Uniandes EPISTEME. Revista digital de Ciencia, Tecnología e Innovación
ISSN 1390-9150/ Vol. 8 / Nro. 2 / enero-abril / Año. 2021 / pp. 211-234

ARTÍCULO DE REVISIÓN

CIENCIAS SOCIALES

Ciberseguridad en las redes sociales: una revisión teórica

Cybersecurity in social media: a theoretical review

Martínez Chérrez, Whymper Eduardo [I]; Ávila Pesantez, Diego Fernando [II]

[I.] whymper.e.martinez.c@pucesa.edu.ec. Maestría en Ciberseguridad. Pontificia Universidad Católica del Ecuador, Ambato, Ecuador
[II.] davila@espoch.edu.ec. Facultad de Informática y Electrónica. Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador.

Recibido: 25/01/2021
Aprobado: 31/03/2021

Como citar en normas APA el artículo:
Martínez Chérrez, W. E., Ávila Pesantez, D. F. (2021). Ciberseguridad en las redes sociales: una revisión teórica. *Uniandes Episteme*, *8*(2), 211-234.

RESUMEN

Las redes sociales, constituyen una de las formas más novedosas de comunicación a nivel mundial. Su utilización es exponencial y paradójicamente a las innumerables ventajas que tiene, se evidencia un alto grado de vulnerabilidad, debido entre otros aspectos a los constantes ataques y amenazas de las cuales son objeto. El propósito de este estudio se concreta mediante la Revisión Sistemática de Literatura, permitiendo reflexionar sobre las teorías y aportes precedentes en relación con los ataques, vulnerabilidad y mitigación en las redes sociales. Los resultados del trabajo permitieron identificar 28 estudios potenciales desarrollados entre el 2012 y 2020. Derivado del estudio se sistematizaron tres teorías fundamentales: a) El impacto de las redes sociales en las formas actuales de comunicación; b) La alta incidencia de ataques y vulnerabilidad; c) El factor humano, el apoyo de la tecnología y las políticas, normativas y regulaciones. Como se resultado se obtuvo que los principales ataques son phishing, trolling y malware.

PALABRAS CLAVE: ciberseguridad; redes sociales; ataques; vulnerabilidad; mecanismos de seguridad.

ABSTRACT

Social networks constitute one of the newest forms of communication worldwide. Its use is exponential, and paradoxically to the innumerable advantages, a high degree of vulnerability

is evident due to other aspects to the constant attacks and threats to which they are subjected. The purpose of this study is specified through the Systematic Review of Literature, allowing reflection on the theories and previous contributions about attacks, vulnerability, and mitigation in social networks. The results of the work allowed the identification of 28 studies developed between 2012 and 2020. Three fundamental theories were systematized derived from the study: a) The impact of social networks on current forms of communication; b) The high incidence of attacks and vulnerability; c) The human factor, the support of technology and policies, standards, and regulations. As a result, it was obtained that the primary attacks are phishing, trolling, and malware.
KEYWORDS: cybersecurity, social networks, attacks; vulnerability, security mechanisms.

INTRODUCCIÓN

Los avances producidos en la ciencia y la tecnología, unidos a la globalización en las diferentes áreas y saberes han tenido un impacto importante en las formas de comunicación que se han venido empleando desde hace algunos años. Un ejemplo lo constituye el uso de las redes sociales, las cuales desde sus inicios captaron la atención de miles de usuarios que ante esta nueva experiencia fueron dejando atrás los métodos tradicionales o convencionales de comunicación para ir incursionando de forma progresiva y ascendente en estas modalidades (Rahman, Huang, Madhyastha & Faloutsos, 2016). Según Ciolan (2014) con la apertura de los nuevos canales de la información se ha logrado revolucionar tanto las formas de comunicación como las experiencias en su uso y empleo; cada día son más las personas que acceden al uso de las redes sociales en busca de alcanzar mayor rapidez, viabilidad y factibilidad en los diferentes procesos. Es por ello que la introducción de Facebook, Twitter, YouTube, LinkedIn e Instagram constituye sin lugar a dudas una de las formas más novedosas de comunicación.

En este orden de ideas es importante comprender ¿Qué son las redes sociales? ¿Cuáles son las más empleadas actualmente? ¿Qué público las utiliza? Con base a estas interrogantes iniciales se puede entender que cada red social tiene sus propios objetivos y alcances, por tanto, el lenguaje y formas de utilización van a estar determinados también por el tipo de público que haga uso de estas (Ikhalia, Serrano, Bell & Louvieris, 2019). Por otra parte, si se analiza desde una perspectiva holística e integral la relación entre las categorías beneficios y perjuicios, ocasionados por la introducción y crecimiento exponencial de estas formas de comunicación, se pudiera valorar de muy positivo el empleo de las redes sociales; precisamente porque estamos enmarcados en la nueva era del conocimiento. Sin embargo, no se puede dejar de considerar que conjuntamente con los altos beneficios que ha traído el uso de estas redes, también se han derivado importantes hechos que de manera general y

específica necesitan ser atendidos con carácter urgente. Alguno de estos se relaciona con los ataques, vulnerabilidad y mecanismos de seguridad en las redes sociales (Alufaisan, Zhou, Kantarcioglu & Thuraisingham, 2017).

Los estudios precedentes intentan afirmar una situación compleja; pues por un lado se encuentran los reconocidos beneficios del uso de las redes sociales y, por otra parte, la valoración y significación que ha tenido y tiene el empleo inadecuado de las redes sociales. Sobre todo, cuando se está en presencia de los múltiples ataques de phishing y de spam, esto por la alta vulnerabilidad que se da por no tener mecanismos adecuados para su manejo, o cuando no se hace un uso correcto que conlleven a buenas prácticas (Vishwanath, 2015). Todo esto se sitúa en la siguiente situación problémica: ¿Cómo perfeccionar los mecanismos de seguridad para mitigar los ataques y vulnerabilidad causada en las redes sociales? De la anterior situación problémica se deriva el propósito de esta investigación, la cual intenta reflexionar sobre las teorías precedentes en relación con los mecanismos de seguridad, que actualmente se emplean como una vía para mitigar los ataques y la vulnerabilidad del uso de las redes sociales. Finalmente, se establecen orientaciones que pueden ser tomadas en cuenta para reforzar los actuales mecanismos de seguridad, para contribuir a la mitigación de los ataques y vulnerabilidad en las redes sociales.

DESARROLLO

En este estudio, las pautas generales propuestas por Kitchenham & Carters se adaptaron para la RSL (Revisión Sistemática de Literatura), lo que permitió recoger pruebas empíricas sobre las preguntas de investigación formuladas. Para investigar este proceso, consta de tres fases principales: Planificación de la revisión, realización de la revisión y análisis (Keele, 2007).

Planificación de la revisión

Se enfoca en las principales amenazas, vulnerabilidades y los posibles mecanismos de seguridad que existen para mitigar los ataques en las redes sociales. Los investigadores coinciden que la información e inclusive la integridad física puede estar en riesgo si no se utiliza de manera correcta las diferentes aplicaciones, y además recomiendan tomar medidas básicas de seguridad. Por lo descrito anteriormente se realiza la pregunta general de investigación, ¿Cómo perfeccionar los mecanismos de seguridad para mitigar los ataques y vulnerabilidad causada en las redes sociales? Para responder a la pregunta planteada se elaboraron cuatro preguntas secundarias.

RQ1: ¿Cuáles son las principales modalidades de ataques y vulnerabilidades identificadas en las redes sociales?

RQ2: ¿Los actuales mecanismos de seguridad son eficientes ante los ataques y amenazas que se dan en las redes sociales?

RQ3: ¿Cuáles serían las posibles soluciones o los algoritmos a adoptar?

Para dar respuesta a las interrogantes planteadas se consultaron las bases de datos electrónicas Science Direct Elsevier, IEEE eXplorer Digital Library, Springer, Proquest y ACM, que incluyeron áreas asociadas a la ciencia como: Computación, Ingeniería y Tecnología. Se identificaron como fuentes de información revistas, congresos y actas. Se tomaron trabajos publicados entre enero 2012 y febrero 2020. La estrategia de búsqueda fue la siguiente: a) vulnerability social networks, b) social networks attacks, c) good practices Facebook, d) social networks malware, f) social networks fishing, g) social networks security ("vulnerability" AND "attacks" AND "social" AND "network").

