cuanto a la seguridad y protección de ellos, mientras las redes sociales o páginas web requiere sistemas que le permitan validar la información de una manera más ágil y rápida.

Por otra parte, también se resalta la necesidad de que, a nivel empresarial, los factores de autenticación escogidos cumplan con la normatividad vigente que permitan brindarles garantías a los usuarios en cuento a la seguridad y al manejo de su información[44], lo cual le permitirá aumentar la fidelización de sus usuarios y optimizar el rendimiento en las bases de datos. Finalmente, se encontró que algunos documentos se expresa que, además de los elementos mencionados, se debe tener en cuenta el conocimiento y el recurso humano para que se pueda diseñar e implementar un sistema de autenticación de 2FA[45] y se menciona la importancia de la cultura organizacional, puesto que ella permite o dificulta la efectividad del establecimiento de una estrategia de seguridad para la información[46], aunque estos últimos elementos poseen una connotación más subjetiva en relación a factores más como el contexto y los costos, que se hallan más enfocados en el ámbito económico y comercial.

[43] Ibid. p 25.
[44] SECLÉN ARANA, Javier Alfonso. Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001 (Tesis de maestría). Universidad Nacional Mayor de San Marcos. Facultad de Ingeniería de Sistemas e Informática, 2016, p 25.
[45] SECLÉN ARANA, Javier Alfonso. Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001 (Tesis de maestría). Universidad Nacional Mayor de San Marcos. Facultad de Ingeniería de Sistemas e Informática, 2016, p 25.
[46] ibid. p 11.

6. ANALISIS DE LOS MÉTODOS DE AUTENTICACIÓN 2FA Y MFA TENIENDO EN CUENTA RIESGOS Y MANEJO INADECUADO EN LOS DISPOSITIVOS MOVILES

La seguridad informática se ha convertido en uno de los desafíos más grandes en la actualidad para los desarrolladores de las aplicaciones móviles, esto ha dado pie para que ellos construyan un sistema de autenticación estable y seguro, que permita la validación de la información suministrada y la protección de esta. Por lo anterior, es común encontrar en la actualidad las aplicaciones móviles requieran o implementen un sistema de autenticación multifactorial, en los cuales se utilizan dos o más técnicas de autenticación, lo que permitió el desarrollo continuo de sistemas más seguros y estables.

Sin embargo, para realizar el proceso de análisis de estos sistemas de seguridad de las aplicaciones Android y IOS se encontró que los sistemas que se basan en la utilización de algo conocido por el usuario son los más básicos, económicos y utilizados en la actualidad, pero al ser tan básico se ha convertido en el más vulnerable de todos a los que existen ya que únicamente se crean claves alfanuméricas[47]. Es así que este tipo de factores de autenticación se caracterizan por su fácil adopción, el conocimiento que tiene la mayoría de la población sobre él y el hecho de poder adaptarse fácilmente a otros métodos de autenticación, los cuales convierten a los sistemas de seguridad en uno multifactorial, permitiendo obtener una mayor seguridad y validez en la información proporcionada por los usuarios, como por ejemplo, en la actualidad gracias a los avances en la telefonía móvil, se han desarrollado escáneres que permiten la validación e intercambio de información mediante tarjetas con chips integrados[48] esto ha facilitado el proceso los usuarios, no obstante, solo las personas que poseen a tecnología adecuada pueden implementar este tipo de factor o herramienta de autenticación.

Por otro lado, las aplicaciones móviles requieren el acceso de información cada vez más personal lo que ha significado procesos más rigurosos de autenticación, es por esto que en aplicaciones ya es común encontrar sistemas multifactores para la autenticación, empleándose entre dos y tres factores de autenticación para darle acceso a los usuarios, pero, en muchas ocasiones esto solo se da cuando el sistema advierte una amenaza o intento de ingreso no autorizado, estableciendo como principal el uso de contraseñas y usuarios establecidos por los usuarios al momento de registrarse y dar la información inicial.

[47] SILVELO PALLÍN, Arturo. Sistema de autenticación biométrica basado en el análisis del comportamiento mediante interacción por pantalla táctil y sensores de movimiento (Tesis de Pregrado). Universidad e Da Coruña. 2019, p6.
[48] Ibid. p 7.

Teniendo en cuenta los avances en teléfonos móviles, se encuentra que cada vez más dispositivos poseen lector de huella, lo que ha significado que las aplicaciones consideren la lectura biométrica como herramienta alternativa para el ingreso a sus interfaces, un ejemplo de esto son las aplicaciones bancarias en los dispositivos Android e IOS que permiten optimizar el proceso de inicio de sesión vinculando la huella digital con el nombre de usuario y la contraseña alfanumérica para que, al momento de iniciar sesión, únicamente deba emplear la lectura biométrica, reduciendo los tiempos de los usuarios al momento de ingresar. Pero este no ha sido el único elemento biométrico que ha ganado notoriedad en los últimos tiempos ya que el escáner facial ha llegado de la mano con las mejoras en la calidad de las cámaras que vienen incluidas en los dispositivos, no obstante, a pesar de la notoriedad que ha ganado la mayoría de las aplicaciones móviles no la han integrado a sus sistemas de seguridad y autenticación. Aunque estos factores de identificación han permitido que sea más fácil y ágil el ingreso a plataformas, aplicaciones e información desde los dispositivos móviles, también se pueden considerar uno los métodos que permiten una seguridad más fuerte al complementarse con contraseñas y usuarios de ingresos gracias a la dificultad que existe en de replicar los elementos utilizados. Con respecto a los sistemas IOS La autenticación de dos factores es una medida de protección adicional para el Apple ID que se diseñó para garantizar que únicamente que solo el dueño pueda acceder a su cuenta, aunque alguien más conozca la contraseña. Con la autenticación de dos factores, solo el dueño del dispositivo puede acceder a su cuenta en un dispositivo de confianza o en la Web. Cuando se inicie sesión en un dispositivo nuevo por primera vez, se tendrá que proporcionar dos datos: la contraseña y el código de verificación de seis dígitos que se muestra automáticamente en los dispositivos de confianza o que se envían a el número de teléfono.