Para afinar la selección de las obras, se aplicaron los criterios de inclusión y exclusión, y una revisión general del título. (Tabla 1)

Tabla 1. Criterios de selección

CRITERIO DE SELECCIÓN	CRITERIO DE EXCLUSIÓN
Ataques, metodologías de seguridad	Documentos con extensión .xml
Ciberseguridad en redes sociales, en adolescentes	Tesis
Privacidad en las redes sociales	Editoriales.
Buenas prácticas en el uso de las redes sociales.	Artículos publicados en sitios web

Realización de la revisión

En esta fase se estableció la selección de los artículos en base a los criterios de inclusión y exclusión. Se realizó el análisis del contenido de los documentos seleccionados, lo que permitió determinar su relevancia y contribución, de acuerdo a las preguntas de investigación que se plantearon. Como resultado de la búsqueda se identificaron 328 documentos, de los cuales se seleccionaron 28 por cumplir con los criterios establecidos anteriormente (Figura 1).

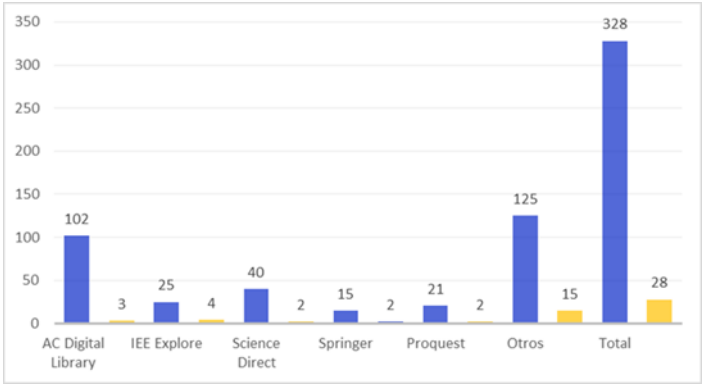

Figura 1. Artículos seleccionados en la base de datos electrónica

La figura 2 muestra la tendencia de las publicaciones; el histograma indica que en el 2019 se ha producido un aumento de los artículos relacionados con el tema, relacionado a la ciberseguridad en las redes sociales. Además, es evidente que a inicios del 2012 empieza a publicarse artículos relacionados al tema, donde indican que las redes sociales se han consolidado como herramientas de comunicación dentro de la sociedad.

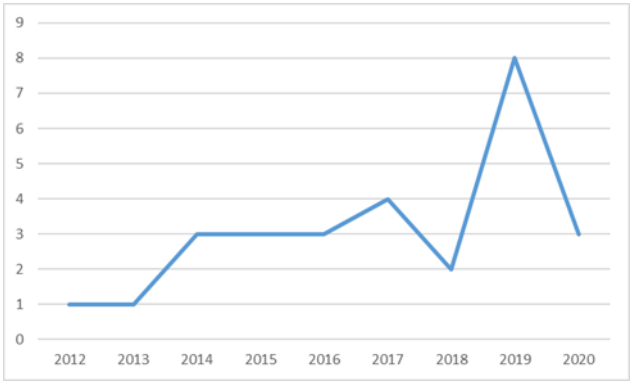

Figura 2. Actividad investigadora sobre ciberseguridad en las redes sociales

Análisis de la revisión

Teniendo en cuenta los documentos analizados, se procede a responder a las tres preguntas de investigación destinadas a determinar los ataques, vulnerabilidades y mecanismos de seguridad y posibles soluciones que se pueden aplicar para mitigar en las redes sociales los ataques, vulnerabilidades a que están expuestos.

RQ1: ¿Cuáles son las principales modalidades de ataques y vulnerabilidades identificadas en las redes sociales?

Para iniciar el análisis sobre este importante tema, se considera esencial entender el significado del término: redes sociales. Atendiendo a ello y asumiendo un concepto simple definido por Celaya (2008), y seguido por Herrera (2012), al señalar que las redes sociales son lugares en Internet donde las personas publican y comparten todo tipo de información, personal y profesional, con terceras personas, conocidos y absolutos desconocidos. Considera Herrera (2012) que más allá de las definiciones puntuales, semánticamente una red social se constituyen un espacio creado virtualmente para facilitar la interacción entre personas, las cuales independientemente de todos los avances alcanzados y del surgimiento de nuevas plataformas, seguirán siendo uno de los medios de comunicación masiva más importantes, debido a sus características (pág. 123). Actualmente, las redes sociales se han consolidado como herramientas de comunicación dentro de la sociedad, a través de las cuáles, tanto individuos como empresas, han logrado proyectar, informar, compartir y difundir información con públicos o grupos específicos.

Los autores citados anteriormente establecen tres clasificaciones o tipos principales de redes sociales:

- Redes profesionales (por ejemplo, LinkedIn, Xing, Viadeo)
- Redes generalistas (por ejemplo, MySpace, Facebook, Tuenti, Hi5)
- Redes especializadas (por ejemplo, Ediciona, eBuga, CinemaVIP, 11870.com)

En el Manual de Gestión y Buenas Prácticas en Redes Sociales, de la Pontifica Universidad Javeriana de Bogotá se identificaron las redes sociales más utilizadas, las cuales se listan a continuación (Bello & Mejía, 2019).

Facebook: Es la más grande red social consultada por los usuarios. Allí se encuentra la mayor diversidad de públicos, por tanto, hay que orientar de manera correcta cada publicación. Permite compartir texto, imágenes, videos, enlaces, álbumes de fotografías, historias y permite realizar transmisiones en vivo.

- Twitter: Es una plataforma social bidireccional, cuyo objetivo es compartir información de diverso tipo de forma rápida y sencilla. Su éxito se basa en la inmediatez de mensajes cortos, lo que la hace una red social para leer y escribir muy rápido. En el ámbito institucional, Twitter permite divulgar noticias, eventos, servicios, entre otros. Cabe recordar que es una red muy interactiva, para público externo y que las publicaciones no deben sobrepasar los 280 caracteres.
- Instagram: Es una aplicación móvil que permite a los usuarios compartir fotografías o videos con variedad de efectos, marcos, temperatura de color. Actualmente es una de las redes más populares entre adolescentes y jóvenes, por tanto, su buena gestión y calidad en las fotografías puede impactar de manera positiva.
- YouTube: Es la plataforma más popular para la publicación y visualización de videos. Los temas son variados: videos musicales, documentales, entretenimiento, piezas educativas, entre otras categorías.
- LinkedIn: Es la mayor red de profesionales en el mundo, está orientada a generar relaciones comerciales y profesionales.

Teniendo en cuenta estas premisas generales y considerando las características de las redes sociales, estamos en condiciones de adentrarnos en el tema relacionado con los ataques y vulnerabilidad en las redes sociales. Primero se debe reconocer que se trata de un tema actual, complejo y pertinente, el cual dada sus propias dimensiones requiere de una mirada permanente e integral. Por tanto, abordar el mismo implica situarnos frente a una problemática social aún sin resolver, precisamente porque cada vez las personas hacemos más uso de las redes sociales y estamos siendo más vulnerables antes los posibles ataques y amenazas. Entender esta relación desde una posición holística y responsable nos permite encontrar posibles soluciones.

Según varios autores se identifican diversos tipos de ataques que se presentan en las redes sociales, como phishing, trolling y malware (Alsharnouby, Alaca y Chiasson, 2015, Mansour, 2016, Fokes & Li, 2014, y Vishwanath, 2015). Los ataques de phishing en las redes sociales ocurren en plataformas relativamente nuevas y en evolución como Facebook y Google Plus, donde la interfaz, sus funcionalidades y sus protecciones de usuario cambian constantemente. Este tipo de ataque suelen tener dos etapas; en la primera, el *phiser* envía una solicitud de amistad e intenta hacer amistad (contactarse con la posible víctima), la aceptación podría ayudar al atacante a recopilar gran cantidad de información, lugar de trabajo, donde reside, números telefónicos entre otros datos personales. La segunda etapa utiliza la función de mensajería incorporada que viene incorporada en Facebook para solicitar información directamente a la víctima.

Otro tipo de ataque es el Trolling, se refiere a los usuarios que responden en las redes sociales con publicaciones y comentarios inventados y, a menudo, inflamatorios para provocar un aumento en los usuarios (Hanson, 2019). En este sentido, DiResta et al. (2019) señalan que un actor malicioso interesado en trollear busca "empujar" opiniones sobre temas polarizantes o controvertidos discutidos a través de las redes sociales, por ejemplo, campañas electorales, cambio climático, vacunación, política de inmigración, salud reproductiva y libertad de expresión política.

Dentro de las modalidades de ataque que se presentan con frecuencia se encuentran los malware; estos virus podrían programarse para dispersarse en determinados momentos y extraer información del teléfono inteligente, la computadora. En concordancia con Stewart et al. (2019) una alternativa más económica es un malware que actúa como intermediario en el intercambio de información en línea y manipula la autenticidad del contenido percibido por individuo objetivo. La ventaja del malware es que es independiente de la plataforma (es decir, puede funcionar en Facebook, Twitter o Reddit) puede empaquetar estratégicamente como una extensión del navegador web o una aplicación de redes sociales de terceros para teléfonos inteligentes.

De acuerdo con Cialdini (2007) al igual que el phishing, el malware también emplea los principios psicológicos de persuasión para obtener los bienes de las personas (por ejemplo, permisos), pero no para dañar los archivos locales o la filtración de datos (pág. 4). En su lugar, según Zannettou et al. (2019), el objetivo es utilizar los permisos del sistema para manipular encubiertamente los datos textuales en interpretación del contenido legítimo, sesgado hacia el objetivo del actor malintencionado, por ejemplo, los trabajadores furtivos o los votantes sesgados (pág. 255).

En este sentido, se coincide con Conteh y Schmick (2016), en que las personas son fácilmente pirateadas, por lo que ellas y sus publicaciones son objetivos de ataque de alto riesgo (pág. 32). Particular interés tiene en este orden el estudio realizado por los autores precedentes,

quienes evaluaron las vulnerabilidades de la infraestructura de tecnología de la información de una organización, que incluyo los sistemas de hardware y software. En su investigación destacan la importancia y el papel de la ingeniería social en las intrusiones en la red y el robo cibernético, analizando además las razones de la rápida y alarmante expansión del ciberdelito. Bisson (2019) señala que la ingeniería social es "un término que abarca un amplio espectro de actividades maliciosas" e identifica cinco de los tipos más comunes de ataques de ingeniería social dirigidos a víctimas, que incluyen: Suplantación de identidad, Pretextos, Cebo, Tailgating, todos altamente peligrosos. Siguiendo estas ideas es importante considerar otros aspectos que están relacionados con los ataques y vulnerabilidad que se dan en sitios abiertos, es decir, aquellos que se encuentran en bases de información disponible públicamente, fuentes tales como: periódicos, revistas, sitios de redes sociales, sitios para compartir videos, wikis, blogs, los cuales son también muy vulnerables.

Para Mittal, Das, Mulwad, Joshi, y Finin (2016), indican que: las fuentes de información de ciberseguridad se pueden dividir en dos grupos abstractos, fuentes formales como la Base de Datos Nacional de Vulnerabilidad (NVD) del NIST, el Equipo de Preparación para Emergencias Informáticas de los Estados Unidos (US-CERT), y varias fuentes informales como blogs, foros de desarrolladores, salas de chat y plataformas de redes sociales como: Twitter, Reddit y Stackoverflow, proporcionan información relacionada con vulnerabilidades de seguridad, amenazas y ataques (pág. 860). Señalan que diariamente se publica mucha información sobre estas fuentes, lo que hace que sea casi imposible para un analista humano peinar manualmente. (pág. 806). Ellos explican que Twitter, en la última década se ha convertido en una fuente vital de inteligencia de código abierto, señalando que los datos proporcionados en estas redes sociales han sido utilizados por investigadores para recopilar información importante en temas como: el impacto de desastres naturales, ataques terroristas, elecciones gubernamentales predicción de mercados de valores; sin embargo resulta interesante que en su artículo utilizan Twitter como fuente de información para estudiar diversos eventos de ciberseguridad y destacar su importancia desde otra mirada.

También, estos autores plantean que los usuarios de Twitter, cuando se hacen públicas nuevas vulnerabilidades, tuitean sobre estas vulnerabilidades para difundir información en la red, de modo que otros puedan usar esa información en particular para proteger sus sistemas. Resulta meritorio reconocer que si bien Twitter, puede ser una red objeto de alta vulnerabilidad, también puede emplearse como una vía eficaz para mitigar o contrarrestar dichos ataques. Señalan que CyberTwitter puede ayudar a los analistas de seguridad a tomar decisiones importantes manteniéndolos actualizados sobre diversas vulnerabilidades y amenazas.

En el caso de Facebook y en el resto de las redes sociales con mucha frecuencia también son objetos de constantes ataques y amenazas; lograr controlar esto va a depender mucho del

nivel de cultura y educación que se alcance en todos los usuarios y en establecer mecanismos adecuados de protección y mitigación. La literatura consultada enfatiza en que dentro de las vulnerabilidades más importantes se puede mencionar: Los ataques de confidencialidad, sobre todo los referidos al almacenamiento criptográfico inseguro, referencia insegura a objetos directos, fuga de información y manejo incorrecto de errores; comprometiendo así el principio de confidencialidad de la información. Otro ejemplo lo constituyen los ataques de integridad, el cual hace un desbordamiento de búfer, una falsificación de solicitudes en sitios cruzados, scripting de sitios cruzados, restringe el acceso a la URL, o una ejecución maliciosa de archivos afectando directamente a uno de los principios básicos de la información como es la integridad. Y por último citan como otra forma de vulnerabilidad a la disponibilidad la cual hace una denegación de servicio a los Sistemas de Gestión de Aprendizaje misma que incide directamente al principio de la disponibilidad de la Información.

Otro ataque que se presentan en las redes sociales según Gómez Almanza, Castillejo, y Vargas (2013), es el cyberbulling y la intimidación entre adolescentes que se presentan de manera frecuente en los centros educativos, por la gran facilidad que se presenta al acceso y uso de nuevas tecnologías por parte de los estudiantes (pág. 34) Esto se da por la falta de regulación o supervisión del uso del internet. Actualmente al evaluar como inciden los ataques y amenazas en el uso de las redes sociales se ha tornado un tema recurrente y de particular interés en todos los escenarios, incluyendo Ecuador; país donde según Hernández Mite, Yánez Palacios y Carrera Rivera (2017), se exhibe hoy un mayor número de penetración de las Tecnologías de la Información y la Comunicación entre los países de América Latina, superando a los países de Bolivia, Honduras, Nicaragua. Facebook es quien lidera en tabla de ranking entre los 90 sitios más visitados, lo que demuestra que las redes sociales en la actualidad son un medio de comunicación importante en el país.

En este orden de ideas se parte de considerar que la incidencia de los ataques y amenazas afectan grandemente la optimización del uso de las redes sociales. Cabe señalar que los artículos analizados han mostrado gran preocupación al respecto. Especial interés tiene para el investigador de este estudio delimitar la incidencia de los ataques y amenazas en el uso adecuado de las redes sociales, no sólo por su incidencia a nivel individual, sino también por la afectación en el orden social, profesional, académico y psicológico. Como puede apreciarse existe una gran variedad de modalidades y formas de ataques en las redes sociales, todo esto las hace en extremo vulnerables para los usuarios; los cuales se ven en la necesidad de adoptar medidas que mitiguen tanto los posibles ataques como su alta vulnerabilidad.

Se analizó las diferentes redes sociales, ocupando un lugar fundamental Facebook, por ser esta la red con mayor número de usuarios. Según cita Vishwanath (2015), en su estudio sobre: El uso habitual de Facebook y su impacto en ser engañado en las redes sociales, explica que el uso habitual o frecuente de Facebook por parte del individuo, manteniendo una gran red

social y siendo deficiente en su capacidad para regular tales comportamientos, es el mayor predictor de victimización individual en los ataques a las redes sociales. Además, señala que a diferencia de los ataques de phishing basados en correo electrónico que tienen una tasa de éxito inferior al 1%, los ataques de phishing en las redes sociales parecen ser mucho más exitosos y los ataques simulados reportan una tasa de éxito superior al 40%. Infiriendo que la alta tasa de victimización se puede atribuir a la naturaleza única de los ataques de phishing en las redes sociales, ya que en muchas ocasiones están relacionadas con la interfaz, sus funcionalidades y sus protecciones de usuario debido a que estos cambian constantemente. En consecuencia, según indica el autor es posible que las personas no puedan lograr cierto grado de dominio sobre el uso de la plataforma.