Ilustración 3.Autenticación IOS

Fuente: Mantovani, Valentino (2018). Autenticación de Múltiples factores (MFA).Disponible en: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1524_MantovaniV.pdf

La autenticación multi-factor (MFA) es lo mínimo que puede hacer si realmente quiere proteger sus cuentas. El uso de algo más allá de la contraseña aumenta significativamente los costos para los atacantes, razón por la cual la tasa de compromiso de las cuentas que utilizan cualquier tipo de MFA es inferior al 0,1 % de la población general como lo explicó el director de seguridad de identidad de Microsoft, Alex Weinert, hace un par de años. En comparación con los ataques de contraseña, los ataques dirigidos a autenticadores sin contraseña son extremadamente raros. Cuando se evalúan todos los tokens emitidos con reclamos de MFA, se observa que menos del 10 % de los usuarios usan MFA por mes en cuentas empresariales (y eso incluye MFA local y de terceros). Hasta que MFA se adopte más ampliamente, hay pocas razones para que los atacantes evolucionen

A pesar de la seguridad que brindan los modelos de seguridad y autenticación en las aplicaciones móviles que emplean los desarrolladores para el almacenamiento de información, en los teléfonos móviles los protocolos de seguridad aún deben enfrentarse a diferentes riesgos los cuales pueden propiciar la pérdida de información, accesos no deseados y fraudes, especialmente los fraudes bancarios, ya que en ellos se ha llegado a almacenar la información y los datos necesarios para ello[49].
Lo anterior ha podido ser el resultado de diversos factores tales como el inadecuado manejo en las claves de ingreso o la ausencia de sistemas de bloqueo, lo que ha facilitado el acceso de terceros, a esto se le agrega el hecho de que en muchas ocasiones se suele recurrir a fuentes no oficiales para descargar las aplicaciones lo que ha dado vía de acceso a malwares que pueden tener diferentes efectos sobre nuestro dispositivo móvil y la información que en él se encuentra gracias a la ausencia de aplicaciones o extensiones que permiten el reforzamiento de la seguridad del dispositivos y la identificación de las vulnerabilidades que se pueden sufrir[50]. Todos los autenticadores son vulnerables, ya que existe una amplia gama de mecanismos para descifrarlos sin embargo, no hace que todos estos sean igualmente vulnerables. Los costos varían enormemente según el tipo de ataque.

Desafortunadamente, todos los autenticadores de uso común en la actualidad (teléfonos, correo electrónico, tokens de código de acceso único (OTP) y notificaciones automáticas) son vulnerables a ataques que involucran la toma del canal de comunicación utilizado para el autenticado (Channel-Jacking) o interceptar y reproducir mensajes de autenticación utilizando una máquina en el medio (phishing en tiempo real). Entre las

[49] RODRÍGUEZ POVEDA, Alcibíades. Seguridad aplicada en los procesos transaccionales de las aplicaciones móviles. Universidad Piloto de Colombia, 2018.
[50] RODRÍGUEZ POVEDA, Alcibíades. Seguridad aplicada en los procesos transaccionales de las aplicaciones móviles. Universidad Piloto de Colombia, 2018.

vulnerabilidades que se pueden presentar son los ataques SS7, en este los cibercriminales acceden a los mensajes de diferentes maneras y presentan una máxima concentración en los protocolos de error que generan algunas compañías de telecomunicaciones para poder preestablecer el envío de mensajes. En este no es de importancia quien envía la solicitud por lo tanto si un ciberdelincuente accede a la red seguirá los comandos como si estos fueran legítimos. También existen los llamados Skimmers los cuales son dispositivos electrónicos establecidos en las ranuras de los cajeros para tarjetas de crédito, estos buscan copar los datos de dicha tarjeta obteniendo el pin del usuario. Una de las formas más comunes es colocar un lector falso sobre el verdadero para evitar que el usuario se percate de la operación fraudulenta. Los ciberdelicuentes cada día buscan nuevas metodologías para estafar o ya sea obtener información importante valiéndose de técnicas de ingeniería. Uno de los más conocidos es el phishing por medio de correos, llamadas telefónicas y otros. Los correos contienen links que redirigen al usuario a páginas web que suelen ser clonadas pidiendo ingresar usuario y contraseña, además de otros datos que están vinculados con sus tarjetas de crédito vulnerando de esta manera a los dos factores de autenticación utilizadas por muchas instituciones[51].

Finalmente, en la actualidad existen diversos tipos de métodos de autenticación, sin embargo, a pesar de los esfuerzos y recomendaciones que se hacen al respecto, siempre la información y los datos se encuentran vulnerables ya que, en ocasiones, para facilitar las tareas se suelen omitir o no implementar adecuadamente los métodos disponibles y recomendados lo que lleva a un potencial peligro para los datos que se proporcionan en las aplicaciones móviles para sistemas Android e IOS. La autenticación en varios pasos es una aproximación en niveles, para acceder a recursos o a información cada vez más sensible. Se irá accediendo de forma secuencial realizando una autenticación cada vez que se acceda a un nivel. Cada nivel de autenticación permite el acceso con mayores privilegios que los niveles anteriores, hasta obtener el nivel de privilegios deseado En este caso, cada nivel de autenticación puede utilizar un solo factor o MFA. Un ejemplo común de autenticación en varios pasos se da cuando un solicitante puede acceder a un recurso haciendo uso de una contraseña, pero el sistema requiere una autenticación adicional (por ejemplo, un código OTP) para realizar cambios de configuración o de credenciales. La autenticación en varios pasos mejora la seguridad respecto al uso de un solo factor, ya que añade protección adicional para accesos a acciones privilegiadas o a información sensible. Sin embargo, si no se requieren acciones privilegiadas y existe un solo nivel de acceso, presentará la misma debilidad que el uso de un solo factor[51].