De ahí que se dé una alta incidencia de estos ataques y amenazas en el uso adecuado de las redes sociales. Como es lógico su impacto siempre compromete su utilidad y uso adecuado, afectando e incidiendo en planos más complejos como son los aspectos psicológicos de los usuarios; los cuales al ser recurrentes en su uso pueden volverse adictos y muy vulnerables ante los posibles ataques y amenazas (Tai, Dhaliwal y Shariff, 2020).

RQ2: ¿Los actuales mecanismos de seguridad son eficientes ante los ataques y amenazas que se dan en las redes sociales?

Siguiendo este orden de ideas es importante reconocer que con la implantación y desarrollo de la información en tiempo real y del auge de la inteligencia artificial surge un problema principal: la integridad y la seguridad de la información. Precisamente una de las problemáticas a la que deben enfrentarse los responsables de la ciberseguridad está dado, en que deben crear mecanismos de seguridad, que sean capaces de contrarrestar las vulnerabilidades que presentan los sistemas informáticos instalados. El problema como tal, surge desde el propio inicio de la creación de estos sistemas y fue mayormente relacionado con la inteligencia militar.

En este contexto, Steele (1996), señaló que, en el amplio dominio de la seguridad, los analistas y los responsables de la formulación de políticas necesitan conocer el estado del mundo para tomar decisiones críticas oportunas, tanto operativas / tácticas como estratégicas. Este conocimiento debe extraerse de una variedad de fuentes diferentes y luego representarse en una forma que permita un mayor análisis y toma de decisiones. Algunos de los datos subyacentes a este conocimiento se encuentran en fuentes textuales tradicionalmente asociadas con la inteligencia de código abierto (OSINT).

Conforme a Mathews, Halvorsen, Joshi y Finin, (2012), OSINT es información recopilada de información disponible públicamente de fuentes abiertas, tales como periódicos, revistas, sitios de redes sociales, sitios para compartir videos, wikis, blogs, etc. En el dominio de la ciberseguridad, la información disponible a través de OSINT puede complementar los datos

obtenidos a través de los sistemas de seguridad tradicionales y herramientas de monitoreo como los sistemas de prevención y detección de intrusiones (IDPS).

Dado lo anterior, Neri y Geraci (2009), y Maciolek y Dobrowolski (2013), han señalado que la extracción automática de información relevante de fuentes OSINT ha recibido la atención de la comunidad de investigadores. En este enfoque, Mittal et al. (2016) enfatizan que la naturaleza en tiempo real de la información en Twitter ha permitido a los investigadores proporcionar información significativa durante los "eventos de alto impacto".

En esta dirección Mittal et al. (2016) explican que la detección y actualización de diversas amenazas y vulnerabilidades pueden considerarse eventos de ciberseguridad que afectan los sistemas informáticos. Por lo tanto, son del criterio que Twitter puede ser una fuente eficaz para recopilar información sobre amenazas a la seguridad cibernética.

Según Informe presentado por *European Union Agency for Network and Information Security*, (2018), indica registra el comportamiento a nivel europeo en el último decenio, las principales causas de incidentes de seguridad, se han producido por: Error Humano 21%, Acciones maliciosas 7%, Fallo en los Sistemas de Seguridad 36% y Fallos de Terceras Partes 37%. Respecto a ello, Soria Olivas (2019) comenta que un porcentaje muy importante de los incidentes de seguridad se deben a errores humanos y otro porcentaje considerable a errores de los sistemas de seguridad. Además, respecto a la severidad de los Incidentes de Seguridad registrados, indican que el 54% fue significante, un 23 % fue severo y otro 23 % fue desastroso.

En este ámbito, la evolución de los incidentes registrados en España a partir de los datos obtenidos por el Centro Criptológico Nacional-*Computer Emergency Response Team*, también conocido por su sigla CCN–CERT, (CCN-CERT, 2020), en el período 2014 al 2019, tuvo el siguiente comportamiento:

- Año 2014: Se produjeron 12916 ciberataques.
- Año 2015: Se produjeron 18232 ciberataques.
- Año 2016: Se produjeron 20807 ciberataques, de ellos 556 de muy alta peligrosidad.
- Año 2017: Se produjeron 26472 ciberataques, de ellos 900 de muy alta peligrosidad.
- Año 2018: Se produjeron 38192 ciberataques, de ellos 2219 de muy alta peligrosidad.
- Año 2019: Se produjeron 42997 ciberataques, de ellos 3209 de muy alta peligrosidad.

Todo lo anterior, demuestra que no obstante al desarrollo alcanzado en los sistemas y mecanismos de seguridad, se continúan produciendo ataques y amenazas a las organizaciones y sus Sistemas de Información y a las Redes de Comunicaciones.

Para Conteh & Schmick, (2016), la tasa de éxito y el número de delitos cibernéticos aumentan constantemente debido al nivel de anonimato que la ingeniería social ofrece a los actores maliciosos. Las empresas deben estar al tanto de los diversos actores de amenazas y su gran

cantidad de ataques para poder responder en consecuencia. Se puede concluir que los actuales mecanismos de seguridad son eficientes en contrarrestar los ataques y amenazas que se dan en las redes sociales; pero debido a los constantes ataques, amenazas y vulnerabilidad a la cual están expuestas las redes sociales, y en particular los usuarios de estas, los mecanismos de seguridad deben ser objeto de constante actualización y desarrollo, dado que como se ha demostrado, los ciberataques continúan registrando segundo tras segundo en la redes sociales.

Al respecto se coincide con Conteh & Schmick (2016), al indicar que actualmente existen salvaguardas técnicas y no técnicas que se pueden implementar para reducir el riesgo asociado con la ingeniería social a un nivel tolerable. Además, expresan que las empresas están añadiendo múltiples capas a sus esquemas de seguridad de modo tal que si falla el mecanismo en la capa externa, un mecanismo en al menos una capa interna puede ayudar a prevenir que una amenaza se convierta en un desastre (Mitigación de Riesgos). Este concepto se conoce como defensa multicapa o defensa en profundidad.

RQ3: ¿Cuáles serían las posibles soluciones o los algoritmos a adoptar?

Como se ha expresado con antelación y en conformidad con Polakis, Maggi, Zanero y Keromytis (2014), la participación masiva de los usuarios ha convertido a las redes sociales en línea, en un objetivo valioso para los atacantes y en una plataforma lucrativa para implementar varios tipos de ataques, que van desde spam, hasta campañas personalizadas de phishing. Para mitigar el ataque de phishing, Jamil et al. (2018) presentaron algunos esquemas heurísticos que detectan este tipo de ataque. El modelo funciona para ataques unidireccionales, observa que el enlace solicitado por el usuario es seguro o engañoso y adicional es capaz de identificar si el atacante evita el modelo de verificación.

Para el spammers, Luhach, Kosa, Poonia, Gao y Singh (2020) crea un mecanismo de detección de mediante el uso de un modelo basado en aprendizaje automático que utiliza el algoritmo de optimización por enjambre de partículas (PSO, por sus siglas en inglés) de un conjunto de característica y algunos métodos de aprendizaje supervisados, el resultado de este mecanismo según pruebas realizadas por los proponentes indica una tasa de detección del 99%. Todo lo anterior, corrobora que las redes sociales y de comunicaciones se encuentran en un constante incremento de sus usuarios, por lo que se hace vital encontrar soluciones más eficientes para contrarrestar, tal y como se ha expuesto, el ciber delito que se realiza a estas redes. Para ello, se hace contar con la seguridad informática requerida.

Según Trufanov, Kinash, Tikhomirov, Berestneva y Rossodivita (2017), para una mayor aclaración de las cuestiones metodológicas de la seguridad de la información de la red social, se debe estratificar los sistemas que sustentan las relaciones humanas en tres componentes de diferente naturaleza: informática, comunicación y social. De esta forma, ellos sugieren que

debe desarrollarse un modelo de seguridad para un componente de red teniendo en cuenta la seguridad de los nodos individuales. El modelado de los ataques a las redes en su conjunto se analiza teniendo en cuenta la especificación del nivel de seguridad de la red. Como regla para cualquier estructura de red, se aducen cuatro problemas principales de riesgo topológico:

a) Desintegración bajo ataques aleatorios o coordinados en redes complejas;
b) Fallas en cascada;
c) Congestión;
d) Procesos de difusión de actividades maliciosas.