[51] Arias, N. A. (2019). Análisis de seguridad de vulnerabilidades y ataques presentados en 4 dispositivos de Internet de las cosas. [Monografía]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/33326.

7. VULNERABILIDADES DE LOS MODELOS DE AUTENTICACION 2FA Y MFA A TRAVES DE LOS DIFERENTES MECANISMOS DE PROTECCION DE LA INFORMACION PARA VALIDAR EL NIVEL DE SEGURIDAD EN EL MANEJO DE LAS PLATAFORMAS.

El proceso de detección de vulnerabilidades en los métodos de autenticación permite que los procesos de seguridad de las aplicaciones móviles se optimice constantemente, además le brinda la posibilidad a los usuarios de seleccionar los dos factores de autenticación que desean implementar para proteger su información, siendo los más utilizados por ellos la contraseñas o pines y la detección biométrica, mientras que en las redes sociales y aplicaciones se ha recurrido a un sistema multifactorial, donde se mezclan la información de los usuarios, los OTPs y los elementos biométricos para poder acceder a ellas.

Entendiéndose esta vulnerabilidad como fallos en la seguridad del sistema[52], se puede establecer que a pesar de que elementos utilizados juntos conforman un sistema fuerte de seguridad, individualmente estos pueden ser vulnerables a ataques o accesos no autorizados arriesgando la información de los usuarios.
Pero para establecer las debilidades de cada uno de estos sistemas es necesario analizarlos individualmente para que el usuario determine cuál de estos es el más útil para proteger su información. Es así como algunas debilidades identificadas son:

Para el sistema basado en la información que solo el individuo conoce la principal debilidad es que, al solicitar una contraseña extensa y con una combinación de números, letras y signos especiales, los usuarios recurren a guardarlas en lugares visibles o se la comentan a amigos y familiares, exponiendo y debilitando la seguridad que estas contraseñas poseen, además los sistemas basados únicamente en este modelo han facilitado los ataques, robos y filtraciones de información de los usuarios y dueños de dispositivos móviles, además de que es recurrente el olvido de esta información.

No obstante, este no es el único mecanismo que presenta vulnerabilidades, aunque es el más usado y por ende el más alarmante, el sistema biométrico también posee puntos débiles ya que para poder utilizarlo se requiere que los dispositivos cuenten con las actualizaciones y características físicas específicas.
Así mismo, los elementos de autenticación son vulnerables a la conexión de redes móviles o wifi abiertas o el descargar aplicaciones en fuentes poco seguras ya que no

[52] ESCOBAR MARTÍNEZ, Jorge Iván y QUINTO ROJAS, Luis Carlos. Vulnerabilidad en dispositivos móviles con sistema operativo Android. Cuaderno Activa, 2015, vol. 7, p. 55-65.

advierten o protegen la información del acceso que terceros pueden tener a la interfaz del dispositivo Android[53].

Por otro lado, es necesario aclarar que la vulnerabilidad a la que se enfrentan los usuarios no es únicamente por la falta o mal uso de los factores de autenticación, sino que también se debe adicionar que muchos usuarios realizan la instalación de aplicaciones desde galerías de aplicaciones piratas que en muchos casos poseen virus que dañan, eliminan o filtran la información de los dispositivos móviles[54.]

	SEGURIDAD PLATAFORMAS DIGITAL	
MODELO	**VENTAJAS**	**DESVENTAJAS**
MFA	• La capacidad de autenticar dispositivos fuera del lugar de trabajo. • Detección temprana de intentos de inicio de sesión sospechosos y mayor seguridad. • Ahorra costos • Menor riesgo de robo de identidad y fraude. • Rompe el ciclo de phishing	• Es necesario un teléfono para obtener un código de mensaje de texto. • los tokens de hardware pueden perderse o ser robados. • los teléfonos pueden perderse o ser robados. • los datos biométricos calculados por los algoritmos MFA para las identificaciones personales, como las huellas digitales, no siempre son precisos y pueden generar falsos positivos o negativos. • la verificación de MFA puede fallar si hay una interrupción de la red o de internet. • las técnicas de MFA deben actualizarse constantemente para proteger contra los delincuentes que trabajan incesantemente para romperlas.
2FA	• Extra de seguridad a todas las cuentas o perfiles. • Está disponible e incluida en una gran	• Implica dedicar que unos segundos más para acceder en la cuenta cada vez que sea necesario. • No es infalible.

[53] Ibid, p60.
[54] Ibid, p61

	cantidad de servicios que usamos cada día como Instagram, Facebook y otras webs o tiendas online como es la propia Amazon. • Permite recibir el código de autenticación en dos pasos. En caso de no ser el usuario significaría que hay alguien que está tratando de acceder sin permiso.	• Costo. Si bien es relativo a la organización, inevitablemente un sistema de autenticación de dos factores implicará algún costo adicional y para las organizaciones más pequeñas, eso puede ser restrictivo

7.1 METODOLOGÍAS Y TÉCNICAS UTILIZADAS POR LOS CIBERDELINCUENTES

- **Phising**

  El phishing consiste en usurpar la identidad de una empresa u organización gubernamental. Se hacen llegar correos electrónicos a la víctima con un enlace a una página aparentemente legal, pero en realidad es duplicada, en donde piden datos personales para después cometer el fraude.

- **Vishing y smishing**

  Estas dos prácticas son variantes del phising. En el primer caso, el vishing, se usan mensajes de texto SMS fraudulentos para obtener datos personales de la víctima y, en el segundo, en cambio, se obtiene los datos mediante llamadas telefónicas o mensajes de voz.

- **Pharming**

  Es la práctica de suplantar el dominio de un sitio web. En este caso, se dirige al usuario a un sitio falso, con apariencia prácticamente igual al que es de su interés acceder, en el que se captura la información confidencial de la víctima.

- **WiFi público**

  Pocos establecimientos no tienen conexión a WiFi actualmente, a pesar de que esto pueda resultar ventajoso para aquellos que no tienen datos móviles, estas

redes no son del todo seguras y pueden usarse para acceder a los datos de los diferentes dispositivos. Los expertos recomiendan usar los datos siempre que sea posible, sobre todo si se van a realizar pagos.

- **Man in the middle**

  Este ataque informático suele afectar sobre todo a las empresas y puede suponer un gran daño económico. Los ciberdelicuentes suelen espiar las transacciones realizadas por las compañías y cuando detectan una que les interesa, mandan un correo fingiendo ser la otra empresa a la que realizan la transferencia y les informan de que supuestamente han cambiado de número de cuenta para recibir ellos el dinero.

- **SIM swapping**

  Los ciberdelicuentes pueden duplicar la tarjeta SIM de los móviles para robar dinero a los usuarios. En concreto, esto se hace para obtener el código de confirmación que envían los bancos a través de SMS cuando realizamos transferencias bancarias.

7.2 VULNERABILIDADES DE LOS MFA

Si bien son los sistemas de MFA son más seguros que los mecanismos de autenticación simple, éstos no son infalibles. Existen muchos tipos de ataques y de hecho muy ingeniosos para poder burlar a estos sistemas. Los cibercriminales pueden acceder a los mensajes de distintas formas y una de las más extravagantes es explotando un error en el protocolo SS7 utilizado por las compañías de telecomunicaciones para coordinar el envío de mensajes. Se trata de un conjunto de protocolos de señalización telefónica empleado en la mayor parte de redes telefónicas mundiales. Otra forma conocida son los llamados skimmers, estos son dispositivos electrónicos que son colocados en aquellas maquinas que tienen una entrada de tarjeta de crédito, como por ejemplo un cajero automático, una estación de carga automática de combustible para engañar a las personas que lo utilizan. También se destaca la clonación de huellas dactilares y el phishing en el cual el estafador se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, atacando al eslabón más débil de la cadena de seguridad que es el usuario por lo general enviándole un correo electrónico, o por algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas.

7.3 VULNERABILIDADES DE LOS 2FA

Independientemente del método utilizado para autenticar con un segundo factor, se sigue estando vulnerables. Cuando se inicia sesión en un sitio web, se le envía al servidor responsable de servir la página y de atender la petición de inicio de sesión con usuario y contraseña. El servidor comprueba la información de acceso con la que ya tiene y, si todo es correcto, otorga acceso.

Al otorgar este acceso, el servidor instala en el navegador web del usuario una cookie de sesión de usuario autenticado. Esta cookie es un “recordatorio” para el servidor, que trata al navegador que la tenga instalada como autenticado. Si un atacante consigue dicha cookie de sesión y la inserta en otro navegador el ataque podría comenzar como un ataque phishing en el que la víctima recibe un enlace malicioso. Este enlace lleva a la página de inicio de sesión que el atacante estime oportuno a través de un proxy. Es decir, la víctima verá por su navegador el sitio web original al que quiera acceder, no una copia. Lo que sucede en este caso es que el tráfico se redirige a través de la máquina del atacante (man-in-the-middle). Cuando la víctima se autentique ante el servicio, el atacante podrá interceptar las credenciales junto con la cookie de sesión, lo que le otorga acceso inmediato a la cuenta de la víctima.

No obstante, conviene resaltar que este ataque fallaría en caso de que el servicio web controle la multi-sesión, no permitiendo que el usuario se conecte a través de más de un dispositivo simultáneamente, puesto que el intento de Loguin con la cookie robada provocaría que se destruyese la sesión.

En la actualidad, se considera que uno de los mayores activos tanto para las empresas como para los usuarios es la información, es por esto que la búsqueda de métodos o herramientas que permitan obtener una mayor veracidad de ella mientras se garantiza su seguridad y protección, ha cobrado un gran protagonismo. Aun así, a pesar de todos los esfuerzos que los desarrolladores y usuarios realizan para proteger los datos e información importante, siempre se encuentra la amenaza de un ataque cibernético, el robo o pérdida de información debido al acceso de terceros no autorizados, quienes han buscado y diseñado estrategias que burlan los diferentes sistemas de seguridad que se desarrollan.

Lo anterior se anuda al hecho de que en los dispositivos móviles y aplicaciones se deposita una mayor cantidad de información delicada puesto que, debido a la necesidad de adaptarse a las nuevas exigencias del medio, se han creado nuevos ambiente

virtuales que anteriormente solo existían en la presencialidad, tales como el denominado banca móvil, que hace referencia al nuevo espacio que ha decidido implementar el sector bancario para agilizar y facilitar los procesos para sus usuarios, lo que se ha traducido en la necesidad de introducir información que, en años anteriores, no se hubiera pensado ingresar como lo son las claves bancarias, números de identificación y direcciones.

Es por esto que, tanto servidores como aplicaciones móviles han considerado necesario la aplicación de un mayor número de herramientas que permitan garantizar una autenticación y seguridad mayor, es por esto que se desarrolla el término 2FA o autenticación multi-factor, que hace referencia a la implementación de dos o más factores de autenticación para el acceso a los servidores o inicio de sesión en una página web o aplicación.
Es así que se ha dado lugar a la consideración de nuevos aspectos incluyendo la lectura y reconocimiento de elementos biométricos, como las huellas dactilares y el reconocimiento facial, además de la implementación de OTP's que son códigos que son enviados vía correo electrónico o vía telefónica (mensajería o llamada) y que permite validar la información del ingreso, siendo unos de los más utilizados por las aplicaciones y en los dispositivos móviles además del factor básico que se caracteriza por la combinación de información de usuario y una combinación alfanumérica que es utilizada como contraseña de acceso.