En otro punto de vista, Valle (2018) destaca que, si bien es cierto que internet y la tecnología, son herramientas con mucho potencial, es importante considerar que un mal uso puede traernos complicaciones, por tanto, es obvio que hay que aprovechar las bondades tecnológicas y comunicativas actuales, pero a partir del conocimiento de los riesgos para poder prevenirlos. Todo lo anterior reafirma que, dentro de las primeras soluciones para hacer frente a los ciberataques, pueden ser citadas las de orden tecnológicas, con herramientas y equipos especializados, programas, software altamente fiable de protección de acceso a servidores y nubes, antivirus y también legales, requiriéndose de leyes estrictas y severas que permitan la disuasión de los atacantes.

Otra de las formas para poder desarrollar acciones conducentes a mitigar los ataques, amenazas y vulnerabilidad presente por el uso de las redes sociales, está ubicado en un elemento de alta significatividad, se trata del control y educación del factor humano. En este orden de ideas especial interés tiene, lo planteado por Altamirano & Bayona (2017) se requiere tener una mirada multidisciplinar del tema, para dar cumplimiento a las políticas de seguridad es necesario en primer lugar, comprender el comportamiento humano a través de teorías psicológicas o sociales, lo cual conduce a tener un enfoque interdisciplinario que permita una visión global, no solo desde la perspectiva tecnológica, sino también desde otras disciplinas, que en su conjunto conlleve a un enfoque real del problema.

Kruger, Drevin, Flowerday y Steyn, (2011) señala la importancia de evaluar el factor humano en todo lo concerniente a las vías de protección y seguridad, especialmente cuando se hace uso de las TIC. En este sentido consideran que un programa de sensibilización sobre la seguridad de la información puede ser un instrumento importante en la protección de los activos de información. Shoufeng, Shixin, Geng y Yi (2019) resaltan la importancia de proponer y probar un modelo de investigación para examinar el impacto de la educación InfoSec en el uso de las redes sociales, reafirmando la idea de atender el factor humano como uno de los elementos más críticos en torno a los temas de seguridad.

Siguiendo en esta línea sobre el factor humano, es importante considerar que el trabajo educativo debe iniciarse desde las primeras edades. Educar a nuestros hijos en el uso adecuado de las redes sociales, constituye además de una responsabilidad un deber

ineludible. En correspondencia con ello, Astorga Aguilar y Schmidt Fonseca (2019) evalúan en su estudio el rol de los padres y las madres de familia en relación con la educación y preparación de los hijos para el uso correcto de las redes sociales. Enfatizan en que educar en ciberseguridad a las personas menores de edad es un nuevo reto para los padres y las madres de familia, que deben prepararse y conocer para enseñarles a protegerse de estos nuevos peligros.

En el caso de Ecuador, al ser una población con un alto índice de uso de las redes sociales, se han venido implementando una serie de acciones encaminadas mitigar los posibles ataques, amenazas y vulnerabilidades a los cuales están expuesto los usuarios. Sin embargo, el tema aún persiste. Destaca aquí los aportes de Toapanta, Quimi, Lambogglia y Gallegos (2019), al explicar que, para mitigar los riesgos, vulnerabilidades y amenazas en el manejo de la información pública a corto plazo, se deben generar modelos de seguridad integrados como alternativa acompañados de la utilización de algoritmo criptográfico para asegurar que el manejo de la información sea con identidad, autenticidad, autorización y auditoría (IAAA). Señalan los autores que se debe contar además con políticas de seguridad, responsables, tecnologías y algoritmos criptográficos adecuados para mejorar la confidencialidad, integridad y disponibilidad de la información en base a su misión, visión, objetivos estratégicos de cada organismo gubernamental y disposiciones legales como la ley orgánica de transparencia y acceso a la información pública LOTAIP 2017.

Lo anterior deja claro una idea esencial y es que precisamente los temas de seguridad y los posibles mecanismo o soluciones para su mitigación, no solo se resuelven con la protección desde el punto de vista técnico, es decir sólo creando medidas tecnológicas o políticas que puedan mitigar los ataques y amenazas; de nada serviría esto si no van acompañadas de la valoración del factor humano. De ello se desprende a nuestro criterio dos puntos de interés:

1. El primero está relacionado con la educación y cultura social sobre cómo manejar y emplear de forma adecuada el uso de las redes sociales, lo cual implica educar a diferentes usuarios y desde las primeras edades en un uso correcto de las redes.
2. El segundo a nuestro juicio tiene que ver con la implementación de sistemas de capacitación y actualización sistemática a los usuarios. Esto permitiría mantener a los usuarios preparados y alertas ante cualquier ataque o amenaza.

En resumen, estar alerta y buscar verdaderas soluciones sobre los posibles ataques y amenazas, presupone comenzar a entender que, dada la complejidad de la situación, los procesos de intervención y solución tienen que tener un accionar multidisciplinar y ello implica:

1. Contar con una población y usuarios capacitados y actualizados.
2. Tener un sistema tecnológico moderno, amplio e integral que pueda hacer frente a las disímiles manifestaciones de ataques, amenazas y vulnerabilidades.

3. Contar con un sistema de políticas que normen, regulen y protejan a los usuarios sobre el uso de las redes sociales.

Análisis de los resultados obtenidos

En este trabajo se identificaron un total de 328 artículos científicos, de los cuales quedaron seleccionados 28 trabajos potenciales, por cumplir estos con los criterios de inclusión determinados previamente en relación con el tema de investigación. Un análisis del histograma muestra que la producción científica relacionada con los ataques, vulnerabilidades y mecanismos de seguridad en las redes sociales contempló un rango comprendido entre los años 2012 y 2020, el cual expone que, a inicios del 2012, empiezan a publicarse artículos relacionados al tema, resultando el 2019, el año donde se produjo el mayor número de publicaciones científicas tocantes con la ciberseguridad en las redes sociales.

De lo expuesto en los materiales y documentos ubicados en el rango de tiempo señalado y que fueron consultados por el autor, se lograron determinar y sistematizar tres teorías que según criterios del investigador resultan de extrema importancia para analizar y debatir sobre el tema que nos ocupa: ataques, vulnerabilidad y posibles soluciones para su mitigación desde una concepción teórica de las ciencias. (Figura 3)

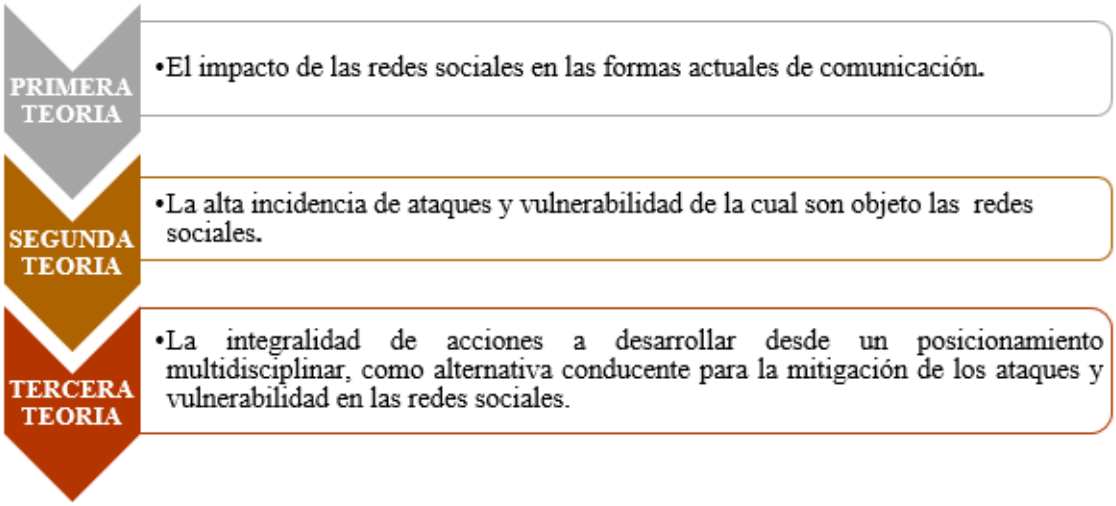

Figura 3. Teorías sistematizadas en relación al tema de investigación.