Sin embargo, el desarrollo e implementación de ese modelo de factores significa para los desarrolladores y usuarios la necesidad de realizar una inversión para mejorar o cambiar los factores que se están utilizando actualmente, siendo en los usuarios la necesidad de adquirir nuevos dispositivos más actualizados mientras que los desarrolladores de aplicaciones móviles deben adquirir y desarrollar servidores que posean los factores de autenticación necesarios para garantizar la seguridad y almacenamiento de los datos que proporcionan los usuarios durante el registro y uso de la aplicación.

Los elementos antes mencionados pueden significar una dificultad en el desarrollo e implementación de estos factores puesto que en muchos casos no se poseen los recursos necesarios para ellos o los cambios que deben realizarse requieren una mayor inversión ya que se deben realizar modificaciones en aspectos adicionales para garantizar el correcto funcionamiento de dichos factores.
Del mismo modo, mediante la revisión se identificaron algunos otros aspectos que dificultan o disminuyen la efectividad de los modelos de autenticación, resaltando el papel que juegan los propios usuarios en esto, puesto que el compartir las calves de seguridad o dejarlas en lugares accesibles a terceros, o la no implementación de un factor que proporcione seguridad extra, son acciones comunes que, a pesar de percibirse

inofensivas, al caer en las manos equivocadas puede convertirse en una amenaza considerable para la privacidad e información personal que se almacenen en las aplicaciones y en el dispositivo, la cual puede ser utilizada, alterada o eliminada por estas personas.
Cabe resaltar que este no ha sido el único aspecto identificado que puede debilitar estos la seguridad que proporcionan estos factores ya que la instalación de aplicaciones de páginas no oficiales le abre la puerta a Malware que pueden dañar o robar la información del usuario, asimismo se encuentra el hecho de que en muchos casos únicamente es utilizado un solo factor o método de autenticación para el ingreso a las aplicaciones móviles y al propio dispositivo, esto a pesar de los esfuerzos que realizan los desarrolladores para el uso de otros factores de autenticación como los OTP's, la identificación de imágenes o el uso de contraseñas adicionales.

Aunque todavía es objeto de estudio las razones por la cual evitan el uso de factores de autenticación, en la información revisada se evidencia que uno de los elementos que detonan esos aspectos antes mencionados se encuentra relacionada al olvido constante de las contraseñas lo que lleva a la necesidad de escribirlas o compartirlas con terceros, algo a rescatar de esto es que ha motivado el desarrollo de dispositivos móviles que permitan más de un factor e autenticación, adicionando los lectores de huellas y el reconocimiento facial como medios de apoyo para solventar estas debilidades en la seguridad de los dispositivos, permitiendo ganar más eficiencia y facilitando las actividades de los usuarios.

Por otro lado, en cuanto a la metodología implementada en esta investigación se resalta el hecho de que en el margen de tiempo establecido, la mayor parte de la literatura encontrada en español han sido el resultado de tesis de investigación para la obtención de estudios postgrado y poseen un carácter exploratorio, lo que ha genero una mínima dificultad para encontrar información sobre los nuevos factores de autenticación que se están implementando y cuáles son las debilidades identificadas en ellos, lo que dificultó un poco la indagación sobre estos y generó la necesidad de realizar la búsqueda en base de datos en el idioma inglés.

7.4 INGENIERÍA SOCIAL CONTRA LA 2FA

El problema llega cuando también surgen métodos capaces de romper la autenticación de dos factores. Los piratas informáticos pueden hacer uso de la ingeniería social para lograr sus objetivos y poder entrar así en las cuentas de los usuarios incluso cuando han habilitado la 2FA para protegerse.

Generalmente la autenticación en dos pasos consiste en un código en el que se recibe por SMS. Ese código permite posteriormente iniciar sesión en una cuenta o acceder a un dispositivo. Sin embargo esto abre la puerta a la ingeniería social, como así ha ocurrido en algunos casos.

Un posible pirata informático podría obtener los datos de la víctima y hacerse pasar por ella de cara a la operadora móvil, por ejemplo. Podría solicitar un nuevo envío de una tarjeta SIM por pérdida. Es cierto que esto está controlado, al menos sobre el papel, pero no hace que sea imposible que ocurra.

Con la tarjeta SIM de la víctima los ciberdelicuentes podrían recibir los códigos de autenticación de dos factores al móvil. Tendría por tanto el control total de sus cuentas.

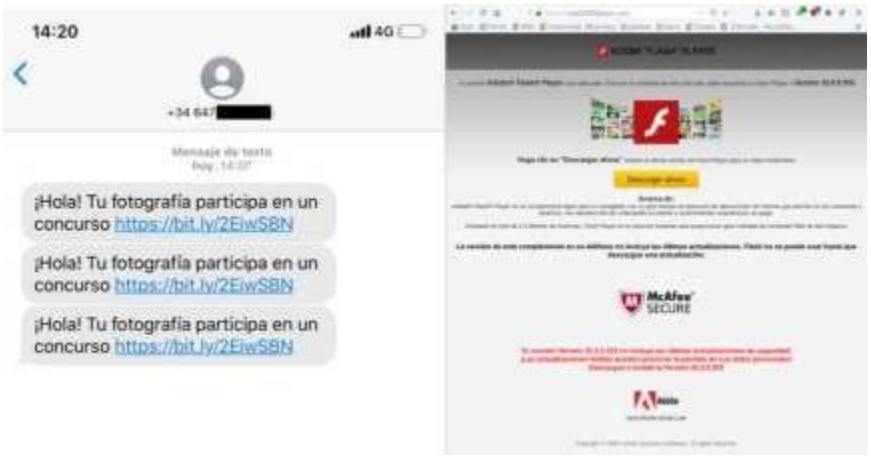

Ilustración 4.SMS como vector de ataque.
Fuente: ALBORS, Josep. AUGE DE LOS MENSAJES SMS COMO VECTOR DE ATAQUE. Disponible en: https://blogs.protegerse.com/2021/05/17/auge-de-los-mensajes-sms-como-vector-de-ataque/. 2019.

Otro método que podrían utilizar relacionado con la ingeniería social es la instalación de aplicaciones fraudulentas. Pueden hacer creer a la víctima que se trata de software legítimo, pero en realidad podría tener intereses ocultos. Podría, llegado el momento, reenviar todos los SMS que el usuario recibe a un dispositivo controlado por el pirata informático. De esta forma también podrían recibir el código de 2FA para poder acceder a nuestras cuentas.

7.5 INGENIERÍA SOCIAL CONTRA LA MFA

Una autenticación multifactor o MFA por sus siglas en inglés, se ha convertido en una necesidad para poder prevenir ataques, reduciendo el éxito que pueden tener los ciberdelicuentes. El doble factor de autenticación se ha convertido en el próximo campo de batalla de los atacantes, donde la guerra ha sido complicada, debido principalmente a

los errores de configuración o implementación que abren la puerta para eludir estos controles.
Algunos de los métodos utilizados para eludir estos controles son los siguientes:

- **Ingeniería social para evitar el MFA.** Los atacantes dependen de este engaño en gran medida para que los objetivos hagan click en enlaces y/o archivos adjuntos, correos de phishing, o revelen contraseñas en línea o vía telefónica. Muchos expertos en ingeniería social aprovechan esto para burlar el MFA.

- **Ataques BEC.** en muchas ocasiones, este tipo de ataques son exitosos cuando no se tiene una política de MFA implementada, lo que facilita a los atacantes robar las credenciales.

- **SIM Swapping.** Esta técnica hace uso de un dispositivo comprometido, regularmente celulares, esta se puede lograr a través de la ingeniería social donde el objetivo accede a intercambiar la SIM de su equipo, este es un ataque muy común para eludir los controles MFA.

- **Malas configuraciones y fallas.** Además de las configuraciones incorrectas, la falta de implementación de MFA en todos los puntos de acceso remoto en una empresa deja una puerta abierta para los atacantes.

8. MECANISMOS DE PROTECCION Y DEFENSA EN PLATAFORMAS DIGITALES

Los factores actualmente existentes hacia los consumidores producen necesidades hacia nuevos productos, así como el libre acceso de servicios por medio de plataformas electrónicas, esto ha impulsado el uso continuo de datos personales, sin embargo por medio de las normas legislativas se ha venido estableciendo una serie de mecanismos que ayudan a proteger uno de los derechos citados en el artículo 15 de la constitución política colombiana , la cual estipula lo siguiente : “todas las personas tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución”.
La anterior citación hace referencia al derecho existente en Colombia sobre el Habeas Data, ya que este se considera a nivel de categoría constitucional.

Es importante destacar el manejo de la información y la transferencia de la misma ,a través de la Protección de Datos de la Superintendencia de Industria y Comercio, la cual ejerce funciones de Control y sanciones en asuntos relacionados con la protección de la Información, perteneciente a la Red Ibero latinoamericana de Protección de Datos (RIPD) y de la cual hacen parte 24 países de la región y que desde hace algunos años se han dedicado a redactar y publicar Estándares para la Protección de Datos cuyos objetivos son los siguientes:

- Establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región.

- Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales.

- Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región.

8.1 NIVELES DE SEGURIDAD INFORMÁTICA

Los niveles de seguridad informática son establecidos según una serie de factores que definen el grado de madurez en seguridad o de confianza de las TIC de una empresa u organismo

El primer estándar desarrollado para medir el nivel de seguridad informática fue el TCSEC (Trusted Computer System Evaluation Criteria), del Departamento de Defensa de los Estados Unidos, y define siete niveles distintos de seguridad:

- Nivel D1: El sistema no es seguro, ya que no cumple con ninguna especificación de seguridad. No dispone de protección del hardware ni autenticación de los usuarios.

- Nivel C1: Se implementa un mecanismo de control de acceso laxo para la identificación y autenticación de los usuarios. Se distingue entre administradores del sistema y usuarios normales.

- Nivel C2: Aplica un mecanismo seguro de control de acceso de los usuarios e implementa registros de auditoría.

- Nivel B1: Incorpora un mecanismo de seguridad jerárquico o multinivel asignando etiquetas para ello a los distintos objetos del sistema, tanto a los datos como a los usuarios.

- Nivel B2: Sistema de seguridad estructurado, en el que se etiquetan los objetos del sistema de nivel superior con respecto a los del inferior.

- Nivel B3: Se incluyen dominios de seguridad y distintas políticas de acceso, gestionadas de manera centralizada y con un control de acceso seguro implementado.

- Nivel A: El sistema implementa mecanismos de seguridad para el control y la verificación mediante métodos matemáticos. Este es el máximo nivel de seguridad de un sistema.

9. CONCLUSIONES

Finalmente, de la investigación y revisión de literatura se puede resaltar que, en la mayoría de las publicaciones revisadas, existe la necesidad de que los usuarios implementen más de un método de autenticación al ingresar a las plataformas online para que la probabilidad de acceso de terceros no autorizados se disminuya, aumentando la seguridad de la información.

Por otro lado, es necesario resaltar que los factores de autenticación más utilizados en un modelo 2FA son: la información de usuario y contraseña, la lectura de huellas dactilares o el escaneo facial y el uso de OTP's, quienes, entre sí, suponen la construcción de un fuerte sistema de seguridad y autenticación. Esto ya que en la actualidad la vulnerabilidad que existe se debe a diversos factores, como las características de cada uno de estos factores, el tipo de información que se desee proteger, la plataforma a utilizar y los recursos e intereses del usuario.