A continuación, se procede a debatir y emitir los juicios y valoraciones derivados del estudio realizado y de la sistematización de las teorías precedentes.

Primera Teoría. El impacto de las redes sociales en las formas actuales de comunicación.

Después de analizar las teorías precedentes una de las primeras ideas que se logró extraer y sistematizar del estudio realizado, es que, en la mayoría de las fuentes consultadas, se indica

que, a la luz de los nuevos avances científicos –tecnológicos, las redes sociales se han consolidado como una de las herramientas de comunicación más utilizadas dentro de la sociedad actual. En este orden destacan los aportes de Ciolan (2014), Rahman et al. (2016) y Ikhalia et al. (2019), los cuales apuntan que las redes sociales, han captado la atención de miles de usuarios. Lo anterior nos permite asumir que la revolución tecnológica, marcada desde hace algunos años por la introducción de las redes sociales, ha ido desechando progresivamente los métodos tradicionales o convencionales de comunicación para ir incursionando de forma ascendente en estas nuevas modalidades, lo cual sin lugar a dudas ha dado lugar a grandes avances en todos los procesos.

En esta misma línea, es meritorio señalar que el caso de Ecuador, ha quedado evidenciado que se encuentra entre los países de América Latina, donde se hace un uso sistemático de la red social. En la actualidad constituyen un medio de comunicación importante en el país, superando a países como Bolivia, Honduras, Nicaragua; siendo Facebook, la red social que lidera en tabla de ranking entre los 90 sitios más visitados.

Lo cierto es que, con la llegada de Facebook, Twitter, YouTube, LinkedIn y recientemente Instagram, se han instaurado tanto a nivel internacional como nacionales formas más novedosas de comunicación, lo cual ha incidido positivamente en la viabilidad y factibilidad en los diferentes procesos (Ciolan, 2014). Esto ha permitido revolucionar tanto las vías de comunicación, como las experiencias en su uso y empleo. Dentro de sus ventajas destacan las relacionadas con los bajos costos, la facilidad que ofrecen para establecer la interacción entre las personas, el acercamiento y la accesibilidad a la información, la eficacia y rapidez en múltiples áreas del conocimiento, entre otras. A ello se une las posibilidades que tienen de ser utilizadas por diferentes públicos de diversas edades y características. (Hernández Mite et al., 2017).

Sin embargo, independientemente de los múltiples beneficios que ha traído el uso de las redes sociales, paradójicamente con su utilización exponencial, surgen nuevas preocupaciones relacionadas con los ataques y alta vulnerabilidad que se presenta como consecuencia de su uso indiscriminado y es aquí donde comenzamos a sistematizar la segunda teoría que se desprende de esta investigación.

Segunda Teoría. La alta incidencia de ataques y vulnerabilidad del cual son objeto las redes sociales.

En este sentido se considera que, si bien el uso de las redes sociales es ya una parte integrante de nuestra cotidianidad, también hay que observar que los ataques, amenazas y alta vulnerabilidad son cada vez más frecuente y aún no se encuentran los mecanismos que logren mitigarlos en su totalidad. Es consideración del autor de la presente investigación que estamos ante un problema social muy complejo, de múltiples dimensiones y por supuesto que

requiere de un accionar multidisciplinar para solucionarlo en la media de las posibilidades. Se coincide con Hernández Mite et al. (2017), en que los ataques y amenazas en el uso de las redes sociales se ha tornado un tema recurrente y de particular interés en todos los escenarios, incluyendo Ecuador.

Conforme con lo planteado por Fokes y Li (2014), Alsharnouby et al. (2015), Vishwanath (2015), Mansour (2016), Hanson (2019), y otros autores, se pueden identificar varios tipos de ataques, dentro de los más frecuentes se encuentran los phishing, trolling y malware, los cuales suelen ocurrir en plataformas relativamente nuevas y en evolución como Facebook y Google Plus, donde la interfaz, sus funcionalidades y sus protecciones de usuario cambian constantemente. Uno de los aspectos que más caracterizan y preocupan en relación con estos tipos de ataques es que emplean principios psicológicos para persuadir a los usuarios y obtener autorización de ellos para operar con determinadas informaciones. (Cialdini, 2007, Zannettou et al., 2019).

Se concuerda con Conteh y Schmick (2016), en que las personas son fácilmente pirateadas, por lo que ellas y sus publicaciones en redes sociales son objetivos de ataque de alto riesgo, requiriendo para evitarlo conocer el manejo adecuado de las regulaciones existentes para su mitigación y uso apropiado. De igual manera las empresas y organismos que hacen uso de las redes sociales se tornan altamente vulnerables teniendo que recurrir al empleo de sistemas de hardware y software que los protejan del robo cibernético y la alarmante expansión del ciberdelito.

Las revisiones de las teorías precedentes nos han permitido también convenir con los aportes Bisson (2019), al identificar dentro de los tipos más comunes de ataques de ingeniería social dirigidos a víctimas, cinco ejemplos, dentro de estos se incluyen: Suplantación de identidad, Pretextos, Cebo, Quid pro quo, Tailgating, todos altamente peligrosos. Otro de los tipos muy frecuentes de ataques dirigidos a personas que hacen uso de las redes sociales, son los denominados cyberbulling, que según los criterios de Gómez Almanza et al. (2013) y el nuestro es muy perjudicial, debido a que implica la intimidación constante entre los adolescentes, siendo este por sus modos y consecuencias muy importante de ser atendido y regulado a tiempo. Una posible solución estaría en enseñar a los adolescentes que hagan un uso adecuado del internet.

De igual manera han quedado identificados en el proceso investigativo desarrollado que existen otros aspectos que están relacionados con los ataques y vulnerabilidad y que se dan en sitios abiertos, es decir, aquellos que se encuentran en bases de información disponible públicamente, fuentes tales como: periódicos, revistas, sitios de redes sociales, sitios para compartir videos, wikis, blogs, los cuales son también muy vulnerables.

En correspondencia con lo explicado y siguiendo esta línea de pensamientos se debe señalar que la incidencia de los ataques y amenazas afectan grandemente la optimización del uso de

las redes sociales, siendo Facebook la red con mayor incidencia de ataques y amenazas. Cada vez las personas hacemos más uso de las redes sociales y cada vez, estamos siendo más vulnerables antes los posibles ataques y amenazas. Entender esta relación desde una posición holística y responsable nos permite valorar con mayor objetividad la eficacia de los actuales mecanismos de protección en función de encontrar posibles soluciones y proteger la integridad y la seguridad de la información tanto gubernamental, empresarial como individual. Es precisamente en este punto donde se deriva la tercera idea o teoría del presente estudio.

Tercera Teoría: La integralidad de acciones a desarrollar desde un posicionamiento multidisciplinar, como alternativa conducente para la mitigación de los ataques y vulnerabilidad en las redes sociales.

La necesidad de integrar los mecanismos de seguridad para buscar que estos sean realmente eficientes ante los ataques, amenazas y vulnerabilidad que se dan en las redes sociales es una acción prioritaria en los momentos actuales, máxime si tenemos en cuenta que cada día son más los usuarios que hacen uso de estas redes. En este orden se concierta con Altamirano y Bayona (2017), en que a nivel organizacional y empresarial la mayoría se rigen por políticas de seguridad para proteger la confidencialidad, integridad y disponibilidad de los recursos de la información. Como bien plantean estos autores y con los cuales se comparte, existen políticas y procedimientos establecidos para buscar mitigar los riesgos y amenazas relacionados con el uso inescrupuloso de las redes sociales.

Existen además controles técnicos dirigidos a regular y prevenir los ataques y amenazas que constituyen mecanismos establecidos tanto a nivel internacional como nacional, por ejemplo para mitigar el ataque de phishing (Jamil et al., 2018) presentaron algunos esquemas heurísticos que detectan este tipo de ataque, mientras que Luhach et al., (2020) crea un mecanismo de detección mediante el uso de un modelo basado en aprendizaje automático que utiliza el algoritmo de Optimización por enjambre de partículas PSO de un conjunto de característica y algunos métodos de aprendizaje supervisados.