Se encontró que una de las debilidades que presentan las plataformas online en Colombia, es que muchas de estas solo presentan un solo factor de autenticación, lo que implica un mayor índice de vulnerabilidad, puesto que en la cotidianidad los usuarios recurren a fuentes poco confiables para descargar aplicaciones o se conectan a redes Wifi-abiertas, que pueden ser la puerta de entrada de virus o terceros que pueden acceder, alterar o eliminar la información que se tiene en los dispositivos.

Esto ha significado la necesidad de la elaboración y fortalecimiento de los factores de autenticación, buscando garantizar una mayor protección de la información, es por esto que con la implementación de sistemas de seguridad más robustos se busca garantizar una mejor experiencia a los usuarios, agregando el reconocimiento facial con la cámara frontal y la lectura de las huellas digitales mediante la adición de lectores dactilares, puesto que el solo utilizar un método de seguridad ha demostrado ser insuficiente en la protección ante robo o pérdida de información en cualquier tipo de plataforma.

Por otra parte, durante la elaboración de la revisión literaria se halló que en los últimos años la investigación e interés ha aumentado, enfocándose en la aplicabilidad de dos factores en el proceso de autenticación, planteando las ventajas y desventajas de cada uno de ellos y planteando los retos a los que se enfrenta para poder obtener cambios y mejoras en la seguridad de la información en plataformas de red y dispositivos electronicos, ya que, con el nuevo ambiente que han adaptado la comunidad bancaria, escolar y de la salud, en ellos se recopila una gran cantidad de información personal valiosa como los números de identificación, las tarjetas y cuentas bancarias, los

historiales médicos y los horarios e información académica, siendo información de gran interés para los hackers y ladrones cibernéticos.

Por último, si es necesario tener en cuenta de que estos no son los únicos elementos de autenticación que existen, puesto que las tarjetas con chips, dispositivos USB y credenciales también se utilizan como medios de identificación y autenticación, sin embargo, la utilización de estas requiere el manejo de componentes específicos y son mayormente utilizado por las empresas para que sus empleados puedan acceder remotamente a una interfaz para realizar su trabajo.

9. RECOMENDACIONES

Para trabajos futuros y para el uso de un método de 2FA se realizan las siguientes recomendaciones:

- Restringir el acceso a terceros en procesos que implican información de alto nivel, como es el caso de contraseñas y datos personales con el fin de disminuir la pérdida o filtración de información privada.

- Realizar ingresos a plataformas de red principal y no conceder acceso a permisos de páginas desconocidas.

- Cambiar de manera regular los métodos de autenticación que se utilizan para acceder a las redes sociales y a las demás plataformas online, donde se tenga una cuenta registrada, además de los métodos de seguridad para el acceso a estas.

- Considerar aspectos culturales y personales en estudios futuros sobre cuáles son los factores de autenticación más utilizados en una población determinada ya que fue poca la documentación encontrada que permitieran el acceso de este tipo de información.

- Para la elaboración o el planteamiento de futuros factores de autenticación, es necesario tener en cuenta el riesgo que representan las conexiones Wifi-abiertas.

- Para proteger los archivos en los dispositivos a la ora de ingresar a una plataforma online se recomienda cifrarlos para dificultar o impedir el acceso de terceros, activando las herramientas de doble autenticación como la creación de un OTP y la identificación dactilar o facial.

- Se recomienda la instalación de antivirus verificados para aumentar la seguridad de cualquier dispositivo electrónico para el respectivo ingreso de plataformas online.

10. BIBLIOGRAFIA

ALOU, F., ZAHIDI, S., EL-HAJJ, W. *Two factor authentication using mobile phones. In: International Conference on Computer Systems and Applications IEEE/ACS.* 2009,pp. 641–644

ALTINKEMER, Kemal; WANG, Tawei. *Cost and benefit analysis of authentication systems. En: Decision Support Systems.* 2011, vol. 51, no 3, p. 394-404.

ANDRESS, Jason. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice. En: Syngress Publishing.* 2011, p 240.

BONNEAU, Joseph, *et al.The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. En: IEEE Symposium on Security and Privacy,* 2012.

CABALLERO, MARÍA ÁNGELES Y CILLEROS SERRANO, DIEGO. *El Libro del Hacker. Editorial Anaya*. 2012.

CAMPO RUIZ, Asunción. *La digitalización del sector bancario, En: Revista Scielo. M*ayo, 2019.

CIFUENTES DÍAZ, Erick Fabricio., MARTÍNEZ VÁSQUEZ, Maikol Estiven. *Biohacking para la protección de los activos de información en las pymes por medio de un sistema de doble factor de autenticación. En: Tesis de especialización. Universidad Católica de Colombia.* 2019.

COLOMBIA. CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 23 (28 de enero de 1984. Sobre derechos de autor [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 1984. Nro. 35.949. Disponible en: https://www.habitatbogota.gov.co/transparencia/normatividad/normatividad/ley-23-1982#:~:text=Regula%20los%20derechos%20morales%20y,Marco%20Legal%20de%20la%20Entidad.

COMUNIDAD ANDINA. LA COMISIÓN DEL ACUERDO DE CARTAGENA. Decisión Andina 351 (17 de diciembre de 1993). Se decide aprobar el régimen común sobre derecho de autor y derechos conexos [en línea]. Disponible en: http://derechodeautor.gov.co:8080/decision-andina

CRESPO M. A, Y RAMOS, R. E *Estudio del impacto financiero de las vulnerabilidades de las páginas Web de los bancos en Ecuador. En: Tesis obtención de título. Universidad Politécnica Salesiana. Guayaquil.* 2012.

DASCALESCU, ANA. *Biometric Authentication Overview. En: Advantages & Disadvantages.* 2017.

DEO, Shaneel y FARIK, Mohamed. *Information Security - Recent Attacks in Fiji Techtarget. En: International Journal of Scientific & Technology Research.* 2016, Vol. 55

Dutta, N., Sarma, H.K.D., Polkowski, Z. *Cluster based routing in cognitive radio adhoc. En: networks: reconnoitering SINR and ETT impact on clustering. Comput. Commun. 2018,* 115, 10–20.

Edna Elizabeth, N., Nivetha, S.: *Design of a two-factor authentication ticketing system for transit applicationS. En:IEEE Region 10 Conference (TENCON), Singapore*. 2016, pp. 2496–2502.

Eldefrawy, M.H., Alghathbar, K., Khan, M.K.: OTP-*based two-factor authentication using mobile phones. En: Eighth International Conference on Information Technology: New Generations*. 2011. pp. 327–331

ESCOBAR MARTÍNEZ, Jorge Iván y QUINTO ROJAS, Luis Carlos. *Vulnerabilidad en dispositivos móviles con sistema operativo Android. Cuaderno Activa.* 2015, vol. 7, p. 55-65.

FORTUNY, Sabartés, *Digitalización de historias clínicas y seguridad del proceso. En: papeles médicos.* 2010, vol. 19, no 2.

GÉNERO, Marcela; CRUZ LEMUS, Jose. y PIATTINI, Mario. *Métodos de investigación en ingeniería del software. RAMA Editorial.* 2014, p.314. ISBN: 9789587624304

GONZÁLEZ ARRIETA, Angélica*. Llaves FIDO (Fast IDentify Online) como segundo factor de autenticación en la gestión on-line de los procesos de enseñanza y aprendizaje*. 2018.

GONZÁLEZ, *G Software de desarrollo para aplicaciones móviles. En: Universidad Veracruzana*. 2012.

GUERRERO RAMÍREZ, Javier*. Autenticación de doble factor mediante OTPs. Tesis Maestría. Universitat Oberta de Catalunya. 2019.*

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). ICONTEC. Documentación, presentación de tesis, trabajos de grado y otros trabajos de investigación, 2008. NTC-1486 [En línea]. Bogotá D.C: Instituto colombiano de normas técnicas y certificación (Icontec).

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Referencias bibliográficas. Contenido, forma y estructura, NTC 6166, (2016). [En línea]. Bogotá D.C: Instituto colombiano de normas técnicas y certificación (Icontec).

ISRAA M. ALSAADS. *Physiological Biometric Authentication Systems, Advantages, Disadvantages and Future Development. En: International journal of scientific & technology.* 2004, *v*olumen 4.

KITCHENHAM, B, CHARTERS S, *Guidelines for performing systematic literature reviews in software engineering. Technical report, Keele University*. 2007.

Kumar, D., Agrawal, A., Goyal, P.: *Efficiently improving the security of OTP. En: International Conference on Advances in Computer Engineering and Applications, Ghaziabad.* 2015, pp. 912–915.

MANTOVANI, Valentino. *Autenticación de Múltiples factores (MFA). En: Trabajo de grado. Universidad de Buenos Aires, Facultad de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería.* 2004.

MIFSUD, E. *Introducción a la seguridad informática - Seguridad de la información/Seguridad informática.* 2012.

ÑIQUE, Víctor*, Implementación De Solución De Autenticación Segura Basada En Doble Factor En Una Entidad Del Estado. En: trabajo de grado. Universidad San Ignacio de Loyola, Facultad de Ingeniería.* 2006.

Park, W., Hwang, D., Kim, K.: *A TOTP-based two factor authentication scheme for hyperledger fabric blockchain. En: Tenth International Conference on Ubiquitous and Future Networks (ICUFN*), Prague, pp. 817–819, 2018.

Rodrigues, B., Chaudhari, A., More, S*.: Two factor verification using QR-code: a unique authentication system for Android smartphone users. En 2nd International Conference.* 2016.

RODRÍGUEZ POVEDA, Alcibíades*. Seguridad aplicada en los procesos transaccionales de las aplicaciones móviles. En: Universidad Piloto de Colombia.* 2018.

RODRIGUEZ VALDES, Osviel; LEGON, C.M. Y SOCORRO LLANES, Raisa. *Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica. Rev cuba cienc informat*. 2018, vol.12, suppl.1, Pp.13-27.

Sathwara, S., Dutta, N., Pricop*, En: IoT forensic a digital investigation framework for IoT systems. En: IEEE International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. 2017, Romania, pp. 1–5

SECLÉN ARANA, Javier Alfonso. *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001. En: (Tesis de maestría). Universidad Nacional Mayor de San Marcos. Facultad de Ingeniería de Sistemas e Informática*, 2016.

SILVELO PALLÍN, Arturo. *Sistema de autenticación biométrica basado en el análisis del comportamiento mediante interacción por pantalla táctil y sensores de movimiento. En: Tesis de Pregrado,* Universidad Da Coruña. 2018.

SINGH, Ajay, y MASUKU, Micah. *Sampling Techniques & Determination of Sample Size in Applied Statistics Research: An Overview. En: International Journal of Economics, Commerce and Management.* 2014, Vol 11, no 2, p. 1-22.

Shah, S.U., Fazl-e-Hadi, Minhas, A.A.: *New factor of authentication: something you process. In: International Conference on Future Computer and Communication.* 2009, Kuala Lumpur, pp. 102–106.

Universidad Internacional Sek. *Facultad de Ingeniería. En Reconocimiento de Similitud de Imágenes. En: Tesis de Maestría*. 2019.

VELÁSQUEZ LAGOS, Ignacio Andrés. *Framework para la Comparación y Selección de Esquemas para la Autenticación Multi-Factor. En: tesis de Maestría. Universidad del Bio-Bio.Facultad de Ingeniería*. 2019.

VIEITES, Álvaro*. Enciclopedia de la Seguridad Informática. Grupo Editorial RA-MA.* , 2011. 2 a edición.

ZDENEK RÍHA Y VÁCLAV MATYÁŠ. *Biometric Authentication Systems. En: Masaryk University.* 2006.