En el contexto ecuatoriano resaltan las contribuciones de Toapanta et al. (2019) al explicar que, para mitigar los riesgos, vulnerabilidades y amenazas en el manejo de la información pública a corto plazo, se deben generar modelos de seguridad integrados, acompañados de la utilización de algoritmo criptográfico, para así asegurar que el manejo de la información sea con identidad, autenticidad, autorización y auditoría (IAAA). Ahora bien, independientemente a todo lo explicado y pesar de las acciones desarrolladas desde el punto de vista de políticas, normativas y apoyo tecnológicos para mitigar los ataques y prevenir el alto grado de vulnerabilidad que se presenta en las redes sociales, estamos convencidos que lo realizado hasta el momento es ineficiente y difícilmente controlable en su totalidad.

Cabe recalcar que la comunidad científica que se ha venido dedicando a investigar estos temas, no solo ha identificado en las posibles soluciones los elementos relacionados con políticas, regulaciones, normativas y apoyos en cuanto a tecnología e infraestructura, unido a ello ha registrado como uno de los principales eslabones que incide de manera positiva o negativa en la prevención y mitigación de estos flagelos, el comportamiento humano frente al uso de las redes sociales. Ante lo planteado se comparte con Kruger et al. (2011), al insistir en la necesidad de educar a los usuarios en el empleo correcto de las redes sociales. De igual manera resultan muy interesante los criterios de Astorga Aguilar y Schmidt Fonseca (2019), al enfatizar en el rol de los padres en relación con la educación y preparación de los hijos para el uso correcto de las redes sociales desde edades. Se trata por tanto de tener una mirada multidisciplinar al problema relacionado con los ataques, amenazas y alta vulnerabilidad a las cuales son objetos los usuarios de las redes sociales.

Como hemos venido sistematizando a lo largo de esta investigación estamos ante una situación social, compleja, que demanda de urgentes soluciones debido a que los temas de seguridad y los posibles mecanismo o soluciones para su mitigación, no solo se resuelven con la protección desde el punto de vista técnico, o creando medidas tecnológicas o políticas que puedan mitigar los ataques y amenazas a las cueles están expuestas las redes sociales de manera permanente; de nada serviría esto si no van acompañadas de la valoración del factor humano.

Es por ello tan significativo, contar con una población culta, educada con valores éticos, que le permitan hacer un uso adecuado de estas novedosas y útiles formas de comunicación llamadas a ser parte indispensable de nuestro diario vivir. Hacer un uso responsable de las mismas no solo mitigará los posibles ataques y vulnerabilidad, que como es lógico pensar, van posiblemente a estar presentes, sino que permitirá optimizar su utilización e incidir positivamente en la diversidad de su empleo.

Derivado del análisis y debate realizado se considera importante insistir en la integralidad del fenómeno estudiado (Figura 4).

Estableciendo la integralidad del problema objeto de estudio y analizando la expresión gráfica de la figura 4, podemos apreciar las siguientes particularidades:

- Presencia de un alto porcentaje en cuento al uso de las diversas redes sociales.
- Constantes ataques y amenazas que las tornan muy vulnerables.
- Mecanismos de seguridad que intentan cada vez más ser efectivos, pero que no se logra en su totalidad.
- Necesidad de una intervención multidisciplinar del problema.
- Presencia de dos grandes desafíos.

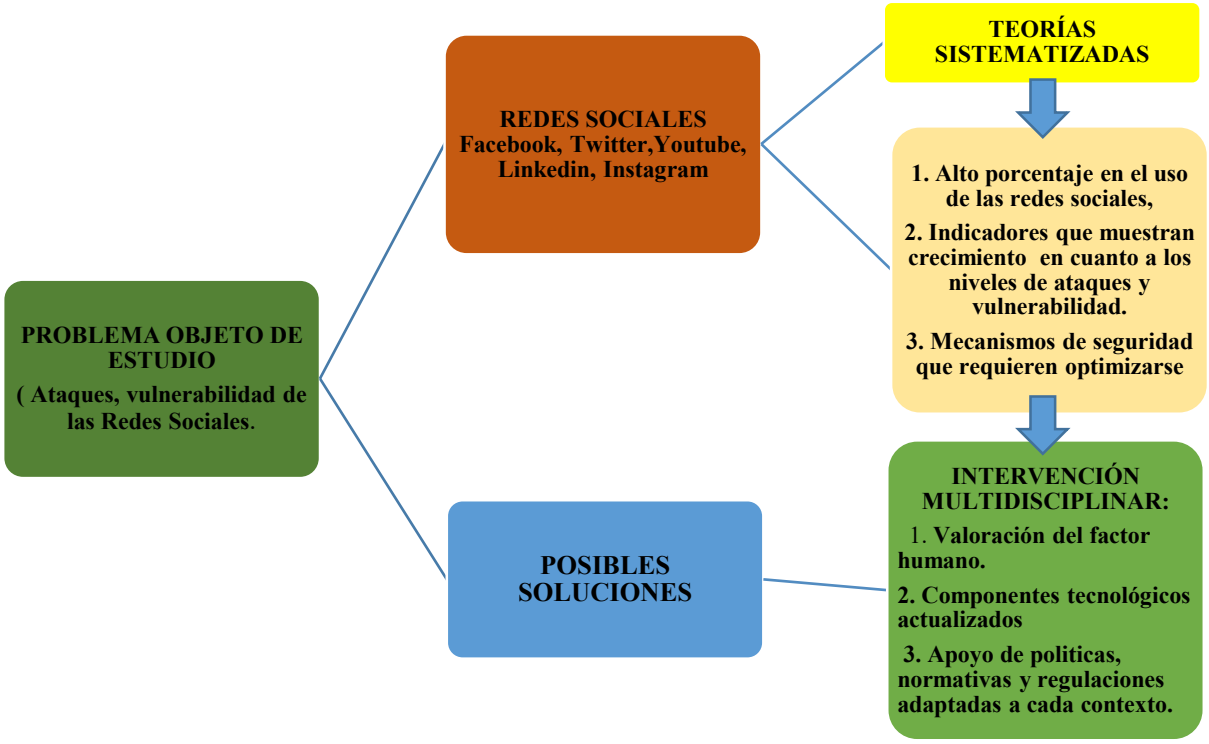

Figura 4. Integralidad del fenómeno estudiado. Posibles soluciones.

En resumen, a juicio del autor existen a corto y mediano plazo dos grandes desafíos para poder solventar la situación actual, el primero está relacionado con encontrar alternativas que ayuden a hacer converger en una misma línea de trabajo los tres componentes: el factor humano, el apoyo tecnológico y las políticas y normativas que regulen un uso correcto de las redes sociales. El segundo desafío para tener presente se ubica en la necesidad de mantenernos actualizados y capacitados de forma permanente; no olvidemos que la información y la tecnología cambian segundo a segundo, provocando la aparición de diferentes retos, dentro de los cuales se encuentran las nuevas modalidades de ataques y amenazas que nos hacen altamente vulnerables ante el uso frecuente de las redes sociales.

CONCLUSIONES

El uso de las redes sociales como Facebook, Twitter, YouTube, LinkedIn e Instagram son el resultado del desarrollo científico – tecnológico; y se han propagado de manera exponencial en los últimos años, llegando a captar la atención de millones de personas tanto a nivel nacional como internacional. Las mismas constituyen sin lugar a dudas una de las formas más novedosas de comunicación entre los diferentes tipos de público. En este trabajo se ha podido evidenciar y sistematizar que las redes sociales son objeto de constantes ataques y amenazas

de tipo phishing, trolling, cyberbulling y malware. Esto hace que se requiera prestar especial atención a todo lo relacionado con las diferentes formas de prevención o mitigación contra los ataques y vulnerabilidad a que se están expuesto por su uso.

Por otro lado, el desarrollo de políticas, normativas, resoluciones, unidas a los apoyos y controles técnicos son una de las vías que se han venido empleando tanto por los gobiernos, empresas, organizaciones, directivos y empleados para mitigar los posibles ataques. Sin embargo, la solución a este grave problema queda incompleto, sino somos capaces de atender el comportamiento humano. Se requiere contar con una población educada y culta acerca de cómo utilizar las redes sociales de manera conveniente.

Para mitigar los ataques se puede definir tres aspectos fundamentales: a) políticas y normativas actualizadas que regulen el uso adecuado de las redes sociales, b) apoyos, recursos tecnológicos y personal preparado que permitan detectar y prevenir tempranamente cualquier anormalidad en su uso y c) contar con usuarios altamente capacitados y educados, con sólidos conocimientos sobre el uso de las redes sociales, que puedan promover su praxis basada en principios y valores éticos y morales.

Todo lo anterior, implica potenciar el desarrollo y la utilización de acciones conducentes a mitigar los ataques y vulnerabilidad desde un posicionamiento multidisciplinar, donde converjan a su vez las políticas y normativas, el desarrollo tecnológico y el factor humano.

REFERENCIAS

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82,* 69–82.

Altamirano, J. R., & Bayona, S., (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. *RISTI. Revista Ibérica de Sistemas e Tecnologías de Información*. (25), 112-134.

Alufaisan, Y., Zhou, Y., Kantarcioglu, M., & Thuraisingham, B. (22-24 de julio de 2017). *Hacking social network data mining*. Documento presentado en 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 54–59, Beijing, China

Astorga Aguilar, C., & Schmidt Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *Revista Electronica Educare, 23(3*), 1–24.

Bello, N. & Mejía, P., (2019) *Manual de Gestión y Buenas Prácticas en Redes Sociales.* Bogotá D. C., Colombia: Pontifica Universidad Javeriana de Bogotá.

Bisson, D. (5 de noviembre de 2019) *5 Social engineering attacks to watch out for. The state of security.* Obtenido de http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/.

CCN-CERT (2020) *El Centro Criptológico Nacional presenta su Memoria de Actividades 2019.* Obtenido de https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/10495-el-centro-criptologico-nacional-presenta-su-memoria-de-actividades-2019.html

Celaya, J. (2008). *La Empresa en la WEB 2.0.* Madrid, España: Editorial Grupo Planeta.

Cialdini, R. B. (2007). *Influence: The psychology of persuasion*. New York: Collins.

Ciolan, I. M. (2014). Defining Cybersecurity as the security issue of the twenty first century. A constructivist approach. *The Public Administration and Social Policies Review VI*(1), 120-136.

Conteh, N. Y., & Schmick, P. J. (2016), Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research, 6*(23), 31–38.

DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., ... & Johnson, B. (2019). *The tactics & tropes of the Internet Research Agency.* Documento de U. S. Senate Documents. Obtenido de https://digitalcommons.unl.edu/senatedocs/2/

European Union Agency for Network and Information Security. (2018). *Annual report trust services security incidents 2017.* Publications Office. Obtenido de https://data.europa.eu/doi/10.2824/835041.

Fokes, E., & Li, L. (2014). *A survey of security vulnerabilities in social networking media: The case of Facebook.* Proceedings of the 3rd Annual Conference on Research in Information Technology - RIIT ’14, 57–62, Atlanta, Georgia, E. U. A.

Gómez Almanza, A. C., Castillejo, D., & Vargas, G. (2013). Cyberbullying: Intimidación entre adolescentes a través de la red social Facebook. *Praxis Pedagógica, 13*(14), 31–44.

Hernández Mite, K. D., Yánez Palacios, J. F., & Carrera Rivera, A. A. (2017). Las redes sociales y adolescencias: Repercusión en la actividad física. *Revista Universidad y Sociedad, 9*(2), 242–247.

Herrera, H. H. (2012). Las redes sociales: una nueva herramienta de difusión social networks. *Rev. Reflexiones, 91*(2), 121-128.

Ikhalia, E., Serrano, A., Bell, D., & Louvieris, P. (2019). Online social network security awareness: Mass interpersonal persuasion using a Facebook app. Information *Technology & People, 32*(5), 1276–1300.

Hanson, J. (2019) *Trolls and their impact on social media*. Universidad de Nebraska-Lincoln.

Jamil, A., Asif, K., Ghulam, Z., Nazir, M., Alam, S., & Ashraf, R. (10-13 diciembre de 2018). *MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing*

attacks on Facebook. Documento presentado en 2018 IEEE International Conference on Big Data (Big Data) (p. 5048), Seattle, WA, USA.

Keele, S. (2007). *Guidelines for performing systematic literature reviews in software engineering. Ver. 2.3.* EBSE Technical Report. School of Computer Science and Mathematics Keele University and Department of Computer Science University of DurhamDurham.

Kruger, H. A., Drevin, L., Flowerday, S., & Steyn, T. (15-17 de Agosto de 2011). *An assessment of the role of cultural factors in information security awareness.* Documento presentado en 2011 Information Security for South Africa, 1–7, Johannesburg, South Africa.

Luhach, A. K., Kosa, J. A., Poonia, R. C., Gao, X. Z., & Singh, D. (Eds.). (2020). *First International Conference on Sustainable Technologies for Computational Intelligence: Proceedings of ICTSCI 2019* (Vol. 1045). Singapur: Springer Singapore

Maciolek, P. & Dobrowolski, G. (2013) Cluo: Web-scale text mining system for open source intelligence purposes. *Computer Science (AGH), 14*(1), 45-62

Mansour, R. F. (2016). Understanding how big data leads to social networking vulnerability. *Computers in Human Behavior, 5*7, 348–351.

Mittal, S., Das, P. K., Mulwad, V., Joshi, A., & Finin, T. (18-21 de Agosto de 2016). *CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities*. Documento presentado en 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 860–867, San Francisco, CA, USA.

Mathews, M. L., Halvorsen, P., Joshi, A., & Finin, T. (14 de octubre de 2012). *A collaborative approach to situational awareness for cybersecurity.* Documento presentado en 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, pp. 216–222, Pittsburgh, United States.

Neri, F., & Geraci, P. (15 de julio de 2009). *Mining textual data to boost information access in OSINT*. Documento presentado en 2009 13th International Conference Information Visualisation, pp. 427–432, Barcelona, España.

Polakis, I., Maggi, F., Zanero, S., & Keromytis, A. D. (11 de septiembre de 2014). *Security and Privacy Measurements in Social Networks: Experiences and Lessons Learned*. Documento presentado en 2014 Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS), pág. 18–29, Wroclaw, Polonia.

Rahman, S., Huang, T. K., Madhyastha, H. V., & Faloutsos, M. (2016). Detecting Malicious Facebook Applications. *IEEE/ACM Transactions on Networking*, 24(2), 773–787.

Stewart, A. J., Mosleh, M., Diakonova, M., Arechar, A. A., Rand, D. G., & Plotkin, J. B. (2019). Information gerrymandering and undemocratic decisions. *Nature, 573*, 117-121.

Shoufeng, M., Shixin, Z., Geng L., & Yi, W. (2019), Exploring information security education on social media use Perspective of uses and gratifications theory. *Aslib Journal of Information Management, 71*(5), 618-636.

Soria Olivas, E. (Ed.). (2019). *Ciberseguridad: El reto del siglo XXI.* Valencia, España: Fundació Parc Científic Universitat de València.

Steele, R. D. (1996) Open source intelligence: What is it? why is it important to the military. *American Intelligence Journa*l, 17(1), 35–41.

Tai, K. Y., Dhaliwal, J., & Shariff, S. M. (2020). Online Social Networks and Writing Styles–A Review of the Multidisciplinary Literature. *IEEE Access, 8*, 67024–67046.

Toapanta, S. M. T., Quimi, F. G. M., Lambogglia, L. M. R., & Gallegos, L. E. M. (enero de 2020). *Impact on the Information Security Management Due to the Use of Social Networks in a Public Organization in Ecuador*. Documento presentado en Third International Conference on Smart Trends in Computing and Communications (SmartCom 2019), Bangkog-Tailandia

Trufanov, A., Kinash, N., Tikhomirov, A., Berestneva, O., & Rossodivita, A. (2017) *Optimal Information Security Investment in Modern Social Networking*. En: Gonçalves B., Menezes R., Sinatra R., Zlatic V. (eds) Complex Networks VIII. CompleNet 2017. Springer Proceedings in Complexity. Springer, Cham.

Valle, M. (2018). *Ciberseguridad. Consejos para tener vidas digitales más seguras.* Madrid, España: Editatum.

Vishwanath, A. (2015). Habitual Facebook Use and its Impact on Getting Deceived on Social Media. *Journal of Computer-Mediated Communication, 20*(1), 83–98.

Zannettou, S., Caulfield, T., De Cristofaro, E., Sirivianos, M., Stringhini, G., & Blackburn, J. (mayo de 2019). *Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web*. Documento presentado en Companion Proceedings of The 2019 World Wide Web Conference, pág. 218–226.